Microsoft System Center 2012 R2

System Center 2012 R2 Operations Manager Documentation

Microsoft Corporation

Published: November 1, 2013

Authors

Byron Ricks

Applies To

System Center 2012 – Operations Manager

System Center 2012 Service Pack 1 (SP1) – Operations Manager

System Center 2012 R2 Operations Manager

Feedback

Send suggestions and comments about this document to sc2012docs@microsoft.com.

Copyright

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet website references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.

© 2013 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Bing, Internet Explorer, JScript, SharePoint, Silverlight, SQL Server, Visio, Visual Basic, Visual Studio, Win32, Windows, Windows Intune, Windows PowerShell, and Windows Vista are trademarks of the Microsoft group of companies. Portions of this documentation related to network monitoring are provided by EMC, and for those portions the following copyright notice applies 2010 © EMC Corporation. All rights reserved. All other trademarks are property of their respective owners.

Revision History

Release Date	Changes
October 17, 2013	Original release of this guide.
November 1, 2013	Minor updates for this guide.

Contents

What's New in System Center 2012 for Operations Manager 22
- What's New in System Center 2012 R2 Operations Manager 22
- What's New in System Center 2012 SP1 - Operations Manager 25
- What's New in System Center 2012 - Operations Manager 32

Operator Learning Roadmap for Operations Manager 38

Operations Manager Key Concepts 41

System Requirements for System Center 2012 - Operations Manager 47
- System Requirements: System Center 2012 R2 Operations Manager 48
- System Requirements: System Center 2012 SP1 - Operations Manager 66
- System Requirements: System Center 2012 - Operations Manager 84

Upgrading System Center 2012 SP1 - Operations Manager to System Center 2012 R2 102
- Pre-Upgrade Tasks When Upgrading to System Center 2012 R2 Operations Manager 105
- How to Upgrade a Single-Server Management Group to System Center 2012 R2 Operations Manager 109
- How to Upgrade a Management Server to System Center 2012 - Operations Manager - Upgrading a Distributed Management Group 111
- How to Upgrade an ACS Collector to System Center 2012 R2 Operations Manager 113
- How to Upgrade a Gateway Server to System Center 2012 R2 Operations Manager 114
- How to Upgrade an Operations Console to System Center 2012 R2 Operations Manager ... 115
- How to Upgrade an Agent to System Center 2012 R2 Operations Manager 116
- How to Upgrade a Web Console to System Center 2012 R2 Operations Manager 120
- How to Upgrade Reporting to System Center 2012 - Operations Manager 121
- Post-Upgrade Tasks When Upgrading to System Center 2012 R2 Operations Manager 122
- How to Upgrade OM2012 SP1 Agents to OM2012 R2 Parallel Environments 124

Upgrading System Center 2012 – Operations Manager to System Center 2012 SP1 125
- Pre-Upgrade Tasks When Upgrading to System Center 2012 SP1 - Operations Manager 127
- How to Upgrade a Single-Server Management Group to System Center 2012 SP1 - Operations Manager 131
- How to Upgrade a Management Server to System Center 2012 - Operations Manager - Upgrading a Distributed Management Group 133
- How to Upgrade an ACS Collector to System Center 2012 SP1 - Operations Manager 135
- How to Upgrade a Gateway Server to System Center 2012 SP1 - Operations Manager 136
- How to Upgrade an Operations Console to System Center 2012 SP1 - Operations Manager 137
- How to Upgrade an Agent to System Center 2012 SP1 - Operations Manager 139
- How to Upgrade a Web Console to System Center 2012 - Operations Manager 142
- How to Upgrade Reporting to System Center 2012 - Operations Manager 143

Post-Upgrade Tasks When Upgrading to System Center 2012 SP1 - Operations Manager .. 144
How to Upgrade OM2007 R2 Agents to OM2012 SP1 - Parallel Environments 146

Deploying System Center 2012 - Operations Manager..... 147
Planning the System Center 2012 - Operations Manager Deployment..... 147
Considerations when Upgrading to System Center 2012 - Operations Manager 148
Considerations for a Clean Installation of System Center 2012 – Operations Manager..... 150
Considerations when Designing a Management Group for Network Monitoring 152
Considerations for Application Performance Monitoring 153
Considerations for High Availability and Disaster Recovery..... 154
Deploying System Center 2012 - Operations Manager 155
Environmental Prerequisites for Operations Manager..... 159
Supporting Infrastructure..... 160
Security Considerations 161
Agent and Agentless Monitoring 168
Single-Server Deployment of Operations Manager..... 170
Walkthrough: Installing Operations Manager on a Single Server 173
Distributed Deployment of Operations Manager 178
How to Install the First Management Server in a Management Group 182
How to Install Additional Management Servers 186
How to Install the Operations Console..... 189
How to Configure the Operations Console to Use SSL When Connecting to a Reporting Server..... 190
How to Install the Operations Manager Web Console 191
Web Console Security in Operations Manager 195
How to Use FIPS Compliant Algorithms..... 196
How to Install the Operations Manager Reporting Server..... 198
Deploying a Gateway Server..... 201
How to Deploy a Gateway Server..... 202
How to Chain Gateways 206
Authentication and Data Encryption for Windows Computers..... 207
How to Obtain a Certificate Using Windows Server 2008 Enterprise CA 212
How to Obtain a Certificate Using Windows Server 2008 Stand-Alone CA..... 216
How to Configure an HTTPS Binding for a Windows Server 2008 CA 221
Deploying ACS and ACS Reporting..... 221
How to Install Audit Collection Services (ACS)..... 223
How to Install an Audit Collection Services (ACS) Collector and Database..... 224
How to Deploy ACS on a Secondary Management Server..... 226
How to Deploy ACS Reporting..... 227
How to Deploy Audit Collection Services for UNIX/Linux 228
Using SQL Server 2012 Always On Availability Groups with System Center 2012 SP1 - Operations Manager 231
How to Upgrade from the Evaluation Version of Operations Manager 235

Installing Operations Manager by Using the Command Prompt Window 236
How to Enable High Availability for the Data Access Service 239
Using a Firewall 240
How to Configure the Operations Manager Database to Listen on a Specific TCP/IP Port 244
How to Configure the Reporting Data Warehouse to Listen on a Specific TCP/IP Port ... 246
Upgrading to System Center 2012 - Operations Manager 248
Upgrading from System Center Operations Manager 2007 R2 249
Upgrade Process Flow Diagrams 251
Upgrade Path Checklists for Operations Manager 253
Checklist: Single-Server Upgrade (Simple) 254
Checklist: Single-Server Upgrade (Complex) 256
Checklist: Distributed Upgrade (Simple) 259
Checklist: Distributed Upgrade (Complex) 262
Pre-Upgrade Tasks for Operations Manager 269
Upgrade Tasks for Operations Manager 277
Improving Upgrade Performance 279
Upgrade Helper Management Pack 280
Upgrading Hardware and Software to Meet System Requirements 283
How to Add an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade) 284
How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade) 285
How to Replace an Operations Manager 2007 R2 Gateway that Has an Unsupported Configuration (Operations Manager Upgrade) 289
How to Remove an Operations Manager 2007 R2 Gateway (Operations Manager Upgrade) 292
Upgrading SQL Server (Operations Manager Upgrade) 293
Upgrading a Single-Server Operations Manager 2007 R2 Environment 293
How to Upgrade an Operations Manager 2007 R2 Single-Server Management Group 294
Upgrading Agents in an Operations Manager 2007 R2 Single-Server Management Group 297
Upgrading a Distributed Operations Manager 2007 R2 Environment 298
How to Upgrade a Secondary Management Server from Operations Manager 2007 R2 299
How to Upgrade a Gateway Server from Operations Manager 2007 R2 300
Upgrading Operations Manager 2007 R2 Agents in a Distributed Management Group 301
How to Upgrade Agents from Operations Manager 2007 R2 302
How to Upgrade a Management Group from an Operations Manager 2007 R2 RMS .. 307
How to Upgrade a Management Group from an Operations Manager 2007 R2 Secondary Management Server 309
Upgrading or Installing Optional Features 313

How to Upgrade a Stand-Alone Operations Console from Operations Manager 2007 R2 313
How to Upgrade a Web Console from Operations Manager 2007 R2 315
How to Upgrade Reporting from Operations Manager 2007 R2 316
How to Upgrade an ACS Collector from Operations Manager 2007 R2 318
Post-Upgrade Tasks when Upgrading from Operations Manager 2007 R2 319
Upgrading to System Center 2012 - Operations Manager by Using the Command Prompt Window 327
Maintaining the System Center 2012 - Operations Manager Infrastructure 329
Backup and Disaster Recovery in Operations Manager 330
Complete and Incremental Backups in Operations Manager 330
Backup File Naming Conventions in System Center 2012 - Operations Manager 332
Back Up System Center 2012 - Operations Manager 332
Recommended Backup Schedule for System Center 2012 - Operations Manager 333
How to Back Up Custom Management Packs 334
How to Schedule Backups of System Center 2012 - Operations Manager Databases 334
Backup and Recovery Using VSS Writer 337
Disaster Recovery in System Center 2012 - Operations Manager 337
Disaster Recovery Command-line Parameters 340
How to Restore Operations Manager Databases 342
Making Changes to an Operations Manager Environment 343
Account Information for Operations Manager 344
How to Change the Credentials for the Action Account 349
How to Change Credentials for the System Center Management Configuration service and System Center Data Access service 349
How to Change IIS ReportServer Application Pool Account Password 350
How to Change the Reporting Server Execution Account Password 351
How to Change the Windows Service Account Password for the SQL Server Reporting Service 351
How to Change the Run As Account Associated with a Run As Profile 352
How to Uninstall Operations Manager 353
How to Manage the Report Server Unattended Execution Account 353
How to Configure the Internet Proxy Settings for a Management Server 354
How to Move the Operational Database 354
How to Move the Data Warehouse Database 357
How to Move the Audit Collection Database 361
How to Move the Reporting Server Role 362
How to Remove the Management Server Role 364
Removing a Gateway Server from a Management Group 367
How to Remove Certificates Imported with MOMCertImport 370
Sending Data to Microsoft 371
Customer Experience Improvement Program (CEIP) 371
Operational Data Reporting (ODR) 372

Error Reporting 374

Operations Guide for System Center 2012 - Operations Manager 376
Quick Reference to Operations Manager Tasks 377
Initial Monitoring After Operations Manager Is Installed 380
Managing Discovery and Agents 381
Operations Manager Agent Installation Methods 382
Install Agent on Windows Using the Discovery Wizard 383
Install Agent on UNIX and Linux Using the Discovery Wizard 386
Install Agent Using the MOMAgent.msi Setup Wizard 388
Install Agent Using the Command Line 390
Install Agent and Certificate on UNIX and Linux Computers Using the Command Line .. 393
Managing Certificates for UNIX and Linux Computers 397
Process Manual Agent Installations 398
Applying Overrides to Object Discoveries 401
Configuring Agents 402
Examples of Using MOMAgent Command to Manage Agents 405
Upgrading and Uninstalling Agents on UNIX and Linux Computers 406
Upgrading Agents on UNIX and Linux Computers Using the Command Line 408
Manually Uninstalling Agents from UNIX and Linux Computers 411
Uninstall Agent from Windows-based Computers 413
Using Management Packs 415
What Is in an Operations Manager Management Pack? 416
Management Packs Installed with Operations Manager 419
Management Pack Life Cycle 422
How to Import an Operations Manager Management Pack 426
How to Remove an Operations Manager Management Pack 430
Creating a Management Pack for Overrides 431
How to Export an Operations Manager Management Pack 434
How to Add Knowledge to a Management Pack 435
Tuning Monitoring by Using Targeting and Overrides 436
Using Classes and Groups for Overrides in Operations Manager 438
How to Override a Rule or Monitor 440
How to Enable or Disable a Rule or Monitor 441
Using the Enforced Attribute in Overrides 442
How to Enable Recovery and Diagnostic Tasks 443
Managing Access in Operations Manager 445
Managing Access in Operations Manager 446

Operations Manager Accounts 447

Implementing User Roles 450

Choose a Profile 452

Define a Scope Using Operations Manager Groups 455
Assign Tasks and Views 455
How to Assign Members to User Roles 456
Operations Associated with User Role Profiles 458
How to Create a New Action Account in Operations Manager 464
How to Manage the Report Server Unattended Execution Account in Operations Manager 465
Control Access by Using the Health Service Lockdown Tool in Operations Manager 466
Accessing UNIX and Linux Computers in Operations Manager 467
Credentials You Must Have to Access UNIX and Linux Computers 469
How to Set Credentials for Accessing UNIX and Linux Computers 472
How to Configure sudo Elevation and SSH Keys 478
Required Capabilities for UNIX and Linux Accounts 481
Configuring SSL Ciphers 484
Administering and Configuring the UNIX/Linux Agent 486
Managing Run As Accounts and Profiles 490
Distribution and Targeting for Run As Accounts and Profiles 492
How to Create a Run As Account 494
How to Associate a Run As Account to a Run As Profile 496
How to Create a New Run As Account for Accessing the Operations Manager Database 497
How to Configure Run As Accounts and Profiles for UNIX and Linux Access 499
Operations Manager Monitoring Scenarios 501
Agentless Monitoring in Operations Manager 502
How to Configure a Computer for Agentless Management 504
How to Configure a Proxy for Agentless Monitoring 507
Monitoring Across Untrusted Boundaries in Operations Manager 508
About Gateway Servers in Operations Manager 509

Determining the Health of Gateway Servers 510
Using Multiple Gateway Servers 511
How to Configure Agent Failover to Multiple Gateway Servers 512
How to Configure a Gateway Server to Failover Between Multiple Management Servers 513
Certificate Renewal for Gateway Servers and Management Servers 514
Client Monitoring Using Agentless Exception Monitoring in Operations Manager 515
How to Configure a Management Server for Client Monitoring 516
How to Configure Clients for Client Monitoring 519
How to Customize Client Monitoring Data Collection and Solution Response URLs for Error Groups 520
How to Configure Error Transmission Settings for Client Monitoring in Operations Manager 521
Forwarding Client Error Reports (Client Monitoring) 523
Monitoring Clusters by Using Operations Manager 524
Monitoring Networks by Using Operations Manager 525
How to Discover Network Devices in Operations Manager 529
Network Device Discovery Settings 537
Run As Accounts for Network Monitoring in Operations Manager 542
How to Delete or Restore a Network Device in Operations Manager 544
Tuning Network Monitoring 545
Viewing Network Devices and Data in Operations Manager 566
Security for Servers Performing Network Discovery 570
Network Devices Supported for Discovery by Operations Manager 570
Reports for Network Monitoring in Operations Manager 571
Monitoring Service Level Objectives by Using Operations Manager 573
Defining a Service Level Objective Against an Application 574
Defining a Service Level Objective Against a Group 576
Running a Service Level Tracking Report 577

Creating a Service Level Dashboard 578
Monitoring .NET Applications 580
Viewing and Investigating Alerts for .NET Applications (Server-side Perspective) 581
Working with the Application Diagnostics Console 591
Working with Events by Using Application Diagnostics 596
Prioritizing Alerts by Using Application Advisor 601
User Roles for Application Performance Monitoring 604
How to Configure Grooming Settings for .NET Application Performance Monitoring Events 605
Working with Sensitive Data for .NET Applications 610
Notes for AVIcode 5.7 Customers 612
Monitoring Java Applications 614
How to Configure Monitoring for Java Applications 615
How to Monitor Java Applications 619
Strategies for Monitoring a New Java Application 621
Fabric Monitoring 622
Getting Started with the Fabric Health Dashboard 624
Scoping the Fabric Health Dashboard to a Specific Cloud and Investigating Details 626
The Fabric Monitoring Diagram View: Displaying Health States of Cloud Environments 627
Using System Center Advisor to Proactively Monitor Cloud Fabric 628
Monitoring UNIX and Linux Computers by Using Operations Manager 629
Supported UNIX and Linux Operating System Versions 630
Using Templates for Additional Monitoring of UNIX and Linux 638
Troubleshooting UNIX and Linux Monitoring 638
Certificate Issues 639
Management Pack Issues 641
Operating System Issues 643

Logging and Debugging 645
Monitoring Linux Computers in Windows Azure by Using Operations Manager 647
Collecting Security Events Using Audit Collection Services in Operations Manager 652
Audit Collection Services Security 656
Audit Collection Services Capacity Planning 658
Audit Collection Services Performance Counters 663
How to Enable Audit Collection Services (ACS) Forwarders 666
How to Enable Event Logging and ACS Rules on Solaris and AIX Computers 667
How to Filter ACS Events for UNIX and Linux Computers 669
How to Configure Certficates for ACS Collector and Forwarder 670
Monitoring Audit Collection Services Performance 673
How to Remove Audit Collection Services (ACS) 676
Audit Collection Services Administration (AdtAdmin.exe) 678
AdtAdmin.exe /AddGroup 681
AdtAdmin.exe /DelGroup 682
AdtAdmin.exe /Disconnect 683
AdtAdmin.exe /GetDBAuth 685
AdtAdmin.exe /GetQuery 686
AdtAdmin.exe /ListForwarders 687
AdtAdmin.exe /ListGroups 689
AdtAdmin.exe /SetDBAuth 690
AdtAdmin.exe /SetQuery 692
AdtAdmin.exe /Stats 693
AdtAdmin.exe /UpdForwarder 696
AdtAdmin.exe /UpdGroup 698
Connecting Operations Manager With Other Management Systems 699

How to Configure a Product Connector Subscription 701
Monitoring Operations Manager from a Second Management Group 702
Integrating Active Directory and Operations Manager 703
Using Active Directory Domain Services to Assign Computers to Operations Manager Management Groups 704
How to Create an Active Directory Domain Services Container for a Management Group 705
How to Use Active Directory Domain Services to Assign Computers to Management Servers . 707
Changing the Active Directory Integration Setting for an Agent 709
Getting Information from Operations Manager 710
Using the Operations Manager Consoles 711
Comparing the Operations Console and Web Console in Operations Manager 712
How to Connect to the Operations Console 713
How to Connect to the Web Console 715
Using the Monitoring Workspace in Operations Manager 716
Using Health Explorer in Operations Manager 717
Using My Workspace in Operations Manager 719
Using the Administration Workspace in Operations Manager 722
Using the Reporting Workspace in Operations Manager 728
Using the Authoring Workspace in Operations Manager 729
Finding Data and Objects in the Operations Manager Consoles 732
Using Advanced Search 736
Examples of Using Advanced Search in Operations Manager 739
Using Views in Operations Manager 740
View Types in Operations Manager 741
Standard Views in Operations Manager 748
Creating Views in Operations Manager 753
How to Personalize a View in Operations Manager 763

Guidance for Scoping and Targeting Views 764
Using SharePoint to View Operations Manager Data 765
Subscribing to Alert Notifications 773
How to Create and Configure the Notification Action Account 774
How to Enable an Email Notification Channel 775
How to Enable an Instant Message Notification Channel 777
How to Enable a Text Message (SMS) Notification Channel 778
How to Enable a Command Notification Channel 780
How to Create Notification Subscribers 781
How to Create Notification Subscriptions 783
How to Customize Message Content for Notifications 785
How to Subscribe to Notifications from an Alert 788
How to Create Subscriptions Using Classes and Groups 789
How to Specify Which Alerts Generate Notifications (Conditions) 791
Sending Notifications for Specific Computers and Specific Alerts to Specific Teams 793
Using Reports in Operations Manager 794
Operations Manager Reports Library 794
How to Create Reports in Operations Manager 801
How to Create an Alert Logging Latency Report 802
How to Create an Alerts Report 803
How to Create an Availability Report 803
How to Create a Configuration Changes Report 804
How to Create an Event Analysis Report 805
How to Create an Operational Data Report 806
How to Save a Report 807
How to Run a Report 808

Scheduling Reports 809
How to Create a Report Schedule 810
How to Email Scheduled Reports 811
How to Schedule the Delivery of a Report to the SQL Report Server Cache 812
How to Cancel a Scheduled Report 813
How to Edit a Scheduled Report 814
How to Export a Report 815
How to Troubleshoot Reports that Return No Data 815
Not Monitored and Gray Agents 818
How to View All Rules and Monitors Running on an Agent-Managed Computer 820
Using the Visio 2010 Add-in and SharePoint 2010 Visio Services Data Provider 821
Install the Visio 2010 Add-in 822
Install the Visio Services Data Provider 823
Grant Visio Services with Read-Only Operator Permissions 824
Configure the Operations Manager Data Source in Visio 2010 825
View an Operations Manager Distributed Application Diagram in Visio 2010 826
Add Links to Operations Manager to a New or Existing Visio 2010 Document 827
Build a simple monitoring dashboard using the Visio Web Part 829
Publish a Visio diagram to SharePoint 2010 830
Change the Way Health State is Represented in Visio 2010 831
Troubleshooting the Visio 2010 Add-in 831
General Tasks in Operations Manager 834
Managing Alerts 835
How Heartbeats Work in Operations Manager 836
Resolving Heartbeat Alerts 838
How an Alert is Produced 840

Viewing Active Alerts 842
Viewing Alert Details 844
Examining Properties of Alerts, Rules, and Monitors 846
Impact of Closing an Alert 849
How to Close an Alert Generated by a Monitor 851
How to Reset Health 852
Identifying the Computer Experiencing a Problem 853
Using Health Explorer to Investigate Problems 856
Using Event View to Investigate Problems 859
Investigating Alert Storms 861
How to Set Alert Resolution States 862
How to Configure Automatic Alert Resolution 864
Diagnostic and Recovery Tasks 865
How to Suspend Monitoring Temporarily by Using Maintenance Mode 867
Creating and Managing Groups 869
Running Tasks in Operations Manager 871
How to Create a Resource Pool 875
Managing Resource Pools for UNIX and Linux Computers 877
Connecting Management Groups in Operations Manager 879
Using Operations Manager Shell 882
Maintenance of Operations Manager 883
Integrating Operations Manager with Development Processes 883
Integrating Operations Manager with Development Processes in System Center 2012 R2 884
How to Configure Integration with TFS in System Center 2012 R2 885
How to Change the Frequency of Synchronization for Integration with TFS in System Center 2012 R2 892
How to Manually Import an Operational Issue WITD to TFS in System Center 2012 R2 894

How to Configure Whether Files Are Attached or Linked in Synchronization with TFS in System Center 2012 R2 895

How to Configure Notifications when Developers Reassign Work Items to IT Operations in System Center 2012 R2 897

How to Automatically Assign New Alerts to Engineering in System Center 2012 R2 898

How to Automatically Close Alerts When Work Items Are Resolved in TFS in System Center 2012 R2 900

How to Stop and Resume Synchronization with TFS in System Center 2012 R2 901

How to Configure File Attachments for Operations Manager Alerts in System Center 2012 R2 903

How to Collect IntelliTrace Historical Profiling Traces from System Center 2012 R2 906

How to Configure Integration with IntelliTrace Historical Profiling in System Center 2012 R2 ... 909

How to Synchronize Alerts with TFS in System Center 2012 R2 911

Monitoring Integration between Operations Manager and TFS in System Center 2012 R2 912

Integrating Operations Manager with Development Processes in System Center 2012 SP1 915

How to Configure Integration with TFS in System Center 2012 SP1 916

How to Change the Frequency of Synchronization for Integration with TFS in System Center 2012 SP1 922

How to Manually Import an Operational Issue WITD to TFS in System Center 2012 SP1 925

How to Configure Whether Files Are Attached or Linked in Synchronization with TFS in System Center 2012 SP1 926

How to Configure Notifications when Developers Reassign Work Items to IT Operations in System Center 2012 SP1 927

How to Automatically Assign New Alerts to Engineering in System Center 2012 SP1 928

How to Automatically Close Alerts When Work Items Are Resolved in TFS in System Center 2012 SP1 931

How to Stop and Resume Synchronization with TFS in System Center 2012 SP1 932

How to Configure File Attachments for Operations Manager Alerts in System Center 2012 SP1 934

How to Collect IntelliTrace Historical Profiling Traces from System Center 2012 SP1 936

How to Configure Integration with IntelliTrace Historical Profiling in System Center 2012 SP1 . 940
How to Synchronize Alerts with TFS in System Center 2012 SP1 941
Monitoring Integration between Operations Manager and TFS in System Center 2012 SP1..... 942
Monitoring with Microsoft Monitoring Agent 944
Installing Microsoft Monitoring Agent 945
Monitoring Web Applications with Microsoft Monitoring Agent 947
Comparing Monitoring Approaches for .NET Applications 949
Microsoft Monitoring Agent Compatibility 952
Index to Security-Related Information for System Center 2012 - Operations Manager..... 954
Authoring for System Center 2012 - Operations Manager 957
Key Concepts for Authors..... 958
What is an Author? 959
Authoring Tools..... 960
Structure of a Management Pack 963
Sealed Management Pack Files..... 966
How to Seal a Management Pack File 968
Selecting a Management Pack File 971
Targets and Objects 973
Understanding Classes and Objects 974
Selecting a target..... 978
Creating a new target 983
Attributes..... 986
Management Pack Templates..... 990
Creating Management Pack Templates 991
Watcher Nodes..... 992
.NET Application Performance Monitoring Template 993

Before You Begin Monitoring .NET Applications 1045
How to Configure Monitoring for .NET Applications 1048
How to Add, Enable, and Disable Namespaces 1056
How to Add, Edit, and Remove Methods 1062
How to Add, Edit, and Remove Exception Tracking 1064
Using Exception Handlers to Define Critical Exceptions 1066
Client-Side Monitoring with Targeted Groups and Load Balancers 1069
How to Configure IP Address Exclusion Filters for Client-Side Monitoring 1070
How to Start Monitoring a New Application 1071
Authoring Strategies for .NET Application Monitoring 1074
Application Monitoring Using the Default Settings 1078
Monitoring SharePoint 2010 Applications in System Center 2012 SP1 1079
Appendix for .NET Application Monitoring 1080
Default Entry Points for .NET Application Monitoring 1080
Default Methods for .NET Application Monitoring 1082
OLE DB Data Source Template 1105
Process Monitoring Template 1112
TCP Port Template 1120
UNIX or Linux Log File 1124
UNIX or Linux Process 1127
Web Application Availability Monitoring Template 1132
How to Configure Web Application Availability Monitoring 1153
Monitoring Web Application Availability Tests and Alerts 1157
Dashboard Views for Web Application Availability Monitoring 1158
Reporting for Web Application Availability Monitoring 1161
Web Application Transaction Monitoring Template 1162

How to Create a Single URL Web Application Monitor 1163
How to Capture Web Application Recording 1165
Troubleshooting Web Capture 1166
How to Edit Settings or Requests in a Web Application 1167
Web Application Properties 1168
Web Application Request Properties 1171
How to Replace Parameters in a URL Request 1175
Windows Service Template 1182
Monitors and Rules 1187
Data Sources 1192
Expressions 1193
Alerts 1198
Event Monitors and Rules 1203
Windows Events 1204
Text Logs 1210
WMI Events 1215
Syslog Events 1221
SNMP Events 1226
Event Monitor Logic 1234
Repeating Events 1235
Correlated Events 1240
Missing Events 1242
Correlated Missing Events 1243
Event Monitor Reset 1244
UNIX/Linux Shell Command Alerts 1246
Performance Monitors and Rules 1250

Performance Monitors 1251
Windows Performance Collection Rules 1255
WMI Performance 1259
UNIX/Linux Shell Command Performance Collection Rules 1262
Script Monitors and Rules 1267
Script Collection Rules 1271
Script Monitors 1278
UNIX/Linux Shell Command Monitors 1284
Dependency Monitors 1290
Aggregate Monitors 1294
Diagnostics and Recoveries 1297
Tasks 1303
Console Tasks 1303
Agent Tasks 1308
Distributed Applications 1315
360 .NET Application Monitoring Dashboards in System Center 2012 SP1 1319
Before You Begin Using 360 .NET Application Monitoring Dashboards in System Center 2012 SP1 1322
How to Configure 360 .NET Application Monitoring Dashboards in System Center 2012 SP1 1323
How to Use the 360 .NET Application Monitoring Dashboards in System Center 2012 SP1 ... 1326
Report Authoring for System Center 2012 - Operations Manager 1327
Cmdlets in System Center 2012 - Operations Manager 1327
Operations Manager Cmdlet Reference 1328
Operations Manager Cmdlet About Help Topics 1328
about_OpsMgr_Cmdlet_Names 1329
about_OpsMgr_Connections 1335
about_OpsMgr_RunAsAccount 1337

about_OpsMgr_WhatsNew 1340
Operations Manager Cmdlets for UNIX and Linux 1345
Glossary for System Center 2012 - Operations Manager 1345
Privacy Statement for System Center 2012 - Operations Manager 1350
Release Notes for System Center 2012 - Operations Manager 1362
Release Notes for Operations Manager in System Center 2012 R2 1362
Release Notes for Operations Manager in System Center 2012 SP1 1365
Release Notes for System Center 2012 - Operations Manager 1369

What's New in System Center 2012 for Operations Manager

System Center 2012 – Operations Manager, System Center 2012 Service Pack 1 (SP1) – Operations Manager, and System Center 2012 R2 Operations Manager have a number of new capabilities and changes outlined in this document. Each version of Operations Manager has its own section covering what is new.

What's New

- What's New in System Center 2012 R2 Operations Manager
- What's New in System Center 2012 SP1 - Operations Manager
- What's New in System Center 2012 - Operations Manager

What's New in System Center 2012 R2 Operations Manager

System Center 2012 R2 Operations Manager has new capabilities and changes, which are outlined here. For details about known issues, read the Release Notes for Operations Manager in System Center 2012 R2

Fabric Monitoring

A close integration between System Center 2012 R2 Virtual Machine Manager and System Center 2012 R2 Operations Manager introduces System Center cloud monitoring of virtual layers for private cloud environments. To get this new functionality, use the System Center 2012 Management Pack for System Center 2012 R2 Virtual Machine Manager Dashboard, which is imported automatically when you integrate Operations Manager and Virtual Machine Manager. For information about how to integrate Operations Manager and Virtual Machine Manager, see Configuring Operations Manager Integration with VMM.

Fabric Health Dashboard – Monitoring the Health of Private Clouds

The Fabric Health Dashboard shows a detailed overview of the health of your private clouds and the fabric that services those clouds. The dashboard helps you answer questions like “What is the health of my clouds and the fabric serving those clouds?”

To view the Fabric Health Dashboard, click **Monitoring**, and in **Cloud Health Dashboard**, click **Cloud Health**. Select the cloud you want to investigate, and then, in the **Tasks** pane, click **Fabric Health Dashboard**.

For each cloud, the Fabric Health Dashboard displays these aspects of the fabric:

- **Host State:** monitors the health state of the hosting groups or the computing aspects of the cloud, such as CPU, memory, disks, and network adapters
- **Storage Pools State File Share and LUN State:** monitors the health state of the storage aspect of fabric for issues, such as disk space capacity and allocation
- **Network Node State:** utilizes network monitoring in Operations Manager and displays the health state of network nodes (devices) that are relevant for the cloud you selected. Only physical network devices within one hop from the hosts are shown. To see the physical network devices, you must enable the Network Monitoring feature of Operations Manager and monitor the physical network devices connected to the hosts. Virtual networks are not shown in the dashboard.

The **Active Alerts** and **Number of VMs** fields on this dashboard help indicate which issues are having the greatest impact on your cloud and can help you prioritize your work.

Fabric Monitoring Diagram View – Displays Health States of Cloud and On-Premise Environments

The Diagram view gives you a diagram of the entire infrastructure and shows the health state of each part of the fabric. The Diagram view helps you answer questions, such as “What is the health of my entire fabric?” Improvements to the diagram ensure that health rolls up and that the relevant fabric components are part of the Diagram View.

To Open Diagram View, click **Monitoring**, and in **Microsoft System Center Virtual Machine Manager Views**, click **Diagram View** for the environment you want to see displayed as a diagram.

Microsoft Monitoring Agent

Microsoft Monitoring Agent is a new agent that replaces the Operations Manager Agent and combines .NET Application Performance Monitoring (APM) in System Center with the full functionality of Visual Studio IntelliTrace Collector for gathering full application profiling traces. Microsoft Monitoring Agent can collect traces on demand or can be left running, which monitors applications and collects traces continuously.

Microsoft Monitoring Agent can be used together with Operations Manager or can be used as a standalone tool for monitoring web applications written with Microsoft .NET Framework. In both cases, the operator can direct the agent to save application traces in an IntelliTrace log format that can be opened in Visual Studio Ultimate. The log contains detailed information about application failures and performance issues.

You can use Windows PowerShell commands to start and stop monitoring and collect IntelliTrace logs from web applications that are running on Internet Information Services (IIS). To open IntelliTrace logs generated from APM exceptions and APM performance events, you can use Visual Studio. For more information, see Monitoring with Microsoft Monitoring Agent.

Integrating Operations Manager with Development Processes (DevOps)

Here are two important changes to the DevOps functionality in System Center 2012 R2 Operations Manager:

New Alert Fields of TFS Work Item ID and TFS Work Item Owner

In System Center 2012 R2 Operations Manager, you can synchronize Operations Manager alerts and Team Foundation Server (TFS) work items. When synchronization is enabled, IT operations can then assign alerts to the engineering team. Assigning an alert to engineering creates a new work item in TFS. The workflow will track and synchronize any changes that are made to TFS work items and any associated Operations Manager alerts.

Integration between System Center 2012 Service Pack 1 (SP1) and TFS used the Ticket ID and Owner fields of the Operations Manager alert to store and display which work item is associated with an alert and who it is assigned to. Beginning in System Center 2012 R2 Operations Manager, two new alert fields, TFS Work Item ID and TFS Work Item Owner, hold these values. These fields are read-only in the Operations Manager console to prevent accidental changes of the values that are controlled in TFS.

If you previously personalized any standard alert views or created your own alert views in System Center 2012 SP1 using Ticket ID and Owner fields to display TFS information, you must replace those fields with the TFS Work Item ID and TFS Work Item Owner fields to continue displaying the same information. The previous Ticket ID and Owner fields are still used for synchronization of alerts with incidents in Service Manager Alert Connector.

Note

You can now use Operations Manager integration with TFS in the same environment with the Service Manager Alert Connector.

Conversion of Application Performance Monitoring (APM) Performance Events to IntelliTrace format

This monitoring capability now allows the opening of APM performance events from Visual Studio IDE as if the performance event was captured during the IntelliTrace historical debugging session. Tightly integrated with TFS Work Item Synchronization Management Pack, this capability instantaneously brings generated IntelliTrace logs to TFS work items assigned to engineering. This can result in streamlining communications between IT Operations and Development and enriching the development experience with analysis of root causes of the application failure, reducing the mean time to recovery (MTTR) for the problems detected by APM.

Support for IPv6

In System Center 2012 R2 Operations Manager the Operations console can take IPv6 addresses as input for Network Discovery and display IPv6 addresses in the network-related views.

Java Application Performance Monitoring

The System Center 2012 Management Pack for Java Application Performance Monitoring lets you monitor Java application performance and exception events by using Operations Manager Application Advisor. You can set method and resource timing for performance events, stack traces for exception events, and set Java specific counters (such as Average Request Time and Requests Per Second) for events. Additionally, you get Operations Manager level alerting on Java application server counters. You can download the management pack from the Microsoft Download Center.

System Center Advisor

System Center Advisor is an online service that analyzes installations of Microsoft server software. With the latest preview version of Advisor, you can now view Advisor alerts in the Operations Manager Operations console.

Advisor collects data from your installations, analyzes it, and generates alerts that identify potential issues (such as missing security patches) or deviations from identified best practices with regard to configuration and usage. Advisor also provides both current and historical views of the configuration of servers in your environment. Ultimately, Advisor recommendations help you proactively avoid configuration problems, reduce downtime, improve performance, and resolve issues faster. For more information about Advisor, see Viewing System Center Advisor Alerts and Advisor online help

UNIX and Linux Monitoring

UNIX and Linux agents for Operations Manager are now based on the Open Management Infrastructure (OMI) open-source CIM Object Manager.

Debian GNU/Linux 7 is now supported by the Universal Linux agents and Management Packs.

What's New in System Center 2012 SP1 - Operations Manager

System Center 2012 Service Pack 1 (SP1), Operations Manager has a number of new capabilities and changes outlines in this document. We urge you to read the Release Notes for Operations Manager in System Center 2012 SP1 for details about known issues.

New capabilities include improvements to .NET Application Performance Monitoring (APM), Audit Collection Service (ACS), and UNIX and Linux monitoring.

New Monitoring Capabilities

Monitoring Windows Services Built on the .NET Framework

One of the most commonly requested features that was present in AVIcode, but not yet re-implemented in System Center 2012 – Operations Manager was the ability to monitor Windows

Services, not just IIS-hosted applications. This is now possible again, and integrated into the APM template.

Automatic Discovery of ASP.NET MVC3 and MVC4 Applications

If the application contains “System.Web.Mvc.dll” in the /bin subfolder, it is now automatically discovered as an ASP.NET Web Application without the need to use the overrides that were documented in the APM.WEB.IIS7.mp Guide. For more information, see Configuring the Management Pack for Operations Manager APM Web IIS 7.

New Transaction Types: MVC Pages and WCF Methods

New transaction types have been introduced for MVC pages and for MVC methods. This augments the capability to specify more detailed settings for a given feature of your application. How to use this feature is documented in the APM template documentation.

Comparing Transaction Monitoring

Here is a comparison of the transactions you can monitor using System Center 2012 – Operations Manager and those you can monitor using the Operations Manager Beta version of System Center 2012 Service Pack 1 (SP1).

Component type	**Transactions you can monitor using System Center 2012 – Operations Manager**	**Transactions you can monitor using The Operations Manager Beta version of System Center 2012 Service Pack 1 (SP1)**
ASP.NET web application	• ASP.NET webpage • ASP.NET web service • Function	• ASP.NET webpage • ASP.NET MVC page • ASP.NET web service • WCF method • Function
ASP.NET web service	• ASP.NET webpage • ASP.NET web service • Function	• ASP.NET webpage • ASP.NET MVC page • ASP.NET web service • WCF method • Function
WCF service	No transactions allowed	• ASP.NET webpage • ASP.NET MVC page • ASP.NET web service • WCF method • Function

Component type	Transactions you can monitor using System Center 2012 – Operations Manager	Transactions you can monitor using The Operations Manager Beta version of System Center 2012 Service Pack 1 (SP1)
Windows Service	Component type did not exist	• WCF method • Function

Enabled APM of SharePoint 2010

Operations Manager lets you monitor SharePoint web front-end components. You can monitor standard and custom SharePoint webpages for performance degradation and server-side exceptions. You can set up monitoring for SharePoint applications in much the same way you enable monitoring for other .NET web applications. Use the .NET Application Performance Monitoring template to configure SharePoint application monitoring. When monitoring SharePoint applications for exceptions, the exception call stack contains the relevant SharePoint specific parameters for troubleshooting.

Integration with Team Foundation Server 2010 and Team Foundation Server 2012

To speed interactions between operations and development, it is essential to quickly detect and fix problems that might need assistance from the engineering team. System Center 2012 Service Pack 1 (SP1), Operations Manager can integrate with development tools, such as Team Foundation Server (TFS) and Visual Studio, enabling deep troubleshooting and streamlining communications between developers and IT operations. You can synchronize Operations Manager alerts and Team Foundation Server (TFS) work items. Operations Manager integration with TFS introduces a new work item type definition, Operational Issue, which can be embedded into any of your organization's engineering processes. After enabling synchronization, IT operations can manually assign alerts to the engineering team. Assigning an alert to engineering creates a new work item in Team Foundation Server. The workflow tracks and synchronizes changes made to TFS work items and changes made to associated alerts in Operations Manager.

Compared to the Microsoft Visual Studio Team Foundation Server 2010 Work Item Synchronization management pack, SP1 features include:

- Shipped as part of Operations Manager, included in the SP1 Media
- Improved security – synchronization account no longer requires TFS administrative rights
- Improved design of the Operational Issue WITD
- Improved design of the configuration Wizard
- Introduced support for TFS Area Path
- Support for default Team Projects

- Synchronization for new APM alert types from IIS8 web applications, WCF, Windows Services, and also for non-APM alerts
- Localization of Wizard UI and MP elements, and compatibility with localized versions of TFS
- Synchronize file attachments that can reside on a network file share or appended to TFS work items.
- Automatically route and close alerts to TFS
- IT operations can open TFS work items directly from the Operations Manager console using built-in integration with TFS web UI.

Conversion of Application Performance Monitoring events to IntelliTrace format

This new monitoring capability allows for opening of APM exception events from Visual Studio IDE as if the exception was captured during the IntelliTrace historical debugging session. Developers can stay within their familiar environment to examine complete exception call stack, for example: method parameters captured at the time of exception, and can navigate between the source code modules that participated in the exception call chain. Tightly integrated with TFS Work Item Synchronization Management Pack, this capability instantaneously brings generated IntelliTrace logs to TFS work items assigned to engineering. This can result in streamlining communications between IT Operations and Development and enriching the development experience with analysis of root causes of the application failure, reducing the mean time to recovery (MTTR) for the problems detected by APM.

Features include:

- APM exception events can be saved in IntelliTrace file format directly from Application Diagnostics
- Debug Symbols can be late-bound in Visual Studio 2012 allowing developers to navigate through source code, even when the production environment has no symbols loaded
- Developers can see one level of parameters that are converted and visible in the Visual Studio 2012 Ultimate **Locals** window, and displayed in the context of the selected call stack frame
- Developers can see additional method specific information (i.e. a connection string for ExecuteReader() method) in the Visual Studio 2012 **Locals** window in the context of the selected call stack frame
- Traces are automatically attached to APM exception events and can be automatically added to TFS work items or stored on a network file share. Developers can open traces using Visual Studio 2012 Ultimate and troubleshoot application problems while staying in their development environment.

Collecting Historical Traces Using IntelliTrace Profiling Management Pack

System Center 2012 SP1 – Operations Manager includes IntelliTrace Profiling Management Pack. This management pack lets you capturing historical traces directly from the Operations

Manager console. These traces can help developers investigate problems by giving them visibility to application execution history without the developers needing access to the servers where the applications ran. Developers can use Visual Studio 2012 Ultimate to open collected traces.

IntelliTrace Profiling Management Pack automatically deploys the necessary infrastructure, IntelliTrace Collector, to the designated servers. When traces are collected, they are uploaded to a network file share and attached to Operations Manager alerts. Traces are uploaded to the management server using the same secure Operations Manager channel that agents use to communicate with the management servers. By configuring Team Foundation Server (TFS) synchronization, traces can be automatically added or linked to TFS work items.

New Management Packs and Support for Windows Server 2012 and IIS 8

To use APM with Windows Server 2012, you must import the following management packs:

- Microsoft.Windows.Server.Library version 6.0.6989.0 or newer
- Microsoft.Windows.Server.2012.Discovery version 6.0.6989.0 or newer
- Microsoft.Windows.InternetInformationServices.CommonLibrary version 7.0.8862.0 or newer
- Microsoft.Windows.InternetInformationServices.2012 version 7.0.8862.0 or newer

Important

If you had previously imported the Microsoft.Windows.InternetInformationServices.6.2 management pack, which was part of the Windows 8 Beta management pack release, it should be removed first.

Also, from the /ManagementPacks folder of the System Center 2012 – Operations Manager media, you should import Microsoft.SystemCenter.Apm.Web.IIS8. This is the equivalent of the Microsoft.SystemCenter.Apm.Web.IIS7 management pack, which was previously (and still is) used for IIS7.

These management pack versions to be used are specific to System Center 2012 Service Pack 1 (SP1) - Operations Manager. Other than these specific prerequisites, how to use this feature is documented in the APM template documentation and the experience is identical to configuring APM for an IIS7-hosted application.

360 .NET Application Monitoring Dashboards

System Center 2012 Service Pack 1 (SP1) - Operations Manager can show you different perspectives of application health in one place—360 .NET Application Monitoring Dashboards. The 360 .NET Application Monitoring Dashboards display information from Global Service Monitor, .NET Application Performance Monitoring, and Web Application Availability Monitoring to provide a summary of health and key metrics for 3-tier applications in a single view. The 360 .NET Application Monitoring Dashboards show where an application is unhealthy and provide a launch point for detail dashboards that highlight component-level issues.

The 360 .NET Application Monitoring Dashboards display data from powerful monitoring tools. .NET Application Performance Monitoring looks deep into the application to get details that can

help you pinpoint solutions from server-side and client-side perspectives. Web Application Availability monitoring in Operations Manager monitors internal synthetic transactions. Global Service Monitor monitors the availability of applications from an outside location, measuring availability from where the user is.

The 360 .NET Application Monitoring Dashboards show the following:

Key application metric or action	Type of monitoring used
Availability	Web Application Availability Monitoring and Global Service Monitor
Reliability	.NET Application Performance Monitoring
Performance	.NET Application Performance Monitoring and Global Service Monitor
Diagnostics	.NET Application Performance Monitoring
Resolution	The Team Foundation Server (TFS) Connector management pack takes an alert, assigns it to development in TFS with all appropriate detail.

ACS support for Dynamic Access Control

Windows Server 2012 enables business data owners to easily classify and label data allowing access policies to be defined for data classes that are critical to business. Compliance management in Windows Server 2012 becomes more efficient and flexible because access and audit policies can be based not only on user and group information but a richer set of user, resource and environmental claims, and properties from Active Directory and other sources. User claims such as roles, projects, organization, resource properties such as secrecy, and device claims such as health can be used in defining access and audit policies.

Windows Server 2012 enhances the existing Windows ACL model to support Dynamic Access Control where customers can define an expression based authorization access policy that includes conditions using user and machine claims, as well as resource (for example, file) properties. The following illustration is descriptive, and not an actual representation of an expression:

- Allow Read and Write access if User.Clearance >= Resource.Secrecy and Device. Healthy
- Allow Read and Write access if User.Project any_of Resource.Project

System Center 2012 Service Pack 1 (SP1) contributes to the fulfilling these scenarios by providing enterprise-wide visibility into the use of the Dynamic Access Control, leveraging Operations Manager's Audit Collection Services to collect events from the relevant machines (file servers, domain controllers) and providing reporting to enable auditors and compliance officers to report on the use of Dynamic Access Control – for example, audit changes in policies, object

access (success and failure), and “what-if” assessment of what would happen if a certain policy were applied.

Additional UNIX and Linux Monitoring Capabilities

Support for CentOS, Debian, Oracle, and Ubuntu Linux

System Center 2012 Service Pack 1 (SP1) - Operations Manager has added support for monitoring of the following Linux operating systems:

- CentOS 5 (x86/x64)
- CentOS 6 (x86/x64)
- Debian GNU/Linux 5 (x86/x64)
- Debian GNU/Linux 6 (x86/x64)
- Oracle Linux 5 (x86/x64)
- Oracle Linux 6 (x86/x64)
- Ubuntu Server 10.04 (x86/x64)
- Ubuntu Server 12.04 (x86/x64)

Support for these operating systems is implemented with the “Universal Linux” monitoring packs. Import the following MP files to enable monitoring of the new Linux operating systems:

- Microsoft.Linux.Universal.Library.mp
- Microsoft.Linux.Universal.Monitoring.mp
- Microsoft.Linux.UniversalD.1.mpb (to support Debian and Ubuntu Linux agents)
- Microsoft.Linux.UniversalR.1.mpb (to support CentOS Linux agents)

Improved Heartbeat Monitoring

Heartbeat monitors for Operations Manager UNIX and Linux agents now support configurable “MissedHeartbeats” – allowing for a defined number of failed heartbeats to occur before generating an alert. Failed heartbeats will now cause Operations Manager to unload rules and monitors for UNIX and Linux agents until the heartbeat is restored. This makes it very easy to identify UNIX and Linux computers with failed heartbeats in the Operations Manager console.

See Also

.NET Application Performance Monitoring Template

Before You Begin Monitoring .NET Applications

What's New in System Center 2012 - Operations Manager

System Center 2012 – Operations Manager has a number of new capabilities and changes outlines in this document. We urge you to read the System Center 2012 – Operations Manager Release Candidate Release Notes for details about known issues.

Setup and Upgrade

Setup

Operations Manager has a new Setup wizard. For important instructions about how to install Operations Manager, see the Deployment Guide for System Center 2012 – Operations Manager.

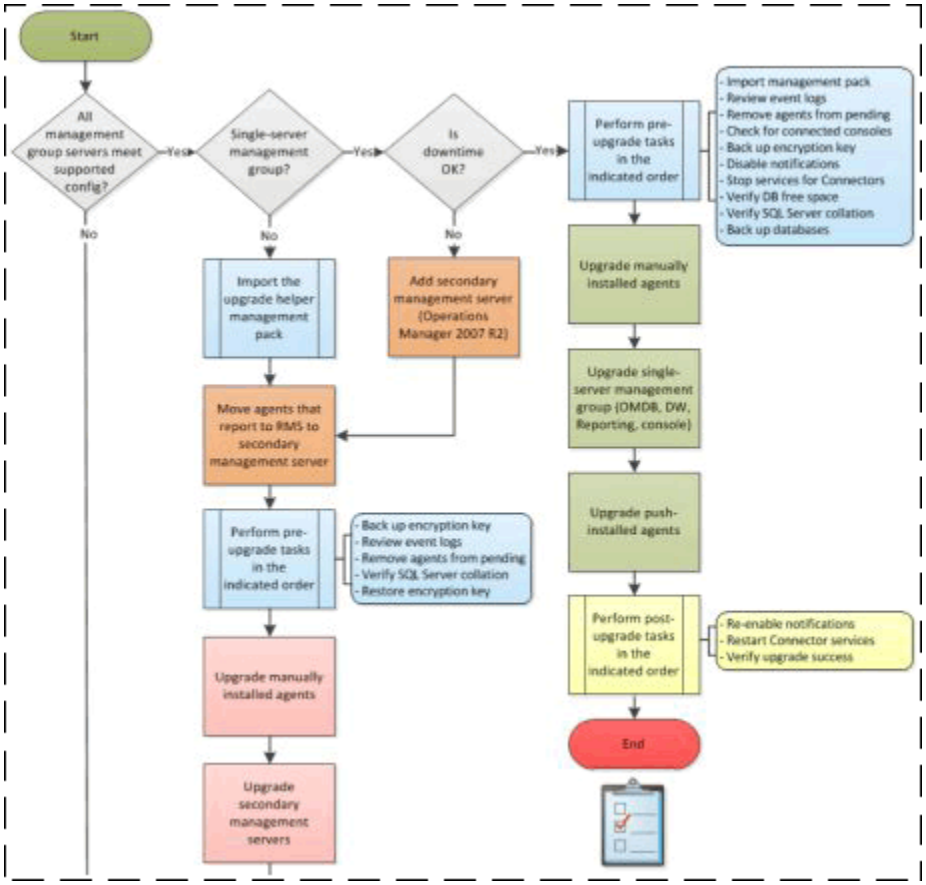
Upgrading to System Center 2012 – Operations Manager

Operations Manager provides an upgrade wizard to help you upgrade your System Center Operations Manager 2007 R2 environment to System Center 2012 – Operations Manager Release Candidate. For more information, see Upgrading to System Center 2012 – Operations Manager.

New process flow diagrams help you determine your upgrade path from System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager Release Candidate and map your upgrade process. To open and view content for any step in the process, just click a process box.

Upgrade process flow diagram

Upgrade process flow diagram



The following table lists the process flow diagrams and descriptions of when each upgrade path should be used.

Condition	Process flow diagram
When you have a single-server or distributed management group that already meets the minimum supported configuration requirements for System Center 2012 – Operations Manager.	Single-Server and Distributed Upgrade (Simple) Process Flow Diagram
When your single-server management group does not yet meet the minimum supported configuration requirements for System Center 2012 – Operations Manager, and requires new hardware.	Single-Server Upgrade (Complex) Process Flow Diagram
When your distributed management group has one or more servers that do not meet the minimum supported configuration requirements	Distributed Upgrade (Complex) Process Flow Diagram

Condition	Process flow diagram
for System Center 2012 – Operations Manager, and might require new hardware.	

New Monitoring Capabilities

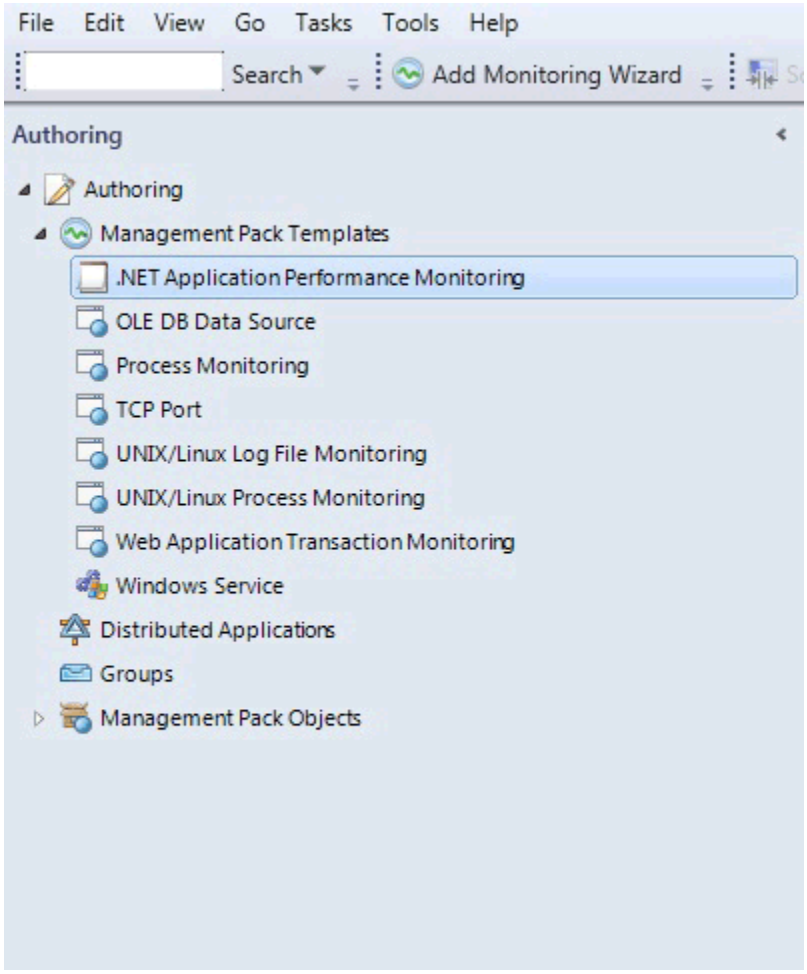
Network Monitoring

Operations Manager provides the ability to discover and monitor network routers and switches, including the network interfaces and ports on those devices and the virtual LAN (VLAN) that they participate in. You can also delete discovered network devices and prevent the deleted network devices from being rediscovered the next time discovery runs.

Application Monitoring

In Operations Manager, you can monitor Internet Information Services (IIS)-hosted .NET applications from server-side and client-side perspectives to get details about application performance and reliability that can help you pinpoint root causes of incidents. When you specify settings, the types of events to collect, the performance goals to measure, and servers to monitor, .NET Application Performance Monitoring reveals how web-based applications are running. You can see how frequently a problem is occurring, how a server was performing when a problem occurred, and the chain of events related to the slow request or method that is raising exceptions. This information is required to partner with software developers and database administrators to help ensure that applications perform correctly and reliably for your customers. For more information, see Authoring the .NET Application Performance Monitoring Template and Monitoring .NET Applications.

Location of .NET Application Performance Monitoring



Performance and Scale

Resource Pools

A resource pool contains only management servers and provides the ability to distribute workloads across multiple management servers, such as availability, network device monitoring, distributed monitor health rollup, and group calculation. For more information, see How to Create a Resource Pool.

Removal of Root Management Server

In Operations Manager, all management servers are peers; there is no root management server. The workload is split among all management servers in a management group, which provides high availability without requiring a cluster.

Improved Experience

Web Console

Operations Manager introduces a new web console that is optimized for faster load times and provides you with access to the new IT pro dashboards.

Dashboard Views

Operations Manager includes new comprehensive dashboard views that combine multiple panels of information into a single view. In Operations Manager, you can add the new dashboard views to My Workspace and the Monitoring workspace.

Creating Dashboard Views

Dashboard views have been significantly upgraded in Operations Manager from their capabilities in System Center Operations Manager 2007 R2, including custom layouts and nested dashboard views.

Display Dashboard Views in SharePoint

The Operations Manager web part displays specified dashboard views and can be added to Microsoft SharePoint 2010 sites. For more information, see Add a Dashboard to a SharePoint Site.

System Center 2012 - Orchestrator Replaces Microsoft-Developed Connector Functionality

Connectors developed by Microsoft have been discontinued for System Center 2012 – Operations Manager and their functionality has been replaced by System Center 2012 - Orchestrator.

Note

Orchestrator is not required to create and test non-Microsoft-developed connectors against System Center 2012.

Orchestrator provides the ability to create and run automated workflows, called runbooks, made of multiple activities that each performs a distinct function. The connector functionality of enabling System Center Operations Manager 2007 R2 to synchronize alerts with remote systems is achieved by creating runbooks, using activities that interact with Operations Manager and one or more other products. Because runbooks can include sophisticated logic and activities from any number of Integration Packs, you can implement scenarios that cannot be easily achieved with connectors. Integration Packs will be delivered for each System Center component and provide additional activities specific to a particular component.

Operations Manager Module for Windows PowerShell

Operations Manager provides a Windows PowerShell 2.0 module containing a full set of new cmdlets. The cmdlets in this module are only compatible with Operations Manager. You can recognize the Operations Manager cmdlets by the "SC" preceding the noun. For additional information about the Operations Manager cmdlets, open the Operations Manager command shell and type **Get-Help about_OpsMgr_WhatsNew**. For information about how the Operations Manager 2007 cmdlets map to the Operations Manager cmdlets, type **Get-Help about_OpsMgr_Cmdlet_Names**.

To use the Operations Manager cmdlets, you must establish a connection to an Operations Manager management group. You can establish either a persistent connection in which you can run multiple cmdlets, or a temporary connection when running a single cmdlet. For more information about connections, open the Operations Manager Shell and type **Get-Help about_OpsMgr_Connections**.

UNIX- and Linux-Based Computers

In Operations Manager, you can perform privileged operations on UNIX-based and Linux-based computers using unprivileged Run As accounts by combining with “sudo” elevation on the target UNIX-based and Linux-based computers. This capability avoids the need for UNIX or Linux root passwords to be known on the management server, and keeps the privilege control entirely within the domain of the UNIX or Linux administrator. Operations Manager also includes new Windows PowerShell cmdlets for performing agent maintenance functions on UNIX-based and Linux-based computers, allowing for scripting and background operations. In addition, the resource pool feature supports computers running UNIX and Linux. If a management server fails, another management server in the resource pool can take over the monitoring, providing high availability. For more information, see Monitoring UNIX- and Linux-Based Computers

Operations Console

You will notice some subtle changes to the Operations console. The **Actions** pane is now the **Tasks** pane, and includes a new section called **Navigation Tasks** that makes it easy for you to open views for a selected object. The **Tasks** pane offers two tabs: one for actions and one for resources and Help links. The **Navigation** and **Tasks** panes can be minimized or expanded instantly by clicking the arrow in the title bar of the pane.

See Also

Operations Guide for System Center 2012 – Operations Manager

Authoring Guide for System Center 2012 – Operations Manager

Operator Learning Roadmap for Operations Manager

System Center 2012 – Operations Manager helps organizations monitor their computers, networks, and applications. In many organizations, Operations Manager operators are the first level of monitoring and support and are limited in the possible actions they can take. This level is sometimes called Tier I support or “front-end support” or “help desk.” As the operator, you are the first to be notified when there is an alert, and the first to get the chance to react to an alert as needed.

This learning roadmap is intended for the operator in a Tier I role. If you are new to Operations Manager, this topic can help you identify what you need to learn to understand and use the features available to the Operations Manager operator role. You must understand the prerequisite topics first, because the other topics for Operations Manager build upon them and assume an understanding of them. Afterwards, you can begin learning about Operations Manager by reading the documents in the Level 100, 200, 300, and 400 sections.

We recommend that you read the topics in the order listed.

- Prerequisite Information
- Level 100
- Level 200
- Level 300

Prerequisite Information

This section contains links to a variety of topics that contain background information that will help you understand how Operations Manager works.

- **Step 1: Learn about the features that comprise a management group**.

  See Key Concepts.

  Your goal is to understand the parts of the management group and the basic process of discovery and monitoring.
- **Step 2: Learn about heartbeats**.

  See How Heartbeats Work in Operations Manager.

  Your goal is to understand how Operations Manager monitors its communication channels with agent-managed computers.

Level 100

The following topics contain introductory information that will help you learn to navigate the workspaces in the Operations Manager consoles.

- **Step 1: Learn about the console layout**.

  See Comparing the Operations Console and Web Console in Operations Manager.

This topic presents the layout of the Operations Manager consoles.

Your goal is to understand the purpose of each section of the consoles.

- **Step 2: Learn about the Monitoring workspace**.

  See Using the Monitoring Workspace in Operations Manager.

  This topic provides an overview of the Monitoring workspace.

  Your goal is to understand the purpose of the Monitoring workspace.

- **Step 3: Learn about the types of views**.

  See View Types in Operations Manager and Standard Views in Operations Manager.

  These topics describe the types of views available in Operations Manager and the preconfigured views created when Operations Manager is installed.

  Your goal is to understand the type of information provided in each view.

- **Step 4: Learn about using scope, search, and find**.

  See Finding Data and Objects in the Operations Manager Consoles.

  This topic explains how to use the **Scope**, **Search**, and **Find** tools to locate data and objects.

  Your goal is to understand how to find specific objects and data.

- **Step 5: Learn about My Workspace**.

  See Using My Workspace in Operations Manager.

  This topic describes My Workspace.

  Your goal is to understand how to use My Workspace.

Level 200

The following topics contain intermediate information that will help you get started monitoring.

- **Step 1: Learn about management group health**.

  See Monitoring the Health of the Management Group.

  This topic describes the **Management Group Health** dashboard view.

  Your goal is to understand how to use the **Management Group Health** dashboard view to monitor the health of the management group.

- **Step 2: Learn about Health Explorer**.

  See Using Health Explorer in Operations Manager and Using Health Explorer to Investigate Problems.

  These topics describe Health Explorer, an essential tool in Operations Manager for identifying and resolving health state issues.

  Your goal is to understand how to navigate in Health Explorer and how to use Health Explorer to investigate problems.

- **Step 3: Learn about viewing alerts**.

  See Viewing Alert Details and Examining Properties of Alerts, Rules, and Monitors.

  These topics describe the type of information you can obtain from an alert.

Your goal is to understand how to identify the source of an alert and locate information to help you resolve the issue that caused the alert.

- **Step 4: Learn about resolving alerts**.

  See Impact of Closing an Alert and How to Close an Alert Generated by a Monitor.

  These topics explain what happens when you close an alert and how to close an alert that was generated by a monitor.

  Your goal is to understand when and how to close alerts.

- **Step 5: Learn about alert notifications**.

  See How to Subscribe to Notifications from an Alert.

  This topic explains how to subscribe to an alert notification.

  Your goal is to understand how to have notifications of alerts sent to you by phone, text message, or instant message.

Level 300

The following documents contain advanced information for users in the Operator role.

- **Step 1: Learn about tasks**.

  See Running Tasks in Operations Manager.

  This topic explains how to run tasks associated with a selected object.

  Your goal is to understand how to run a task.

- **Step 2: Learn about creating views**.

  See Creating Views in Operations Manager.

  This topic explains how to create views. Operators can create views in My Workspace.

  Your goal is to understand how to create customized views.

- **Step 3: Learn about running diagnostics and recoveries**.

  See Diagnostic and Recovery Tasks.

  This topic describes diagnostics and recoveries that can be associated with an alert.

  Your goal is to understand how to run diagnostics and recoveries.

- **Step 4: Learn about maintenance mode**.

  See How to Suspend Monitoring Temporarily by Using Maintenance Mode.

  This topic explains maintenance mode.

  Your goal is to understand when and how to use maintenance mode to temporarily stop monitoring a computer.

Feedback

Your feedback is valuable and welcome! Please rate this content using the stars in the upper-right of your browser window, or send your comments and suggestions to Operations Manager Documentation (opsmgrdocs@microsoft.com). The author will review your comments and use

them to help improve this documentation. Your e-mail address will not be saved or used for any other purposes.

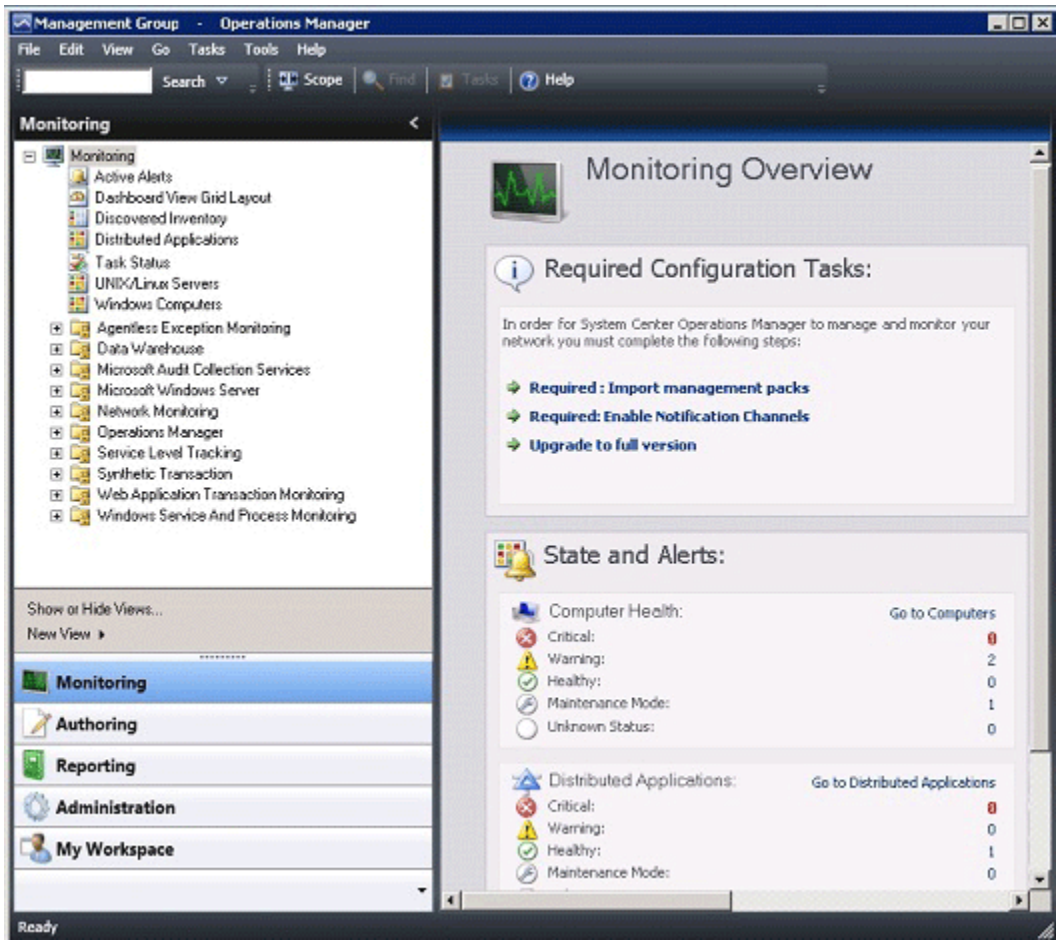
Operations Manager Key Concepts

Operations Manager, a component of Microsoft System Center 2012, is software that helps you monitor services, devices, and operations for many computers from a single console. This topic explains basic concepts about Operations Manager for the administrator who manages the Operations Manager infrastructure and the operator who monitors and supports the computers in your business.

What Operations Manager Does

Businesses, small and large, are typically dependent on the services and applications provided by their computing environment. IT departments are responsible for ensuring the performance and availability of those critical services and applications. That means that IT departments need to know when there is a problem, identify where the problem is, and figure out what is causing the problem, ideally before the users of the applications encounter the problems. The more computers and devices in the business, the more challenging this task becomes.

Using Operations Manager in the environment makes it easier to monitor multiple computers, devices, services, and applications. The Operations console, shown in the following image, enables you to check the health, performance, and availability for all monitored objects in the environment and helps you identify and resolve problems.



Note

To learn how to use the Operations Manager consoles, see Using the Operations Manager Consoles in the Operations Guide.

Operations Manager will tell you which monitored objects are not healthy, send alerts when problems are identified, and provide information to help you identify the cause of a problem and possible solutions. As the administrator, you configure what will be monitored by selecting computers and devices to be monitored and importing management packs that provide monitoring for specific features and applications. To decide which objects to monitor and what to monitor for, you need to understand the features that comprise the Operations Manager infrastructure and how Operations Manager works.

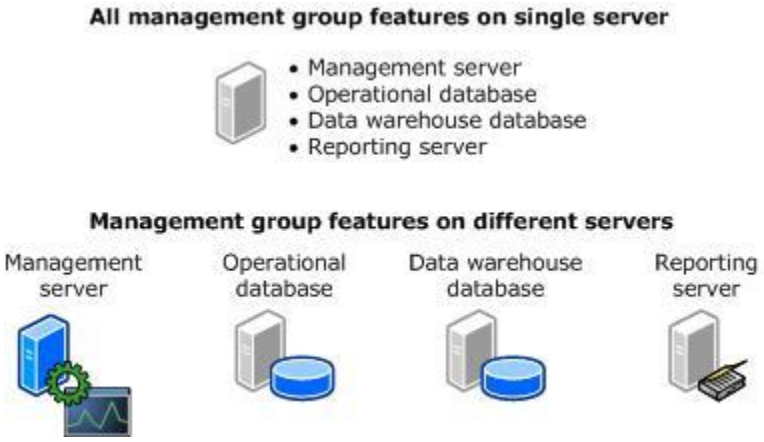
The Operations Manager Infrastructure

Installing Operations Manager creates a *management group*. The management group is the basic unit of functionality. At a minimum, a management group consists of a *management server*, the *operational database*, and the *reporting data warehouse database*.

- The **management server** is the focal point for administering the management group and communicating with the database. When you open the Operations console and connect to a management group, you connect to a management server for that management group. Depending on the size of your computing environment, a management group can contain a single management server or multiple management servers.
- The **operational database** is a SQL Server database that contains all configuration data for the management group and stores all monitoring data that is collected and processed for the management group. The operational database retains short-term data, by default 7 days.
- The **data warehouse database** is a SQL Server database that stores monitoring and alerting data for historical purposes. Data that is written to the Operations Manager database is also written to the data warehouse database, so reports always contain current data. The data warehouse database retains long-term data.

When Operations Manager reporting functionality is installed, the management group also contains a *Reporting server* which builds and presents reports from data in the data warehouse database.

These core components of a management group can exist on a single server, or they can be distributed across multiple servers, as shown in the following image.



For information about installing management group features, see [Operations Manager 2012 Deployment Guide].

Management Servers

The role of the management server is to administer the management group configuration, administer and communicate with agents, and communicate with the databases in the management group.

The management group can contain multiple management servers to provide additional capacity and continuous availability. When two or more management servers are added to a management group, the management servers become part of a *resource pool* and work is spread across the members of the pool. When a member of the resource pool fails, other members in the resource pool will pick up that member's workload. When a new management server is added, the new management server automatically picks up some of the work from existing members in the

resource pool. All members in the resource pool will manage a distinct set of remote objects; at any given time, two members in the same pool will not manage the same object at the same time.

A specialized type of management server is the *gateway server*. A gateway server enables the monitoring of computers in untrusted domains. For more information, see Monitoring Across Untrusted Boundaries.

Agents

An Operations Manager *agent* is a service that is installed on a computer. The agent collects data, compares sampled data to predefined values, creates alerts, and runs responses. A management server receives and distributes configurations to agents on monitored computers.

Every agent reports to a management server in the management group. This management server is referred to as the agent's primary management server.

Agents watch data sources on the monitored computer and collect information according to the configuration that is sent to it from its management server. The agent also calculates the health state of the monitored computer and objects on the monitored computer and reports back to the management server. When the health state of a monitored object changes or other criteria are met, an alert can be generated from the agent. This lets operators know that something requires attention. By providing health data about the monitored object to the management server, the agent provides an up-to-date picture of the health of the device and all the applications that it hosts.

An agent can be configured to act as a *proxy agent*. A proxy agent is an agent that can forward data to a management server on behalf of a computer or network device other than its host computer. For example, an agent that is installed on the physical node of an SQL cluster can be enabled to act as proxy to monitor the cluster resource. Proxy agents enable monitoring of computers and devices on which an agent cannot be installed. For more information, see Agentless Monitoring.

Services

On a monitored computer, the Operations Manager agent is listed as the System Center Management Health service. The System Center Management Health service collects performance data, executes tasks, and so on. Even when the service is unable to communicate with the management server it reports to, the service continues to run and queues the collected data and events on the disk of the monitored computer. When the connection is restored, the System Center Management Health service sends collected data and events to the management server.

Note

The System Center Management Health service is sometimes referred to as the health service.

The System Center Management Health service also runs on management servers. On a management server, the System Center Management Health service runs monitoring workflows

and manages credentials. To run workflows, the System Center Management Health service initiates MonitoringHost.exe processes using specified credentials. These processes monitor and collect event log data, performance counter data, Windows Management Instrumentation (WMI) data, and run actions such as scripts.

Management servers also run the System Center Data Access service and the System Center Management Configuration service.

The System Center Data Access service provides access for the Operations console to the operational database and writes data to the database.

The System Center Management Configuration service manages the relationships and topology of the management group. It also distributes management packs to monitored objects.

Management Packs

The workflows that the System Center Management service runs are defined by *management packs*. Management packs define the information that the agent collects and returns to the management server for a specific application or technology. For example, the BizTalk Server Management Pack contains rules and monitors that collect and evaluate events and operations that are important to ensuring the health and efficiency of the BizTalk Server application.

After Operations Manager installs an agent on a computer, it sends an initial configuration to the agent. The initial configuration includes *object discoveries* from management packs. The management pack defines the types of objects, such as applications and features, that will be monitored on computers that have been discovered by Operations Manager. Agents send data to the management server that identifies the instances of objects discovered on the computer. The management server then sends the agents the elements of management packs that apply to the discovered objects for each computer, such as rules and monitors.

A *rule* defines the events and performance data to collect from computers and what to do with the information after it is collected. A simple way to think about rules is as an If/Then statement. For example, a management pack for an application might contain rules such as the following:

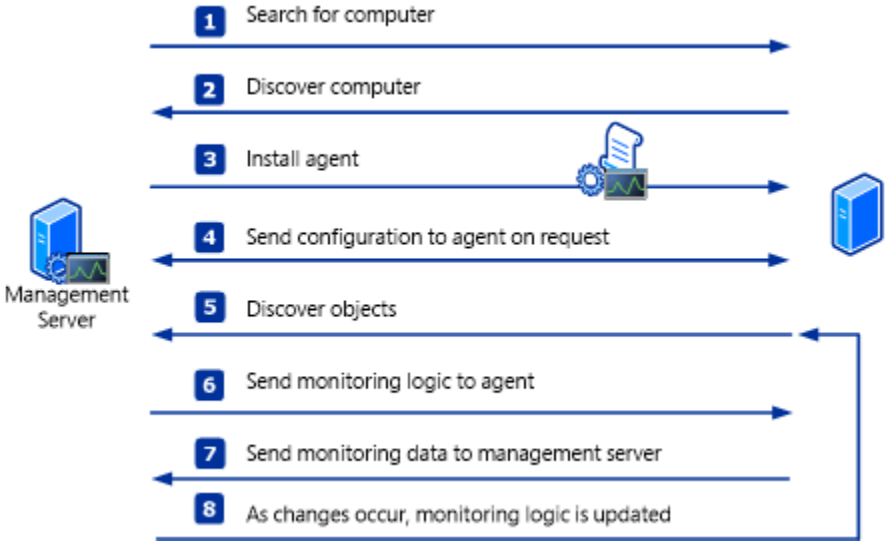
- If a message indicating that the application is shutting down appears in the event log, create an alert.
- If upload of a source file fails, collect the event that indicates this failure.

As these examples show, rules can create alerts and collect events or performance data, which the agent sends to the management server. Rules can also run scripts, such as allowing a rule to attempt to restart a failed application.

Discovered objects have a health state, which is reflected in the Operations console as green (successful or healthy), yellow (warning), or red (critical or unhealthy). *Monitors* define the health states for particular aspects of the monitored object. For example, a monitor for disk drive capacity might define green as less than 85 percent full, yellow as over 85 percent full, and red as over 90 percent full. A monitor can be configured to generate an alert when a state change occurs.

How Objects Are Discovered and Monitored

The following image is a simplified illustration of how objects are discovered and monitored.



1. The administrator configures Operations Manager to search for computers to manage. For more information about discovering computers, see Managing Discovery and Agents.
2. Computers that meet the specified criteria and are not already managed are identified.
3. An Operations Manager agent is installed on the discovered computer.
4. The agent requests configuration data, and then the management server sends the agent configuration data from installed management packs that includes classes to be discovered. For example, if the Windows Server operating system management packs are installed, the management server will send the agent the operating system classes.
5. The agent compares the configuration data to the computer, identifies any objects that it discovers, and returns the information to the management server. For example, the agent will return to the management server that an instance of Windows Server 2008 R2 operating system is on the computer.
6. The management server sends the agent all monitoring logic from installed management packs that applies to the discovered objects. For example, the agent will receive all monitoring logic that applies to Windows Server 2008 R2.
7. The agent applies the monitoring logic, such as rules and monitors, runs workflows, and returns data to the management server.
8. As changes occur to discovered objects, such as applications being added or uninstalled, the agent sends the updated information to the management server, which then sends updated monitoring logic.

Note

Operations Manager can also discover and monitor network devices, computers running UNIX and Linux operating systems, and provide agentless monitoring. For more information, see Operations Manager Monitoring Scenarios in the Operations Guide.

Communication Between Agents and Management Servers

The Operations Manager agent sends alert and discovery data to the primary management server, which writes the data to the operational database. The agent also sends events, performance, and state data to the primary management server for that agent, which writes the data to the operational and data warehouse databases simultaneously.

The agent sends data according to the schedule parameters for each rule and monitor. For optimized collection rules, data is only transmitted if a sample of a counter differs from the previous sample by a specified tolerance, such as 10%. This helps reduce network traffic and the volume of data stored in the operational database.

Additionally, all agents send a packet of data, called a *heartbeat*, to the management server on a regular schedule, by default every 60 seconds. The purpose of the heartbeat is to validate the availability of the agent and communication between the agent and the management server. For more information on heartbeats, see How Heartbeats Work in Operations Manager.

For each agent, Operations Manager runs a *health service watcher*, which monitors the state of the remote Health Service from the perspective of the management server.

Other resources for Operations Manager

- TechNet Library main page for Operations Manager
- To learn how to install Operations Manager and deploy a management group, see Deployment Guide for Operations Manager for System Center 2012
- To learn how to use Operations Manager after the management group is set up, see Operations Guide for Operations Manager for System Center 2012
- To learn how to create a management pack, see Author's Guide for Operations Manager for System Center 2012
- Operations Manager Documentation Downloads
- Operations Manager Community

System Requirements for System Center 2012 - Operations Manager

System Center 2012 – Operations Manager, System Center 2012 Service Pack 1 (SP1) - Operations Manager, and System Center 2012 R2 Operations Manager have requirements for supported operating systems, hardware configurations, software requirements, installation combinations, and security configurations. Both versions of Operations Manager have their own sections covering these supported configurations.

System Requirements

1. System Requirements: System Center 2012 - Operations Manager
2. System Requirements: System Center 2012 SP1 - Operations Manager
3. System Requirements: System Center 2012 R2 Operations Manager

System Requirements: System Center 2012 R2 Operations Manager

This document provides information about the operating systems, hardware configurations, software requirements, installation combinations, and security configurations for System Center 2012 R2 Operations Manager. This document focuses on the system requirements, and it mentions unsupported configurations only when necessary. If operating systems, hardware configurations, software requirements, installation combinations, and security configurations are not presented here, they have not been tested and are not supported.

Note

For system requirements across all components of System Center, see System Requirements for System Center 2012 R2.

The Prerequisites checker is no longer a separate option in Setup. However, you can begin the installation process to check the hardware and software prerequisites, and then cancel installation after the required prerequisites have been determined.

We recommend that you also review the key concepts of Operations Manager. Documents to review include the following:

- Release Notes for Operations Manager in System Center 2012 R2 identifies any changes that could affect planning for a new deployment of System Center 2012 R2 Operations Manager.
- Deploying System Center 2012 - Operations Manager provides detailed information about the security-related features and settings in Operations Manager that can affect your deployment.

This document contains the following sections:

- Operations Manager Virtualization Support
- Running Operations Manager on Windows Azure Virtual Machines
- Minimum Screen Resolution Requirements
- Minimum Hardware Requirements
- Minimum Software Requirements
- Requirements by Feature
  - Management Server
  - Operations Console
  - Web Console
  - Operational Database
  - Microsoft Monitoring Agent – Windows-Based Computers

- Operations Manager Agent – UNIX- or Linux Computers
- Operations Manager Reporting
- Operations Manager Data Warehouse
- Operations Manager Gateway Server

- Supported Firewall Scenarios
- Minimum Network Connectivity Speeds
- Supported Cluster Configurations
- Monitored Item Capacity
- Operations Manager Feature Firewall Exceptions
- Support for Languages in Addition to English
- Supported Network Monitoring Scenarios
- Application Performance Monitoring Requirements

Operations Manager Virtualization Support

Microsoft supports running all Operations Manager server features in any physical or virtual environment that meets the minimum requirements that are stated in this document. However, for performance reasons, we recommend that you store the operational database and data warehouse database on a directly attached physical hard drive, and not on a virtual disk. Specifically, virtual computers that are running any Operations Manager server feature must not use any functionality that does not immediately commit all activity on the virtual computer to the virtual hard drive. This includes making use of point-in-time snapshots and writing changes to a temporary virtual hard drive. This is true for every virtualization technology that is used with Operations Manager.

Running Operations Manager on Windows Azure Virtual Machines

System Center 2012 R2 Operations Manager runs on virtual machines in Windows Azure just as it does on physical computer systems. We recommend using Operations Manager with Windows Azure virtual machines in the following scenarios:

- **Scenario 1:** You can run Operations Manager on a Windows Azure virtual machine and use it to monitor other Windows Azure virtual machines.
- **Scenario 2:** You can run Operations Manager on a Windows Azure virtual machine and use it to monitor virtual machines that are not running on Windows Azure.
- **Scenario 3:** You can run Operations Manager on-premises and use it to monitor Windows Azure virtual machines.

Operations Manager was tested by Microsoft by installing and using it in a Windows Azure virtual machine. The standard sizing and supported configuration for Operations Manager applies to Windows Azure virtual machines.

Minimum Screen Resolution Requirements

Operations Manager is optimized for screen resolutions of 1280 x 1024 or larger. The minimum supported screen resolution is 1024 x 768.

Minimum Hardware Requirements

Use the Operations Manager Sizing Helper to determine hardware requirements for each Operations Manager server feature. If you want to install more than one feature on the same computer, use the higher of the recommended hardware requirements for any of the combined features.

Supported Processors, Memory, and Disk Space

Note

Operations Manager does not support installing the 32-bit agent on a 64-bit operating system. Operations Manager provides native support for x86-based computers for agents and consoles, and x64-based computers for all server features.

Minimum Software Requirements

Operations Manager server features require a supported operating system. For a list of the supported operating systems for each server feature, see the **Requirements by Feature** section in this document.

Installing System Center 2012 R2 Operations Manager on Windows Server 2012 Core requires Windows 32-bit on Windows 64-bit (WoW64) support, .NET 4.5, Windows PowerShell 3.0. In addition, you need AuthManager. To install AuthManager for Windows 2012, add **Server-Gui-Mgmt-Intra** (the Minimal Server Interface.) To install for Windows 2012 R2, install AuthManager with this command: **dism /online /enable-feature /featurename:AuthManager**. If you attempt to install Operations Manager without WoW64 support installed, the bootstrapper will present an error message indicating the side-by-side configuration is incorrect.

We recommend that you check for updates and hotfixes for Microsoft SQL Server. Note the following database considerations for Operations Manager:

- SQL Server 2008 R2 and SQL Server 2012 are available in both Standard and Enterprise editions. Operations Manager will function with both editions.
- Operations Manager does not support hosting its databases or SQL Server Reporting Services on a 32-bit edition of SQL Server.
- Using a different version of SQL Server for different Operations Manager features is not supported. The same version should be used for all features.
- SQL Server collation settings for all databases must be one of the following: SQL_Latin1_General_CP1_CI_AS; Latin1_General_100_CI_AS, // EN, IT, DE, PT-BR, NE, PT-PT; French_CI_AS; French_100_CI_AS; Cyrillic_General_CI_AS; Chinese_PRC_CI_AS; Chinese_Simplified_Pinyin_100_CI_AS, // CN simplified; Chinese_Traditional_Stroke_Count_100_CI_AS, // CN traditional, CN-HKJapanese;_CI_AS; Japanese_XJIS_100_CI_AS; Traditional_Spanish_CI_AS; Modern_Spanish_100_CI_AS; or

Latin1_General_CI_AS; Cyrillic_General_100_CI_AS, // RU; Korean_100_CI_AS; Czech_100_CI_AS; Hungarian_100_CI_AS; olish_100_CI_AS; and Finnish_Swedish_100_CI_AS. No other collation settings are supported.

- The SQL Server Agent service must be started, and the startup type must be set to automatic.
- The db_owner role for the operational database must be a domain account. If you set the SQL Server Authentication to Mixed mode, and then try to add a local SQL Server login on the operational database, the Data Access service will not be able to start. For information about how to resolve the issue, see System Center Data Access Service Start Up Failure Due to SQL Configuration Change
- If you plan to use the Network Monitoring features of System Center 2012 R2 Operations Manager, you should move the tempdb database to a separate disk that has multiple spindles. For more information, see tempdb Database.

If you want to install more than one Operations Manager feature on the same computer, you must install the prerequisite software for all of the combined features.

Requirements by Feature

Management Server

- Disk space: %SYSTEMDRIVE% requires at least 1024 MB free hard disk space.
- Server Operating System: must be Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 Core Installation, or Windows Server® 2012 R2.
- Processor Architecture: must be x64.
- Windows PowerShell version: Windows PowerShell version 2.0, Windows PowerShell version 3.0, or Windows PowerShell version 4.0.
- Windows Remote Management: Windows Remote Management must be enabled for the management server.
- .NET Framework 4 or .NET Framework 4.5 is required. For more information, see .NET Framework 4 redistributable package

Operations Console

- Microsoft Report Viewer 2012 Redistributable Package

> **Important**
> Report Viewer also has a dependency on Microsoft System CLR Types for SQL Server 2012. The SQL Server System CLR Types package contains the components implementing the geometry, geography, and hierarchy ID types in SQL Server 2012. This component can be installed separately from the server to allow client applications to use these types outside of the server. Click the installation instructions and you see the links that point to other requirements for this component: Windows Installer 4.5, X86 Package (SQLSysClrTypes.msi),X64 Package (SQLSysClrTypes.msi), and SQL Server System CLR Types Books on-line page.

- Disk space: %SYSTEMDRIVE% requires at least 512 MB free hard disk space.
- File system: %SYSTEMDRIVE% must be formatted with the NTFS file system.
- Server Operating System: must be Windows 7, Windows 8, Windows Server 2008 R2 SP1, Windows Server 2012, or Windows Server® 2012 R2.
- Processor Architecture: must be x64 for servers and x64 or x86 for a client computer.
- Windows Installer version: at least Windows Installer 3.1.
- Windows PowerShell version: Windows PowerShell version 2.0. Windows PowerShell version 3.0 is required to use Windows PowerShell cmdlets for administration of UNIX and Linux computers.
- .NET Framework 4 is required. For more information, see .NET Framework 4 redistributable package

Web Console

- Operating System: Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server® 2012 R2.
- Processor Architecture: must be x64.
- Web browsers: Internet Explorer 8, Internet Explorer 9, Internet Explorer 10, Internet Explorer 11, Silverlight 5.0
- Internet Information Services (IIS) 7.5 and later versions, with the IIS Management Console and the following role services installed:
  - Static Content
  - Default Document
  - Directory Browsing
  - HTTP Errors
  - HTTP Logging
  - Request Monitor
  - Request Filtering
  - Static Content Compression
  - Web Server (IIS) Support
  - IIS 6 Metabase Compatibility
  - ASP.NET (both the 2.0 and 4.0 versions of ASP.NET are required.)
  - Windows Authentication
- Selected website for web console: requires a configured http or https binding.

  Important
  Installing the web console on a computer that has Microsoft SharePoint installed is not supported.
- The System Center 2012 R2 Operations Manager SharePoint Dashboard Viewer Web Part works on SharePoint 2010 and SharePoint 2013 and is supported. However, it does not work on Office 365 SharePoint and is not supported.

- .NET Framework 4 is required for Setup to run. For more information, see the following documents:
  - .NET Framework 4 redistributable package

Note
Installation of the web console requires that ISAPI and CGI Restrictions in IIS are enabled for ASP.NET 4. To enable this, select the web server in IIS Manager, and then double-click **ISAPI and CGI Restrictions**. Select **ASP.NET v4.0.30319**, and then click **Allow**.

Important
You must install IIS before installing .NET Framework 4. If you installed IIS after installing .NET Framework 4, you must register ASP.NET 4.0 with IIS. Open a Command prompt window by using the **Run As Administrator** option, and then run the following command:

%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -r

Operational Database

Disk space: The operational database must have at least 1024 MB free disk space. This is enforced at the time of database creation, and it will likely grow significantly. For information about SQL Server Planning, see Installing SQL Server 2008 R2 or Install SQL Server 2012.

File system: %SYSTEMDRIVE% must be formatted with the NTFS file system.

Operating System: Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 Core Installation or Windows Server® 2012 R2.

Processor Architecture: x64.

Windows Installer version: at least Windows Installer 3.1.

Microsoft SQL Server: SQL Server SQL 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, SQL Server 2012 SP1.

SQL Server Full Text Search is required.

.NET Framework 4 is required. For more information, see .NET Framework 4 redistributable package

Microsoft Monitoring Agent – Windows-Based Computers

- File system: %SYSTEMDRIVE% must be formatted with the NTFS file system.
- Operating Systems: Windows Server 2003 SP2, Windows Server 2008 SP2, Windows Server 2008 R2, Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server® 2012 R2, Windows XP Professional x64 Edition SP2, Windows XP Professional SP3, Windows Vista SP2, Windows 7, POSReady, Windows XP Embedded Standard, Windows XP Embedded Enterprise, Windows XP Embedded POSReady, Windows 7 Professional for Embedded Systems, Windows 7 Ultimate for Embedded Systems, Windows 8 Pro or Windows 8 Enterprise.
- Processor Architectures: x64 or x86.

- Microsoft Core XML Services (MSXML) version: Microsoft Core XML Services 6.0 is required for the Operations Manager agent for Windows Server 2003.
- Windows PowerShell version: Windows PowerShell version 2.0, or Windows PowerShell version 3.0.

  Note
  Windows PowerShell is required for agents that will be monitored by a management pack that uses Windows PowerShell scripts.

Operations Manager Agent – UNIX- or Linux Computers

Supported operating systems:

- CentOS 5 and 6 (x86/x64)
- Debian GNU/Linux 5, 6, and 7 (x86/x64)
- HP-UX 11i v2 and v3 (PA-RISC and IA64)
- IBM AIX 5.3, AIX 6.1 (POWER), and AIX 7.1 (POWER)
- Novell SUSE Linux Enterprise Server 9 (x86), 10 SP1 (x86/x64), and 11 (x86/x64)
- Oracle Solaris 9 (SPARC), Solaris 10 (SPARC and x86), and Solaris 11 (SPARC and x86)
- Oracle Linux 5 and 6 (x86/x64)
- Red Hat Enterprise Linux 4, 5, and 6 (x86/x64)
- Ubuntu Linux Server 10.04 and 12.04 (x86/x64)

Operations Manager Reporting

- Disk space: The %SYSTEMDRIVE% requires at least 1024 MB free hard disk space.
- Operating System: Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 Core Installation or Windows Server® 2012 R2.
- Processor Architecture: x64.
- Microsoft SQL Server: SQL Server SQL 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, SQL Server 2012 SP1.
- The Remote Registry service must be enabled and started.
- Microsoft SQL Server Reporting Services: SQL Server SQL 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, SQL Server 2012 SP1.
- System Center 2012 – Operations Manager supports SQL Server Reporting Services in native mode only; do not use SharePoint integrated mode.
- .NET Framework 4 is required. For more information, see the following document:
  - .NET Framework 4 redistributable package

Operations Manager Data Warehouse

- Disk space: The data warehouse database must have at least 1024 MB free hard disk space. This is enforced at the time of database creation, and the required disk space will likely grow

significantly. For information about requirements in SQL Server Planning, see Installing SQL Server 2008 or Installing SQL Server 2008 R2.

- File system: %SYSTEMDRIVE% must be formatted with the NTFS file system.
- Operating System: Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 Core Installation or Windows Server® 2012 R2.
- Processor Architecture: x64.
- Windows Installer version: at least Windows Installer 3.1.
- Microsoft SQL Server: SQL Server SQL 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, SQL Server 2012 SP1.
- SQL Server Full Text Search is required.
- .NET Framework 4 is required for Setup to run. For more information, see the following document:
  - .NET Framework 4 redistributable package

Operations Manager Gateway Server

- Disk space: %SYSTEMDRIVE% requires at least 1024 MB free hard disk space.
- Server Operating System: must be Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 Core Installation or Windows Server® 2012 R2.
- Processor Architecture: must be x64.
- Windows PowerShell version: Windows PowerShell version 2.0, or Windows PowerShell version 3.0.
- Microsoft Core XML Services (MSXML) version: Microsoft Core XML Services 6.0 is required for the management server.
- .NET Framework 4 is required if the Gateway server manages UNIX/Linux agents or network devices.

Supported Firewall Scenarios

The following table shows Operations Manager feature interaction across a firewall, including information about the ports that are used for communication between the features, which direction to open the inbound port, and whether the port number can be changed.

Firewall Scenarios for System Center 2012 R2 Operations Manager

Operations Manager Feature A	Port number and direction	Feature B	Configurable	Note
Management server	1433 --->	Operational database	Yes (Setup)	
Management server	1434 UDP < ---	Operational database	No	If the operational database is installed on a named instance of

Operations Manager Feature A	Port number and direction	Feature B	Configurable	Note
				SQL Server SQL 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1 such as in a cluster, and the Windows Firewall is enabled on the management server, you have to also open UDP 1434 inbound on the management server.
Management server	1433 --->	Operational database	Yes (Setup)	
Management server	5723, 5724 -->	Management server	No	Port 5724 must be open to install this feature and can be closed after this feature has been installed.
Management server	1433 -->	Reporting data warehouse	No	
Management server	1433 --->	Reporting data warehouse	No	
Reporting server	5723, 5724 -->	Management server	No	Port 5724 must be open to install this feature and can be closed after this feature has been installed.
Operations console	5724 --->	Management server	No	
Connector	51905 --->	Management	No	

Operations Manager Feature A	Port number and direction	Feature B	Configurable	Note
Framework source		server		
Web console server	Selected web site port --->	Management server	No	
Web console (for Application Diagnostics	1433, 1434 -->	Operational database	Yes (Setup)	
Web console (for Application Advisor)	1433, 1434 -->	Data warehouse	Yes (Setup)	
Web console (for Application Advisor)	80 --->	SQL Server Reporting Services	No	
Web console browser	80, 443 --->	web console server	Yes (IIS Admin)	Default for HTTP or SSL. For either Network Authentication or Mixed Authentication, an account name and password can be sent as part of the request. We recommend you use SSL.
Agent installed by using MOMAgent.msi	5723 --->	Management server	Yes (Setup)	
Agent installed by using MOMAgent.msi	5723 --->	Management server	Yes (Setup)	
Agent installed by using MOMAgent.msi	5723 --->	Gateway server	Yes (Setup)	
Gateway server	5723 --->	Management server	Yes (Setup)	
Agent (Audit Collection Services (ACS) forwarder)	51909 --->	Management server Audit Collection	Yes (Registry)	

Operations Manager Feature A	Port number and direction	Feature B	Configurable	Note
		Services (ACS) Collector		
Agentless Exception Monitoring data from client	51906 --->	Management server Agentless Exception Monitoring (AEM) file share	Yes (Client Monitoring Wizard)	
Customer Experience Improvement Program data from client	51907 --->	Management server (Customer Experience Improvement Program) Endpoint	Yes (Client Monitoring Wizard)	
Operations console (reports)	80 --->	SQL Server Reporting Services	No	The Operations console uses port 80 to connect to the SQL Server Reporting Services website.
Reporting server	1433 --->	Reporting data warehouse	Yes	
Management server (Audit Collection Services Collector)	1433 --->	Audit Collection Services (ACS) database	Yes	
Management Server	161, 162 <--->	Network device	Yes	All firewalls between the management servers in the resource pool and the network devices need to allow SNMP (UDP) and ICMP bi-directionally, and ports 161 and 162 need to be open bi-directionally. This

Operations Manager Feature A	Port number and direction	Feature B	Configurable	Note
				includes Windows Firewall on the management server itself. If your network devices are using a port other than 161 and 162, you need to open bi-directional UDP traffic on these ports as well.
Management server or gateway server	1270 --- >	UNIX or Linux computer	No	
Management server or gateway server	22 --- >	UNIX or Linux computer	Yes	

In the preceding table, if SQL Server SQL 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1 is installed by using a default instance, the port number is 1433. If SQL Server is installed with a named instance, it is probably using a dynamic port. To identify the port, do the following:

1. Run SQL Server Configuration Manager.
2. Open SQL Server Network Configuration.
3. Open Protocols for INSTANCE1 (or the instance that is running under it).
4. Open TCP/IP.
5. Click **IP Addresses**.
6. The port is under IPAll (usually the TCP Dynamic Ports).

Minimum Network Connectivity Speeds

Operations Manager requires the following minimum network connectivity speeds between the specified features.

Feature A	Feature B	Minimum requirement
Management server	Agent	64 Kbps
Management server	Agentless	1024 Kbps
Management server	Database	256 Kbps

Feature A	Feature B	Minimum requirement
Management server	Console	768 Kbps
Management server	Management server	64 Kbps
Management server	Data warehouse database	768 Kbps
Management server	Reporting server	256 Kbps
Management server	Gateway server	64 Kbps
Local management group	Connected management group (tiered)	1024 Kbps
Web console server	web console	128 Kbps
Reporting Data Warehouse	Reporting server	1024 Kbps
Console	Reporting server	768 Kbps
Audit collector	Audit database	768 Kbps

Supported Cluster Configurations

Operations Manager supports the clustering configurations for Operations Manager features as shown in the following table:

Important
Clustering of management servers is not supported in System Center 2012 R2 Operations Manager.

You can use SQL Server failover clustering or SQL Server 2012 AlwaysOn. For more information about SQL Server 2012 AlwaysOn, see Using SQL Server 2012 Always On Availability Groups with System Center 2012 SP1 - Operations Manager.

When using SQL Server failover clustering, only Cluster service quorum node clusters are supported. Multisite clusters (geographically dispersed clusters) are supported for all Operations Manager cluster roles. You can use replication technology to help provide high availability for data in Operations Manager, but the latency of communications between components introduce risks to data replication and might introduce failover issues. We recommend that you use synchronous mirroring of data disks between sites. Synchronous mirroring means that the data is fully synchronized across all sites and ensures the correct behavior of applications in the event of failover across sites.

Important
Microsoft is not obligated to release a hotfix on any Operations Manager issue that cannot be reproduced in a non-multisite cluster environment. If an analysis determines that non-Microsoft components in the configuration are causing the issue, the customer must work with the appropriate vendor for those components.

Server Feature	Cluster	Notes
Operations Manager Operational database	Single Active-Passive cluster	Other Operations Manager features must not be installed on the cluster or nodes of the cluster.
Operations Manager Reporting data warehouse	Single Active-Passive cluster	Other Operations Manager features must not be installed on the cluster or nodes of the cluster.
Audit Collection Services (ACS) database	Single Active-Passive cluster	Other Operations Manager features must not be installed on the cluster or nodes of the cluster.

Supported, But Not Recommended Cluster Configurations

Operations Manager supports the following clustering configurations for Operations Manager server roles, as shown in the following table; however, because of a potential performance effect on your computer running SQL Server, these configurations are not recommended:

Server Feature	Cluster	Notes
Operations Manager operational database and Operations Manager Reporting data warehouse.	Active-Active cluster where the operational database is installed on one node of the cluster and the Reporting data warehouse is installed on the other node of the cluster.	There might be some performance issues with SQL Server in this configuration.
Operations Manager operational database, Reporting data warehouse, and Audit Collection Services (ACS) database.	Single Active-Passive or Active-Active cluster where all three components are on a single cluster.	There might be some performance issues with SQL Server in this configuration.
Operations Manager operational database and Audit Collection Services database.	Single Active-Passive cluster where both components are on a single cluster.	There might be some performance issues with SQL Server in this configuration.
Operations Manager operational database and	Single Active-Passive cluster where both components are	There might be some performance issues with SQL

Server Feature	Cluster	Notes
Reporting data warehouse.	on a single cluster.	Server in this configuration.
Reporting data warehouse and Audit Collection Services database.	Single Active-Passive cluster where both components are on a single cluster.	There might be some performance issues with SQL Server in this configuration.

Monitored Item Capacity

Operations Manager supports the following number of monitored items.

Monitored item	Recommended limit
Simultaneous Operations consoles	50
Agent-monitored computers reporting to a management server	3,000
Agent-monitored computers reporting to a gateway server	2,000
Agentless Exception Monitored (AEM)-computers per dedicated management server	25,000
Agentless Exception Monitored (AEM)-computers per management group	100,000
Collective client monitored computers per management server	2,500
Management servers per agent for multihoming	4
Agentless-managed computers per management server	10
Agentless-managed computers per management group	60
Agent-managed and UNIX or Linux computers per management group	6,000 (with 50 open consoles); 15,000 (with 25 open consoles)
UNIX or Linux computers per dedicated management server	500
UNIX or Linux computers monitored per dedicated gateway server	100
Network devices managed by a resource pool with three or more management servers	1,000

Monitored item	Recommended limit
Network devices managed by two resource pools	2,000
Agents for Application Performance Monitoring (APM)	700
Applications for Application Performance Monitoring (APM)	400
URLs monitored per dedicated management server	3000
URLs monitored per dedicated management group	12,000
URLs monitored per agent	50

Operations Manager Feature Firewall Exceptions

Feature	Exception	Port and protocol	Configured by
Management server	• System Center Management service • System Center Data Access service • Operations Manager Connector Framework • Operations Manager Customer Experience Improvement • Operations Manager Application Error Monitoring	5723/TCP 5724/TCP 51905/TCP 51907/TCP 51906/TCP	Setup Setup Setup Setup Setup
Web console	Operations Manager web console	Selected web site port/TCP	Setup
Web console, http	World Wide Web	80/TCP	Windows Firewall

Feature	Exception	Port and protocol	Configured by
	Services, http		
Web console, https	Secure World Wide Web Service, https	443/TCP	Windows Firewall
Operational database	• SQL Server database server • If using a named instance, add.	1433/TCP 1434/UDP	Windows Firewall Windows Firewall
Operations Manager data warehouse database	• SQL Server database server • If using a named instance, add.	1433/TCP 1434/UDP	Windows Firewall Windows Firewall
Operations Manager Reporting	SQL Server Reporting Services	80/TCP	Windows Firewall
Agent, manual installation of MOMAgent.msi	System Center Management service	5723/TCP	Windows Firewall
Agent, push installation	• System Center Management service • File and Print Sharing • Remote Administration	5723/TCP 137/UDP, 138/UDP, 139/TCP, 445/TCP 135/TCP, 445/TCP	Windows Firewall Windows Firewall Windows Firewall
Agent, pending repair	• System Center Management service • File and Print Sharing • Remote Administration	5723/TCP 137/UPD, 138/UPD, 139/TCP, 445/TCP 135/TCP, 445/TCP	Windows Firewall Windows Firewall Windows Firewall
Agent, pending upgrade	• System Center Management service • File and Print Sharing • Remote Administration	5723/TCP 137/UDP, 138/UDP, 139/TCP, 445/TCP 135/TCP, 445/TCP	Windows Firewall Windows Firewall Windows Firewall

Feature	Exception	Port and protocol	Configured by
Gateway	System Center Management service	5723/TCP	Setup
Operations Manager Audit Collection Services database	• SQL Server • If using a named instance, add.	1433/TCP 1434/UDP	Windows Firewall Windows Firewall
Operations Manager Audit Collection Services Collector	ACS Collector Service	51909/TCP	Windows Firewall

Support for Languages in Addition to English

Operations Manager supports the following languages: English, German, French, Japanese, Spanish, Simplified Chinese, Russian, Italian, and Portuguese (Brazil).

Support for different languages

If your systems run a language other than English, you can install Operations Manager for that language. You also have the option of installing English Operations Manager for your management group.

For example, if you use a German version of a Windows operating system on all your servers, you can install German Operations Manager features for your entire management group. If you have a German version of a Windows operating system on all your servers, you can optionally install English Operations Manager features for your entire management group.

Agents for different languages

If you use an English management group, you can monitor any Windows Operating System Locale type.

If you use another language, you can monitor Windows operating systems for English and that language. For instance, if you use a German management group, you can monitor only English and German Windows operating systems.

Console for different languages

Operations Manager consoles are language independent. For example, you can use an Italian Operations Manager console to connect to a German management group.

Supported Network Monitoring Scenarios

Operations Manager supports monitoring of network devices that support Simple Network Management Protocol (SNMP). Port monitoring is available for devices that have implemented the interface MIB (RFC 2863) and MIB-II (RFC 1213) standards. In addition, peripheral monitoring, including processor and memory monitoring, is supported on a subset of devices. For more information, see System Center Operations Manager 2012: Network Devices with Extended Monitoring Capability.

Operations Manager can identify connected devices in a recursive discovery that use an IPv6 address; however, the initial device that is discovered must use an IPv4 address.

For more information about supported network devices, see Network Devices Supported for Discovery by Operations Manager 2012.

Application Performance Monitoring Requirements

To view Application Performance Monitoring event details, you must install the Operations Manager web console. For more information, see How to Install the Operations Manager Web Console.

Application Performance Monitoring requires the following software on the agent:

- .NET Framework 3.5, .NET Framework 3.5 SP1, .NET Framework 4, or .NET Framework 4.5.

  Note
  Applicatoin monitoring build on .NET Framework 2.0 is supported, but the computer must have .NET Framework 3.5 installed for some parts of the agent to work correctly.

- Internet Information Services (IIS) 7.0 or Internet Information Services (IIS) 8.0. Application monitoring on a Microsoft Failover IIS configuration is not supported. However, application monitoring using load balancing is supported instead.
- ISAPI and CGI Restrictions in IIS be enabled for ASP.NET 4.0. To enable this, select the web server in IIS Manager, and then double-click **ISAPI and CGI Restrictions**. Select **ASP.NET v4.0.30319**, and then click **Allow**.

Additionally, you must start the SQL Server Agent service and set the startup type to automatic. This only refers to the SQL instance where SQL Reporting Services is installed to run report subscriptions.

System Requirements: System Center 2012 SP1 - Operations Manager

This document provides information about the operating systems, hardware configurations, software requirements, installation combinations, and security configurations for Operations Manager in System Center 2012 Service Pack 1 (SP1). This document focuses on the system requirements, and it mentions unsupported configurations only when necessary. If operating systems, hardware configurations, software requirements, installation combinations, and security configurations are not presented here, they have not been tested and are not supported.

Note
For system requirements across all components of System Center 2012 SP1, see **System Requirements for System Center 2012 SP1**.

The Prerequisites checker is no longer a separate option in Setup. However, you can begin the installation process to check the hardware and software prerequisites, and then cancel installation after the required prerequisites have been determined.

We recommend that you also review the key concepts of Operations Manager. Documents to review include the following:

- Release Notes for Operations Manager in System Center 2012 SP1 identifies any changes that could affect planning for a new deployment of Operations Manager in System Center 2012 SP1.
- Deploying System Center 2012 - Operations Manager provides detailed information about the security-related features and settings in Operations Manager that can affect your deployment.

This document contains the following sections:

- Operations Manager Virtualization Support
- Minimum Screen Resolution Requirements
- Minimum Hardware Requirements
- Minimum Software Requirements
- Requirements by Feature
  - Management Server
  - Operations Console
  - Web Console
  - Operational Database
  - Operations Manager Agent – Windows-Based Computers
  - Operations Manager Agent – UNIX- or Linux Computers
  - Operations Manager Reporting
  - Operations Manager Data Warehouse
  - Operations Manager Gateway Server
- Supported Firewall Scenarios
- Minimum Network Connectivity Speeds
- Supported Cluster Configurations
- Monitored Item Capacity
- Operations Manager Feature Firewall Exceptions
- Support for Languages in Addition to English
- Supported Network Monitoring Scenarios
- Application Performance Monitoring Requirements

Operations Manager Virtualization Support

Microsoft supports running all Operations Manager server features in any physical or virtual environment that meets the minimum requirements that are stated in this document. However, for performance reasons, we recommend that you store the operational database and data warehouse database on a directly attached physical hard drive, and not on a virtual disk. Specifically, virtual computers that are running any Operations Manager server feature must not use any functionality that does not immediately commit all activity on the virtual computer to the virtual hard drive. This includes making use of point-in-time snapshots and writing changes to a

temporary virtual hard drive. This is true for every virtualization technology that is used with Operations Manager.

Minimum Screen Resolution Requirements

Operations Manager is optimized for screen resolutions of 1280 x 1024 or larger. The minimum supported screen resolution is 1024 x 768.

Minimum Hardware Requirements

Use the Operations Manager Sizing Helper to determine hardware requirements for each Operations Manager server feature. If you want to install more than one feature on the same computer, use the higher of the recommended hardware requirements for any of the combined features.

Supported Processors, Memory, and Disk Space

Note

Operations Manager does not support installing the 32-bit agent on a 64-bit operating system. Operations Manager provides native support for x86-based computers for agents and consoles, and x64-based computers for all server features and support for agents on computers with 64-bit Itanium processors.

Minimum Software Requirements

Operations Manager server features require a supported operating system. For a list of the supported operating systems for each server feature, see the **Requirements by Feature** section in this document.

Installing Operations Manager in System Center 2012 SP1 on Windows Server 2012 Core requires Windows 32-bit on Windows 64-bit (WoW64) support, .NET 4.5, Windows PowerShell 3.0, and **Server-Gui-Mgmt-Infra** (the Minimal Server Interface). If you attempt to install Operations Manager without WoW64 support installed, the bootstrapper will present an error message indicating the side-by-side configuration is incorrect.

Important

During the initial installation of the operational database, only use Windows Authentication on the SQL server that hosts the Operations Manager operational database. Do not use Mixed Mode (Windows Authentication and SQL Server Authentication) because using SQL Server Authentication mode during the initial installation of the operational database can cause issues. Although enabling Mixed Mode security is possible on the SQL Server hosting the Operations Manager operational database, it is not supported as all contact with the database is accomplished using Windows accounts only.

We recommend that you check for updates and hotfixes for Microsoft SQL Server. Note the following database considerations for Operations Manager:

- SQL Server 2008 R2 and SQL Server 2012 are available in both Standard and Enterprise editions. Operations Manager will function with both editions.
- Operations Manager does not support hosting its databases or SQL Server Reporting Services on a 32-bit edition of SQL Server.
- Using a different version of SQL Server for different Operations Manager features is not supported. The same version should be used for all features.
- SQL Server collation settings for all databases must be one of the following: SQL_Latin1_General_CP1_CI_AS, French_CI_AS, Cyrillic_General_CI_AS, Chinese_PRC_CI_AS, Japanese_CI_AS, Traditional_Spanish_CI_AS, or Latin1_General_CI_AS. No other collation settings are supported.

  The Operations Manager data warehouse installer will always install the data warehouse with SQL_Latin1_General_CP1_CI_AS regardless of the SQL Server collation. Until this issue is resolved, always install the Operations Manager data warehouse on a SQL Server with the SQL_Latin1_General_CP1_CI_AS collation. There are some compatibility issues when the Temp database on the data warehouse SQL Server instance is anything other than SQL_Latin1_General_CP1_CI_AS and the data warehouse database is SQL_Latin1_General_CP1_CI_AS. For more information about SQL Server collation setting impact and installation requirements in System Center 2012 Service Pack 1 (SP1) between Operations Manager and Service Manager, see Clarification on SQL Server Collation Requirements for System Center 2012.

- The SQL Server Agent service must be started, and the startup type must be set to automatic.
- Side-by-side installation of System Center Operations Manager 2007 R2 reporting and Operations Manager in System Center 2012 SP1 reporting on the same server is not supported.
- The db_owner role for the operational database must be a domain account. If you set the SQL Server Authentication to Mixed mode, and then try to add a local SQL Server login on the operational database, the Data Access service will not be able to start. For information about how to resolve the issue, see System Center Data Access Service Start Up Failure Due to SQL Configuration Change
- If you plan to use the Network Monitoring features of System Center 2012 – Operations Manager, you should move the tempdb database to a separate disk that has multiple spindles. For more information, see tempdb Database.

If you want to install more than one Operations Manager feature on the same computer, you must install the prerequisite software for all of the combined features.

Requirements by Feature

Management Server

- Disk space: %SYSTEMDRIVE% requires at least 1024 MB free hard disk space.

- Server Operating System: must be Windows Server 2008 R2 SP1, Windows Server 2012, or Windows Server 2012 Core Installation.
- Processor Architecture: must be x64.
- Windows PowerShell version: Windows PowerShell version 2.0, or Windows PowerShell version 3.0.
- Windows Remote Management: Windows Remote Management must be enabled for the management server.
- .NET Framework 4 is required. For more information, see the following document:
  - .NET Framework 4 redistributable package

Operations Console

- Microsoft Report Viewer 2010 SP1 Redistributable Package
- Disk space: %SYSTEMDRIVE% requires at least 512 MB free hard disk space.
- File system: %SYSTEMDRIVE% must be formatted with the NTFS file system.
- Server Operating System: must be Windows 7, Windows 8, Windows Server 2008 R2 SP1, or Windows Server 2012.
- Processor Architecture: must be x64 for servers and x64 or x86 for a client computer.
- Windows Installer version: at least Windows Installer 3.1.
- Windows PowerShell version: Windows PowerShell version 2.0. Windows PowerShell version 3.0 is required to use Windows PowerShell cmdlets for administration of UNIX and Linux computers.
- .NET Framework 4 is required. For more information, see the following document:
  - .NET Framework 4 redistributable package

Web Console

- Operating System: Windows Server 2008 R2 SP1, or Windows Server 2012.
- Processor Architecture: must be x64.
- Web browsers: Internet Explorer 8, Internet Explorer 9, Internet Explorer 10, Silverlight 5.0
- Internet Information Services (IIS) 7.5 and later versions, with the IIS Management Console and the following role services installed:
  - Static Content
  - Default Document
  - Directory Browsing
  - HTTP Errors
  - HTTP Logging
  - Request Monitor
  - Request Filtering
  - Static Content Compression
  - Web Server (IIS) Support

    - IIS 6 Metabase Compatibility
    - ASP.NET (both the 2.0 and 4.0 versions of ASP.NET are required.)
    - Windows Authentication
- Selected website for web console: requires a configured http or https binding.

  Important
  Installing the web console on a computer that has Microsoft SharePoint installed is not supported.
- The System Center 2012 Service Pack 1 (SP1) SharePoint Dashboard Viewer Web Part works on SharePoint 2010 and SharePoint 2013 and is supported. However, it does not work on Office 365 SharePoint and is not supported.
- .NET Framework 4 is required for Setup to run. For more information, see the following documents:
    - .NET Framework 4 redistributable package

Note
Installation of the web console requires that ISAPI and CGI Restrictions in IIS are enabled for ASP.NET 4. To enable this, select the web server in IIS Manager, and then double-click **ISAPI and CGI Restrictions**. Select **ASP.NET v4.0.30319**, and then click **Allow**.

Important
You must install IIS before installing .NET Framework 4. If you installed IIS after installing .NET Framework 4, you must register ASP.NET 4.0 with IIS. Open a Command prompt window by using the **Run As Administrator** option, and then run the following command:

%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -r

Operational Database

Disk space: The operational database must have at least 1024 MB free disk space. This is enforced at the time of database creation, and it will likely grow significantly. For information about SQL Server Planning, see Installing SQL Server 2008 or Installing SQL Server 2008 R2.

File system: %SYSTEMDRIVE% must be formatted with the NTFS file system.

Operating System: Windows Server 2008 R2 SP1, Windows Server 2012, or Windows Server 2012 Core Installation.

Processor Architecture: x64.

Windows Installer version: at least Windows Installer 3.1.

Microsoft SQL Server: SQL Server SQL 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, SQL Server 2012 SP1.

SQL Server Full Text Search is required.

.NET Framework 4 is required. For more information, see the following document:

- .NET Framework 4 redistributable package

Operations Manager Agent – Windows-Based Computers

- File system: %SYSTEMDRIVE% must be formatted with the NTFS file system.
- Operating Systems: Windows Server 2003 SP2, Windows Server 2008 SP2, Windows Server 2008 R2, Windows Server 2008 R2 SP1, Windows Server 2012, Windows XP Professional x64 Edition SP2, Windows XP Professional SP3, Windows Vista SP2, Windows 7, POSReady, Windows XP Embedded Standard, Windows XP Embedded Enterprise, Windows XP Embedded POSReady, Windows 7 Professional for Embedded Systems, Windows 7 Ultimate for Embedded Systems, Windows 8 Pro or Windows 8 Enterprise.
- Processor Architectures: x64, x86, or IA64.
- Windows Installer version: at least Windows Installer 3.1.
- Microsoft Core XML Services (MSXML) version: Microsoft Core XML Services 6.0 is required for the Operations Manager agent.
- Windows PowerShell version: Windows PowerShell version 2.0, or Windows PowerShell version 3.0.

Note

Windows PowerShell is required for agents that will be monitored by a management pack that uses Windows PowerShell scripts.

Operations Manager Agent – UNIX- or Linux Computers

Supported operating systems:

- CentOS 5 and 6 (x86/x64)
- Debian GNU/Linux 5, 6, and 7 (x86/x64)
- HP-UX 11i v2 and v3 (PA-RISC and IA64)
- IBM AIX 5.3, AIX 6.1 (POWER), and AIX 7.1 (POWER)
- Novell SUSE Linux Enterprise Server 9 (x86), 10 SP1 (x86/x64), and 11 (x86/x64)
- Oracle Solaris 9 (SPARC), Solaris 10 (SPARC and x86), and Solaris 11 (SPARC and x86)
- Oracle Linux 5 and 6 (x86/x64)
- Red Hat Enterprise Linux 4, 5, and 6 (x86/x64)
- Ubuntu Linux Server 10.04 and 12.04 (x86/x64)

Operations Manager Reporting

- Disk space: The %SYSTEMDRIVE% requires at least 1024 MB free hard disk space.
- Operating System: Windows Server 2008 R2 SP1, Windows Server 2012, or Windows Server 2012 Core Installation.
- Processor Architecture: x64.
- Microsoft SQL Server: SQL Server SQL 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, SQL Server 2012 SP1.

- The Remote Registry service must be enabled and started.
- Microsoft SQL Server Reporting Services: SQL Server SQL 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, SQL Server 2012 SP1.
- System Center 2012 – Operations Manager supports SQL Server Reporting Services in native mode only; do not use SharePoint integrated mode.
- .NET Framework 4 is required. For more information, see the following document:
  - .NET Framework 4 redistributable package

Operations Manager Data Warehouse

- Disk space: The data warehouse database must have at least 1024 MB free hard disk space. This is enforced at the time of database creation, and the required disk space will likely grow significantly. For information about requirements in SQL Server Planning, see Installing SQL Server 2008 or Installing SQL Server 2008 R2.
- File system: %SYSTEMDRIVE% must be formatted with the NTFS file system.
- Operating System: Windows Server 2008 R2 SP1, Windows Server 2012, or Windows Server 2012 Core Installation.
- Processor Architecture: x64.
- Windows Installer version: at least Windows Installer 3.1.
- Microsoft SQL Server: SQL Server SQL 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, SQL Server 2012 SP1.
- SQL Server Full Text Search is required.
- .NET Framework 4 is required for Setup to run. For more information, see the following document:
  - .NET Framework 4 redistributable package

Operations Manager Gateway Server

- Disk space: %SYSTEMDRIVE% requires at least 1024 MB free hard disk space.
- Server Operating System: must be Windows Server 2008 R2 SP1, Windows Server 2012, or Windows Server 2012 Core Installation.
- Processor Architecture: must be x64.
- Windows PowerShell version: Windows PowerShell version 2.0, or Windows PowerShell version 3.0.
- Microsoft Core XML Services (MSXML) version: Microsoft Core XML Services 6.0 is required for the management server.
- .NET Framework 4 is required if the Gateway server manages UNIX/Linux agents or network devices.

Supported Firewall Scenarios

The following table shows Operations Manager feature interaction across a firewall, including information about the ports that are used for communication between the features, which direction to open the inbound port, and whether the port number can be changed.

Firewall Scenarios for Operations Manager in System Center 2012 SP1

Operations Manager Feature A	Port number and direction	Feature B	Configurable	Note
Management server	1433 --->	Operational database	Yes (Setup)	
Management server	1434 UDP < ---	Operational database	No	If the operational database is installed on a named instance of SQL Server SQL 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1 such as in a cluster, and the Windows Firewall is enabled on the management server, you have to also open UDP 1434 inbound on the management server.
Management server	1433 --->	Operational database	Yes (Setup)	
Management server	5723, 5724 --->	Management server	No	Port 5724 must be open to install this feature and can be closed after this feature has been installed.
Management server	1433 -->	Reporting data warehouse	No	

Operations Manager Feature A	Port number and direction	Feature B	Configurable	Note
Management server	1433 --->	Reporting data warehouse	No	
Reporting server	5723, 5724 -->	Management server	No	Port 5724 must be open to install this feature and can be closed after this feature has been installed.
Operations console	5724 --->	Management server	No	
Connector Framework source	51905 --->	Management server	No	
Web console server	Selected web site port --->	Management server	No	
Web console (for Application Diagnostics	1433, 1434 -->	Operational database	Yes (Setup)	
Web console (for Application Advisor)	1433, 1434 -->	Data warehouse	Yes (Setup)	
Web console (for Application Advisor)	80 --->	SQL Server Reporting Services	No	
Web console browser	80, 443 --->	web console server	Yes (IIS Admin)	Default for HTTP or SSL. For either Network Authentication or Mixed Authentication, an account name and password can be sent as part of the request. We recommend you use SSL.

Operations Manager Feature A	Port number and direction	Feature B	Configurable	Note
Agent installed by using MOMAgent.msi	5723 --->	Management server	Yes (Setup)	
Agent installed by using MOMAgent.msi	5723 --->	Management server	Yes (Setup)	
Agent installed by using MOMAgent.msi	5723 --->	Gateway server	Yes (Setup)	
Gateway server	5723 --->	Management server	Yes (Setup)	
Agent (Audit Collection Services (ACS) forwarder)	51909 --->	Management server Audit Collection Services (ACS) Collector	Yes (Registry)	
Agentless Exception Monitoring data from client	51906 --->	Management server Agentless Exception Monitoring (AEM) file share	Yes (Client Monitoring Wizard)	
Customer Experience Improvement Program data from client	51907 --->	Management server (Customer Experience Improvement Program) Endpoint	Yes (Client Monitoring Wizard)	
Operations console (reports)	80 --->	SQL Server Reporting Services	No	The Operations console uses port 80 to connect to the SQL Server Reporting Services website.
Reporting server	1433 --->	Reporting data warehouse	Yes	
Management server (Audit Collection Services Collector)	1433 --->	Audit Collection Services (ACS) database	Yes	

Operations Manager Feature A	Port number and direction	Feature B	Configurable	Note
Management Server	161, 162 <--->	Network device	Yes	All firewalls between the management servers in the resource pool and the network devices need to allow SNMP (UDP) and ICMP bi-directionally, and ports 161 and 162 need to be open bi-directionally. This includes Windows Firewall on the management server itself. If your network devices are using a port other than 161 and 162, you need to open bi-directional UDP traffic on these ports as well.
Management server or gateway server	1270 --->	UNIX or Linux computer	No	
Management server or gateway server	22 --->	UNIX or Linux computer	Yes	

In the preceding table, if SQL Server SQL 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1 is installed by using a default instance, the port number is 1433. If SQL Server is installed with a named instance, it is probably using a dynamic port. To identify the port, do the following:

1. Run SQL Server Configuration Manager.
2. Open SQL Server Network Configuration.
3. Open Protocols for INSTANCE1 (or the instance that is running under it).
4. Open TCP/IP.

5. Click **IP Addresses**.
6. The port is under IPAll (usually the TCP Dynamic Ports).

Minimum Network Connectivity Speeds

Operations Manager requires the following minimum network connectivity speeds between the specified features.

Feature A	Feature B	Minimum requirement
Management server	Agent	64 Kbps
Management server	Agentless	1024 Kbps
Management server	Database	256 Kbps
Management server	Console	768 Kbps
Management server	Management server	64 Kbps
Management server	Data warehouse database	768 Kbps
Management server	Reporting server	256 Kbps
Management server	Gateway server	64 Kbps
Local management group	Connected management group (tiered)	1024 Kbps
Web console server	web console	128 Kbps
Reporting Data Warehouse	Reporting server	1024 Kbps
Console	Reporting server	768 Kbps
Audit collector	Audit database	768 Kbps

Supported Cluster Configurations

Operations Manager supports the clustering configurations for Operations Manager features as shown in the following table:

Important
Clustering of management servers is not supported in System Center 2012 Service Pack 1 (SP1), Operations Manager.

Only Cluster service quorum node clusters are supported. Multisite clusters (geographically dispersed clusters) are supported for all Operations Manager cluster roles. You can use replication technology to help provide high availability for data in Operations Manager, but the latency of communications between components introduce risks to data replication and might introduce failover issues. We recommend that you use synchronous mirroring of data disks

between sites. Synchronous mirroring means that the data is fully synchronized across all sites and ensures the correct behavior of applications in the event of failover across sites.

Important
Microsoft is not obligated to release a hotfix on any Operations Manager issue that cannot be reproduced in a non-multisite cluster environment. If an analysis determines that non-Microsoft components in the configuration are causing the issue, the customer must work with the appropriate vendor for those components.

Server Feature	Cluster	Notes
Operations Manager Operational database	Single Active-Passive cluster	Other Operations Manager features must not be installed on the cluster or nodes of the cluster.
Operations Manager Reporting data warehouse	Single Active-Passive cluster	Other Operations Manager features must not be installed on the cluster or nodes of the cluster.
Audit Collection Services (ACS) database	Single Active-Passive cluster	Other Operations Manager features must not be installed on the cluster or nodes of the cluster.

Supported, But Not Recommended Cluster Configurations

Operations Manager supports the following clustering configurations for Operations Manager server roles, as shown in the following table; however, because of a potential performance effect on your computer running SQL Server, these configurations are not recommended:

Server Feature	Cluster	Notes
Operations Manager operational database and Operations Manager Reporting data warehouse.	Active-Active cluster where the operational database is installed on one node of the cluster and the Reporting data warehouse is installed on the other node of the cluster.	There might be some performance issues with SQL Server in this configuration.
Operations Manager operational database, Reporting data warehouse, and Audit Collection Services	Single Active-Passive or Active-Active cluster where all three components are on a single cluster.	There might be some performance issues with SQL Server in this configuration.

Server Feature	Cluster	Notes
(ACS) database.		
Operations Manager operational database and Audit Collection Services database.	Single Active-Passive cluster where both components are on a single cluster.	There might be some performance issues with SQL Server in this configuration.
Operations Manager operational database and Reporting data warehouse.	Single Active-Passive cluster where both components are on a single cluster.	There might be some performance issues with SQL Server in this configuration.
Reporting data warehouse and Audit Collection Services database.	Single Active-Passive cluster where both components are on a single cluster.	There might be some performance issues with SQL Server in this configuration.

Monitored Item Capacity

Operations Manager supports the following number of monitored items.

Monitored item	Recommended limit
Simultaneous Operations consoles	50
Agent-monitored computers reporting to a management server	3,000
Agent-monitored computers reporting to a gateway server	2,000
Agentless Exception Monitored (AEM)-computers per dedicated management server	25,000
Agentless Exception Monitored (AEM)-computers per management group	100,000
Collective client monitored computers per management server	2,500
Management servers per agent for multihoming	4
Agentless-managed computers per management server	10
Agentless-managed computers per management group	60
Agent-managed and UNIX or Linux computers	6,000 (with 50 open consoles); 15,000 (with 25

Monitored item	Recommended limit
per management group	open consoles)
UNIX or Linux computers per dedicated management server	500
UNIX or Linux computers monitored per dedicated gateway server	100
Network devices managed by a resource pool with three or more management servers	1,000
Network devices managed by two resource pools	2,000
Agents for Application Performance Monitoring (APM)	700
Applications for Application Performance Monitoring (APM)	400
URLs monitored per dedicated management server	3000
URLs monitored per dedicated management group	12,000
URLs monitored per agent	50

Operations Manager Feature Firewall Exceptions

Feature	Exception	Port and protocol	Configured by
Management server	• System Center Management service • System Center Data Access service • Operations Manager Connector Framework • Operations Manager Customer Experience	5723/TCP 5724/TCP 51905/TCP 51907/TCP 51906/TCP	Setup Setup Setup Setup Setup

Feature	Exception	Port and protocol	Configured by
	Improvement • Operations Manager Application Error Monitoring		
Web console	Operations Manager web console	Selected web site port/TCP	Setup
Web console, http	World Wide Web Services, http	80/TCP	Windows Firewall
Web console, https	Secure World Wide Web Service, https	443/TCP	Windows Firewall
Operational database	• SQL Server database server • If using a named instance, add.	1433/TCP 1434/UDP	Windows Firewall Windows Firewall
Operations Manager data warehouse database	• SQL Server database server • If using a named instance, add.	1433/TCP 1434/UDP	Windows Firewall Windows Firewall
Operations Manager Reporting	SQL Server Reporting Services	80/TCP	Windows Firewall
Agent, manual installation of MOMAgent.msi	System Center Management service	5723/TCP	Windows Firewall
Agent, push installation	• System Center Management service • File and Print Sharing • Remote Administration	5723/TCP 137/UDP, 138/UDP, 139/TCP, 445/TCP 135/TCP, 445/TCP	Windows Firewall Windows Firewall Windows Firewall
Agent, pending repair	• System Center Management service • File and Print Sharing • Remote	5723/TCP 137/UPD, 138/UPD, 139/TCP, 445/TCP 135/TCP, 445/TCP	Windows Firewall Windows Firewall Windows Firewall

Feature	Exception	Port and protocol	Configured by
	Administration		
Agent, pending upgrade	• System Center Management service • File and Print Sharing • Remote Administration	5723/TCP 137/UDP, 138/UDP, 139/TCP, 445/TCP 135/TCP, 445/TCP	Windows Firewall Windows Firewall Windows Firewall
Gateway	System Center Management service	5723/TCP	Setup
Operations Manager Audit Collection Services database	• SQL Server • If using a named instance, add.	1433/TCP 1434/UDP	Windows Firewall Windows Firewall
Operations Manager Audit Collection Services Collector	ACS Collector Service	51909/TCP	Windows Firewall

Support for Languages in Addition to English

Operations Manager supports the following languages: English, Chinese-Hong Kong, Chinese-Traditional, Czech, Dutch, German, French, Hungarian, Italian, Japanese, Korean, Polish, Portuguese (Brazil), Portuguese (Portugal), Russian, Simplified Chinese, Spanish, Swedish, and Turkish.

Support for different languages

If your systems run a language other than English, you can install Operations Manager for that language. You also have the option of installing English Operations Manager for your management group.

For example, if you use a German version of a Windows operating system on all your servers, you can install German Operations Manager features for your entire management group. If you have a German version of a Windows operating system on all your servers, you can optionally install English Operations Manager features for your entire management group.

Agents for different languages

If you use an English management group, you can monitor any Windows Operating System Locale type.

If you use another language, you can monitor Windows operating systems for English and that language. For instance, if you use a German management group, you can monitor only English and German Windows operating systems.

Console for different languages

Operations Manager consoles are language independent. For example, you can use an Italian Operations Manager console to connect to a German management group.

Supported Network Monitoring Scenarios

Operations Manager supports monitoring of network devices that support Simple Network Management Protocol (SNMP). Port monitoring is available for devices that have implemented the interface MIB (RFC 2863) and MIB-II (RFC 1213) standards. In addition, peripheral monitoring, including processor and memory monitoring, is supported on a subset of devices. For more information, see System Center Operations Manager 2012: Network Devices with Extended Monitoring Capability.

Operations Manager can identify connected devices in a recursive discovery that use an IPv6 address; however, the initial device that is discovered must use an IPv4 address.

For more information about supported network devices, see Network Devices Supported for Discovery by Operations Manager 2012.

Application Performance Monitoring Requirements

To view Application Performance Monitoring event details, you must install the Operations Manager web console. For more information, see How to Install the Operations Manager Web Console.

Application Performance Monitoring requires the following software:

- .NET Framework 2.0, .NET Framework 3.5, .NET Framework 3.5 SP1, .NET Framework 4, or .NET Framework 4.5.
- Internet Information Services (IIS) 7.0. Application monitoring on a clustered IIS configuration is not supported.
- ISAPI and CGI Restrictions in IIS be enabled for ASP.NET 4.0. To enable this, select the web server in IIS Manager, and then double-click **ISAPI and CGI Restrictions**. Select **ASP.NET v4.0.30319**, and then click **Allow**.

Additionally, you must start the SQL Server Agent service and set the startup type to automatic.

System Requirements: System Center 2012 - Operations Manager

This document provides information about the operating systems, hardware configurations, software requirements, installation combinations, and security configurations for System Center 2012 – Operations Manager. This document focuses on the system requirements and only mentions unsupported configurations when necessary. If operating systems, hardware configurations, software requirements, installation combinations, and security configurations are not presented here, they have not been tested and are not supported.

The Prerequisites checker is no longer a separate option in Setup. However, you can begin the installation process to check the hardware and software prerequisites, and then cancel installation after the required prerequisites have been determined.

We recommend that you also review the key concepts of Operations Manager. Areas to review include the following documents:

- Release Notes for System Center 2012 - Operations Manager identify any changes that could affect planning for a new deployment of System Center 2012 – Operations Manager.
- TheSystem Center 2012 - Operations Manager Deployment Guide provides detailed information about the security-related features and settings in Operations Manager that can affect your deployment.

This document contains the following sections:

- Operations Manager Virtualization Support
- Minimum Screen Resolution Requirements
- Minimum Hardware Requirements
- Minimum Software Requirements
- Requirements by Feature
  - Management Server
  - Operations Console
  - Web Console
  - Operational Database
  - Operations Manager Agent – Windows-Based Computers
  - Operations Manager Agent – UNIX- or Linux Computers
  - Operations Manager Reporting
  - Operations Manager Data Warehouse
  - Operations Manager Gateway Server
- Supported Firewall Scenarios
- Minimum Network Connectivity Speeds
- Supported Cluster Configurations
- Monitored Item Capacity
- Operations Manager Feature Firewall Exceptions
- Support for Languages in Addition to English
- Supported Network Monitoring Scenarios
- Application Performance Monitoring Requirements

Operations Manager Virtualization Support

Microsoft supports running all System Center 2012 – Operations Manager server features in any physical or virtual environment that meets the minimum requirements that are stated in this document. However, for performance reasons, we recommend that you store the operational database and data warehouse database on a directly attached physical hard drive, and not on a

virtual disk. Specifically, virtual computers that are running any Operations Manager server feature must not use any functionality that does not immediately commit all activity on the virtual computer to the virtual hard drive. This includes making use of point-in-time snapshots and writing changes to a temporary virtual hard drive. This is true for every virtualization technology that is used with Operations Manager.

Minimum Screen Resolution Requirements

Operations Manager is optimized for screen resolutions of 1280 x 1024 or larger. The minimum supported screen resolution is 1024 x 768.

Minimum Hardware Requirements

Use the Operations Manager Sizing Helper to determine hardware requirements for each System Center 2012 – Operations Manager server feature. If you want to install more than one feature on the same computer, use the higher of the recommended hardware requirements for any of the combined features.

Supported Processors, Memory, and Disk Space

Note

Operations Manager does not support installing the 32-bit agent on a 64-bit operating system. Operations Manager provides native support for x86-based computers for agents and consoles, and x64-based computers for all server features and support for agents on computers with 64-bit Itanium processors.

Minimum Software Requirements

Operations Manager server features require a supported operating system. For a list of the supported operating systems for each server feature, see the **Requirements by Feature** section in this document.

Important

During the initial installation of the operational database, only use Windows Authentication on the SQL server that hosts the Operations Manager operational database. Do not use Mixed Mode (Windows Authentication and SQL Server Authentication) because using SQL Server Authentication mode during the initial installation of the operational database can cause issues. Although enabling Mixed Mode security is possible on the SQL Server hosting the Operations Manager operational database, it is not supported as all contact with the database is accomplished using Windows accounts only.

We recommend that you check for updates and hotfixes for SQL Server. Note the following database considerations for Operations Manager:

- SQL Server 2008 is available in both Standard and Enterprise editions. Operations Manager will function with both editions.

- Operations Manager does not support hosting its databases or SQL Server Reporting Services on a 32-bit edition of SQL Server.
- Using a different version of SQL Server for different Operations Manager features is not supported. The same version should be used for all features.
- SQL Server collation settings for all databases must be one of the following: SQL_Latin1_General_CP1_CI_AS, French_CI_AS, Cyrillic_General_CI_AS, Chinese_PRC_CI_AS, Japanese_CI_AS, Traditional_Spanish_CI_AS, or Latin1_General_CI_AS. No other collation settings are supported.
- The SQL Server Agent service must be started, and the startup type must be set to automatic.
- Side-by-side installation of System Center Operations Manager 2007 R2 Reporting and System Center 2012 – Operations Manager Reporting on the same server is not supported.
- The db_owner role for the operational database must be a domain account. If you set the SQL Server Authentication to Mixed mode, and then try to add a local SQL Server login on the operational database, the Data Access service will not be able to start. For information about how to resolve the issue, see System Center Data Access Service Start Up Failure Due to SQL Configuration Change
- If you plan to use the Network Monitoring features of System Center 2012 – Operations Manager, you should move the tempdb database to a separate disk that has multiple spindles. For more information, see tempdb Database.

If you want to install more than one Operations Manager feature on the same computer, you must install the prerequisite software for all of the combined features.

Requirements by Feature

Management Server

- Disk space: %SYSTEMDRIVE% requires at least 1024 MB free hard disk space.
- Server Operating System: must be Windows Server 2008 R2 SP1.
- Processor Architecture: must be x64.
- Windows PowerShell version: Windows PowerShell version 2.0.
- Windows Remote Management: Windows Remote Management must be enabled for the management server.
- Microsoft Core XML Services (MSXML) version: Microsoft Core XML Services 6.0 is required for the management server.
- Both .NET Framework 3.5 Service Pack 1 (SP1) and .NET Framework 4 are required. For more information, see the following documents:
  - .NET Framework 3.5 SP1 redistributable package
  - .NET Framework 4 redistributable package

Operations Console

- Microsoft Report Viewer 2010 Redistributable Package

- Microsoft .NET Framework 3.5 SP1 hotfix
- Disk space: %SYSTEMDRIVE% requires at least 512 MB free hard disk space.
- File system: %SYSTEMDRIVE% must be formatted with the NTFS file system.
- Server Operating System: must be Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2008 R2 SP1.
- Processor Architecture: must be x64 for servers and x64 or x86 for a client computer.
- Windows Installer version: at least Windows Installer 3.1.
- Windows PowerShell version: Windows PowerShell version 2.0. Windows PowerShell version 3.0 is required to use Windows PowerShell cmdlets for administration of UNIX and Linux computers.
- Both .NET Framework 3.5 SP1 and .NET Framework 4 are required. For more information, see the following documents:
  - .NET Framework 3.5 SP1 redistributable package
  - .NET Framework 4 redistributable package

Web Console

- Operating System: Windows Server 2008 R2 SP1.
- Processor Architecture: must be x64.
- Web browsers: Internet Explorer 7, Internet Explorer 8, Internet Explorer 9
- Internet Information Services (IIS) 7.5 and later versions, with the IIS Management Console and the following role services installed:
  - Static Content
  - Default Document
  - Directory Browsing
  - HTTP Errors
  - HTTP Logging
  - Request Monitor
  - Request Filtering
  - Static Content Compression
  - Web Server (IIS) Support
  - IIS 6 Metabase Compatibility
  - ASP.NET
  - Windows Authentication
- Selected website for web console: requires a configured http or https binding.

  Warning
  Installing the web console on a computer that has SharePoint installed is not supported.
- Both .NET Framework 3.5 SP1 and .NET Framework 4 are required for Setup to run. For more information, see the following documents:

- .NET Framework 3.5 SP1 redistributable package
- .NET Framework 4 redistributable package

Note
Installation of the web console requires that ISAPI and CGI Restrictions in IIS are enabled for ASP.NET 4. To enable this, select the web server in IIS Manager, and then double-click **ISAPI and CGI Restrictions**. Select **ASP.NET v4.0.30319**, and then click **Allow**.

Important
You must install IIS before installing .NET Framework 4. If you installed IIS after installing .NET Framework 4, you must register ASP.NET 4.0 with IIS. Open a Command prompt window by using the **Run As Administrator** option, and then run the following command:

%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -r

Operational Database

Disk space: The operational database must have at least 1024 MB free disk space. This is enforced at the time of database creation, and it will likely grow significantly. For information about SQL Server Planning, see Installing SQL Server 2008 or Installing SQL Server 2008 R2.

File system: %SYSTEMDRIVE% must be formatted with the NTFS file system.

Operating System: Windows Server 2008 SP2 or Windows Server 2008 R2 SP1.

Processor Architecture: x64.

Windows Installer version: at least Windows Installer 3.1.

Microsoft SQL Server: SQL Server 2008 SP1, SQL Server 2008 SP2, SQL Server 2008 SP3, SQL Server 2008 R2, SQL Server 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1.

SQL Server Full Text Search is required.

Both .NET Framework 3.5 SP1 and .NET Framework 4 are required. For more information, see the following documents:

- .NET Framework 3.5 SP1 redistributable package
- .NET Framework 4 redistributable package

Operations Manager Agent – Windows-Based Computers

- File system: %SYSTEMDRIVE% must be formatted with the NTFS file system.
- Operating Systems: Windows Server 2003 SP2, Windows Server 2008 SP2, Windows Server 2008 R2, Windows Server 2008 R2 SP1, Windows Server 2012, Windows XP Professional x64 Edition SP2, Windows XP Professional SP3, or Windows Vista SP2, or Windows 7, POSReady, Windows XP Embedded Standard, orWindows XP Embedded Enterprise, or Windows XP Embedded POSReady, Windows 7 Professional for Embedded Systems, orWindows 7 Ultimate for Embedded Systems.

- Processor Architectures: x64, x86, or IA64.
- Windows Installer version: at least Windows Installer 3.1.
- Microsoft Core XML Services (MSXML) version: Microsoft Core XML Services 6.0 is required for the Operations Manager agent.
- Windows PowerShell version: Windows PowerShell version 2.0.

Note

Windows PowerShell is required for agents that will be monitored by a management pack that uses PowerShell scripts.

Operations Manager Agent – UNIX- or Linux Computers

Supported operating systems:

- HP-UX 11i v2 and v3 (PA-RISC and IA64)
- Oracle Solaris 9 (SPARC), Solaris 10 (SPARC and x86), and Solaris 11 (SPARC and x86)
- Red Hat Enterprise Linux 4, 5, and 6 (x86/x64)
- Novell SUSE Linux Enterprise Server 9 (x86), 10 SP1 (x86/x64), and 11 (x86/x64)
- IBM AIX 5.3, AIX 6.1 (POWER), and AIX 7.1 (POWER)

Operations Manager Reporting

- Disk space: The %SYSTEMDRIVE% requires at least 1024 MB free hard disk space.
- Operating System: Windows Server 2008 R2 SP1.
- Processor Architecture: x64.
- Microsoft SQL Server: SQL Server 2008 SP1, SQL Server 2008 SP2, SQL Server 2008 SP3, SQL Server 2008 R2, SQL Server 2008 R2 SP1, or SQL Server 2008 R2 SP2.
- The Remote Registry service must be enabled and started.
- Microsoft SQL Server Reporting Services: Microsoft SQL Server: SQL Server 2008 SP1, SQL Server 2008 SP2, SQL Server 2008 SP3, SQL Server 2008 R2, SQL Server 2008 R2 SP1, or SQL Server 2008 R2 SP2.
- System Center 2012 – Operations Manager supports SQL Server Reporting Services in native mode only; do not use SharePoint integrated mode.
- Both .NET Framework 3.5 SP1 and .NET Framework 4 are required. For more information, see the following documents:
  - .NET Framework 3.5 SP1 redistributable package
  - .NET Framework 4 redistributable package

Operations Manager Data Warehouse

- Disk space: The data warehouse database must have at least 1024 MB free hard disk space. This is enforced at the time of database creation, and the required disk space will likely grow significantly. For information about requirements in SQL Server Planning, see Installing SQL Server 2008 or Installing SQL Server 2008 R2.

- File system: %SYSTEMDRIVE% must be formatted with the NTFS file system.
- Operating System: Windows Server 2008 SP2 or Windows Server 2008 R2 SP1.
- Processor Architecture: x64.
- Windows Installer version: at least Windows Installer 3.1.
- Microsoft SQL Server: Microsoft SQL Server: SQL Server 2008 SP1, SQL Server 2008 SP2, SQL Server 2008 SP3, SQL Server 2008 R2, SQL Server 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1.
- SQL Server Full Text Search is required.
- Both .NET Framework 3.5 SP1 and .NET Framework 4 are required for Setup to run. For more information, see the following documents:
  - .NET Framework 3.5 SP1 redistributable package
  - .NET Framework 4 redistributable package

Operations Manager Gateway Server

- Disk space: %SYSTEMDRIVE% requires at least 1024 MB free hard disk space.
- Server Operating System: must be Windows Server 2008 R2 SP1.
- Processor Architecture: must be x64.
- Windows PowerShell version: Windows PowerShell version 2.0.
- Microsoft Core XML Services (MSXML) version: Microsoft Core XML Services 6.0 is required for the management server.
- .NET Framework 4 is required if the Gateway server manages UNIX/Linux agents or network devices.

Supported Firewall Scenarios

The following table shows Operations Manager feature interaction across a firewall, including information about the ports used for communication between the features, which direction to open the inbound port, and whether the port number can be changed.

Operations Manager 2012 Firewall Scenarios

Operations Manager Feature A	Port number and direction	Feature B	Configurable	Note
Management server	1433 --->	Operational database	Yes (Setup)	
Management server	1434 UDP < ---	Operational database	No	If the operational database is installed on a named instance of SQL Server 2008 SP1, SQL Server

Operations Manager Feature A	Port number and direction	Feature B	Configurable	Note
				2008 SP2, SQL Server 2008 SP3, SQL Server 2008 R2, SQL Server 2008 R2 SP1, or SQL Server 2008 R2 SP2 such as in a cluster, and the Windows Firewall is enabled on the management server, you have to also open UDP 1434 inbound on the management server.
Management server	1433 --->	Operational database	Yes (Setup)	
Management server	5723, 5724 --->	Management server	No	Port 5724 must be open to install this feature and can be closed after this feature has been installed.
Management server	1433 -->	Reporting data warehouse	No	
Management server	1433 --->	Reporting data warehouse	No	
Reporting server	5723, 5724 --->	Management server	No	Port 5724 must be open to install this feature and can be closed after this feature has been installed.
Operations console	5724 --->	Management server	No	
Connector	51905 --->	Management	No	

Operations Manager Feature A	Port number and direction	Feature B	Configurable	Note
Framework source		server		
Web console server	Selected web site port --->	Management server	No	
Web console (for Application Diagnostics	1433, 1434 -->	Operational database	Yes (Setup)	
Web console (for Application Advisor)	1433, 1434 -->	Data warehouse	Yes (Setup)	
Web console (for Application Advisor)	80 --->	SQL Server Reporting Services	No	
Web console browser	80, 443 --->	web console server	Yes (IIS Admin)	Default for HTTP or SSL. For either Network Authentication or Mixed Authentication, an account name and password can be sent as part of the request. We recommend you use SSL.
Agent installed by using MOMAgent.msi	5723 --->	Management server	Yes (Setup)	
Agent installed by using MOMAgent.msi	5723 --->	Management server	Yes (Setup)	
Agent installed by using MOMAgent.msi	5723 --->	Gateway server	Yes (Setup)	
Gateway server	5723 --->	Management server	Yes (Setup)	
Agent (Audit Collection Services (ACS) forwarder)	51909 --->	Management server Audit Collection	Yes (Registry)	

Operations Manager Feature A	Port number and direction	Feature B	Configurable	Note
		Services (ACS) Collector		
Agentless Exception Monitoring data from client	51906 --->	Management server Agentless Exception Monitoring (AEM) file share	Yes (Client Monitoring Wizard)	
Customer Experience Improvement Program data from client	51907 --->	Management server (Customer Experience Improvement Program) Endpoint	Yes (Client Monitoring Wizard)	
Operations console (reports)	80 --->	SQL Server Reporting Services	No	The Operations console uses port 80 to connect to the SQL Server Reporting Services website.
Reporting server	1433 --->	Reporting data warehouse	Yes	
Management server (Audit Collection Services Collector)	1433 --->	Audit Collection Services (ACS) database	Yes	
Management Server	161, 162 <--->	Network device	Yes	All firewalls between the management servers in the resource pool and the network devices need to allow SNMP (UDP) and ICMP bi-directionally, and ports 161 and 162 need to be open bi-directionally. This

Operations Manager Feature A	Port number and direction	Feature B	Configurable	Note
				includes Windows Firewall on the management server itself. If your network devices are using a port other than 161 and 162, you need to open bi-directional UDP traffic on these ports as well.
Management server or gateway server	1270 --- >	UNIX or Linux computer	No	
Management server or gateway server	22 --- >	UNIX or Linux computer	Yes	

In the preceding table, if SQL Server 2008 SP1, SQL Server 2008 SP2, SQL Server 2008 SP3, SQL Server 2008 R2, SQL Server 2008 R2 SP1, or SQL Server 2008 R2 SP2 is installed by using a default instance, the port number is 1433. If SQL Server is installed with a named instance, it is probably using a dynamic port. To identify the port, do the following:

1. Run SQL Server Configuration Manager.
2. Open SQL Server Network Configuration.
3. Open Protocols for INSTANCE1 (or the instance that is running under it).
4. Open TCP/IP.
5. Click **IP Addresses**.
6. The port is under IPAll (usually the TCP Dynamic Ports).

Minimum Network Connectivity Speeds

Operations Manager requires the following minimum network connectivity speeds between the specified features.

Feature A	Feature B	Minimum requirement
Management server	Agent	64 Kbps
Management server	Agentless	1024 Kbps
Management server	Database	256 Kbps

Feature A	Feature B	Minimum requirement
Management server	Console	768 Kbps
Management server	Management server	64 Kbps
Management server	Data warehouse database	768 Kbps
Management server	Reporting server	256 Kbps
Management server	Gateway server	64 Kbps
Local management group	Connected management group (tiered)	1024 Kbps
Web console server	web console	128 Kbps
Reporting Data Warehouse	Reporting server	1024 Kbps
Console	Reporting server	768 Kbps
Audit collector	Audit database	768 Kbps

Supported Cluster Configurations

Operations Manager supports the clustering configurations for Operations Manager features as shown in the following table:

Warning
Clustering of management servers is not supported in System Center 2012 – Operations Manager.

Only Cluster service quorum node clusters are supported. Multisite clusters (geographically dispersed clusters) are supported for all Operations Manager cluster roles. You can use replication technology to help provide high availability for data in Operations Manager, but the latency of communications between components introduce risks to data replication and might introduce failover issues. We recommend that you use synchronous mirroring of data disks between sites. Synchronous mirroring means that the data is fully synchronized across all sites and ensures the correct behavior of applications in the event of failover across sites.

Important
Microsoft is not obligated to release a hotfix on any Operations Manager issue that cannot be reproduced in a non-multisite cluster environment. If an analysis determines that non-Microsoft components in the configuration are causing the issue, the customer must work with the appropriate vendor for those components.

Server Feature	Cluster	Notes
Operations Manager	Single Active-Passive cluster	Other Operations Manager

Server Feature	Cluster	Notes
Operational database		features must not be installed on the cluster or nodes of the cluster.
Operations Manager Reporting data warehouse	Single Active-Passive cluster	Other Operations Manager features must not be installed on the cluster or nodes of the cluster.
Audit Collection Services (ACS) database	Single Active-Passive cluster	Other Operations Manager features must not be installed on the cluster or nodes of the cluster.

Supported, But Not Recommended Cluster Configurations

Operations Manager supports the following clustering configurations for Operations Manager server roles, as shown in the following table; however, because of a potential performance effect on your computer running SQL Server, these configurations are not recommended:

Server Feature	Cluster	Notes
Operations Manager operational database and Operations Manager Reporting data warehouse.	Active-Active cluster where the operational database is installed on one node of the cluster and the Reporting data warehouse is installed on the other node of the cluster.	There might be some performance issues with SQL Server in this configuration.
Operations Manager operational database, Reporting data warehouse, and Audit Collection Services (ACS) database.	Single Active-Passive or Active-Active cluster where all three components are on a single cluster.	There might be some performance issues with SQL Server in this configuration.
Operations Manager operational database and Audit Collection Services database.	Single Active-Passive cluster where both components are on a single cluster.	There might be some performance issues with SQL Server in this configuration.
Operations Manager operational database and Reporting data warehouse.	Single Active-Passive cluster where both components are on a single cluster.	There might be some performance issues with SQL Server in this configuration.
Reporting data warehouse	Single Active-Passive cluster	There might be some

Server Feature	Cluster	Notes
and Audit Collection Services database.	where both components are on a single cluster.	performance issues with SQL Server in this configuration.

Monitored Item Capacity

Operations Manager supports the following number of monitored items.

Monitored item	Recommended limit
Simultaneous Operations consoles	50
Agent-monitored computers reporting to a management server	3,000
Agent-monitored computers reporting to a gateway server	2,000
Agentless Exception Monitored (AEM)-computers per dedicated management server	25,000
Agentless Exception Monitored (AEM)-computers per management group	100,000
Collective client monitored computers per management server	2,500
Management servers per agent for multihoming	4
Agentless-managed computers per management server	10
Agentless-managed computers per management group	60
Agent-managed and UNIX or Linux computers per management group	6,000 (with 50 open consoles); 15,000 (with 25 open consoles)
UNIX or Linux computers per dedicated management server	500
UNIX or Linux computers monitored per dedicated gateway server	100
Network devices managed by a resource pool with three or more management servers	1,000
Network devices managed by two resource pools	2,000

Monitored item	Recommended limit
Agents for Application Performance Monitoring (APM)	700
Applications for Application Performance Monitoring (APM)	400
URLs monitored per dedicated management server	3000
URLs monitored per dedicated management group	12,000
URLs monitored per agent	50

Operations Manager Feature Firewall Exceptions

Feature	Exception	Port and protocol	Configured by
Management server	• System Center Management service • System Center Data Access service • Operations Manager Connector Framework • Operations Manager Customer Experience Improvement • Operations Manager Application Error Monitoring	5723/TCP 5724/TCP 51905/TCP 51907/TCP 51906/TCP	Setup Setup Setup Setup Setup
Web console	Operations Manager web console	Selected web site port/TCP	Setup
Web console, http	World Wide Web Services, http	80/TCP	Windows Firewall
Web console, https	Secure World Wide	443/TCP	Windows Firewall

Feature	Exception	Port and protocol	Configured by
	Web Service, https		
Operational database	• SQL Server database server • If using a named instance, add.	1433/TCP 1434/UDP	Windows Firewall Windows Firewall
Operations Manager data warehouse database	• SQL Server database server • If using a named instance, add.	1433/TCP 1434/UDP	Windows Firewall Windows Firewall
Operations Manager Reporting	SQL Server Reporting Services	80/TCP	Windows Firewall
Agent, manual installation of MOMAgent.msi	System Center Management service	5723/TCP	Windows Firewall
Agent, push installation	• System Center Management service • File and Print Sharing • Remote Administration	5723/TCP 137/UDP, 138/UDP, 139/TCP, 445/TCP 135/TCP, 445/TCP	Windows Firewall Windows Firewall Windows Firewall
Agent, pending repair	• System Center Management service • File and Print Sharing • Remote Administration	5723/TCP 137/UPD, 138/UPD, 139/TCP, 445/TCP 135/TCP, 445/TCP	Windows Firewall Windows Firewall Windows Firewall
Agent, pending upgrade	• System Center Management service • File and Print Sharing • Remote Administration	5723/TCP 137/UDP, 138/UDP, 139/TCP, 445/TCP 135/TCP, 445/TCP	Windows Firewall Windows Firewall Windows Firewall
Gateway	System Center Management service	5723/TCP	Setup

Feature	Exception	Port and protocol	Configured by
Operations Manager Audit Collection Services database	• SQL Server • If using a named instance, add.	1433/TCP 1434/UDP	Windows Firewall Windows Firewall
Operations Manager Audit Collection Services Collector	ACS Collector Service	51909/TCP	Windows Firewall

Support for Languages in Addition to English

Operations Manager supports the following languages: English, German, French, Japanese, Spanish, Simplified Chinese, Russian, Italian, and Portuguese (Brazil).

Support for different languages

If your systems run a language other than English, you can install Operations Manager for that language. You also have the option of installing English Operations Manager for your management group.

For example, if you use a German version of a Windows operating system on all your servers, you can install German Operations Manager features for your entire management group, or you can optionally install English Operations Manager features for your entire management group.

Agents for different languages

If you use an English management group, you can monitor any Windows Operating System Locale type.

If you use another language, you can monitor Windows operating systems for English and that language. For instance, if you use a German management group, you can monitor only English and German Windows operating systems.

Console for different languages

Operations Manager consoles are language independent. For example, you can use an Italian Operations Manager console to connect to a German management group.

Supported Network Monitoring Scenarios

Operations Manager supports monitoring of network devices that support Simple Network Management Protocol (SNMP). Port monitoring is available for devices that have implemented the interface MIB (RFC 2863) and MIB-II (RFC 1213) standards. In addition, peripheral monitoring, including processor and memory monitoring, is supported on a subset of devices. For more information, see System Center Operations Manager 2012: Network Devices with Extended Monitoring Capability.

Operations Manager can identify connected devices in a recursive discovery that use an IPv6 address; however, the initial device that is discovered must use an IPv4 address.

For more information about supported network devices, see Network Devices Supported for Discovery by Operations Manager 2012.

Application Performance Monitoring Requirements

To view Application Performance Monitoring event details, you must install the Operations Manager web console. For more information, see How to Install the Operations Manager Web Console.

Application Performance Monitoring requires the following software:

- .NET Framework 2.0, .NET Framework 3.5, .NET Framework 3.5 SP1, or .NET Framework 4.
- Internet Information Services (IIS) 7.0. Application monitoring on a clustered IIS configuration is not supported.
- ISAPI and CGI Restrictions in IIS be enabled for ASP.NET 4.0. To enable this, select the web server in IIS Manager, and then double-click **ISAPI and CGI Restrictions**. Select **ASP.NET v4.0.30319**, and then click **Allow**.

Additionally, you must start the SQL Server Agent service and set the startup type to automatic.

Upgrading System Center 2012 SP1 - Operations Manager to System Center 2012 R2

This Upgrade Guide provides information about how to upgrade from System Center 2012 Service Pack 1 (SP1), Operations Manager to System Center 2012 R2 Operations Manager.

Warning

If you are upgrading two or more System Center components, you must follow the procedures that are documented in Upgrade Sequencing for System Center 2012 R2.

The order in which you perform component upgrades is important. Failure to follow the correct upgrade sequence might result in component failure for which no recovery options exist. The affected System Center components are:

1. Orchestrator
2. Service Manager
3. Data Protection Manager (DPM)
4. Operations Manager
5. Configuration Manager
6. Virtual Machine Manager
7. App Controller

Warning

The only supported upgrade path to System Center 2012 R2 Operations Manager is from System Center 2012 Service Pack 1 (SP1), Operations Manager. If you are upgrading from System Center 2012 – Operations Manager, you must first upgrade to System Center 2012 Service Pack 1 (SP1), Operations Manager before upgrading to System Center 2012 R2 Operations Manager. See Upgrading to System Center 2012 - Operations Manager and Upgrading System Center 2012 – Operations Manager to System Center 2012 SP1 for complete upgrade information.

Important

It is assumed in this guide that you are performing an *upgrade* to System Center 2012 R2 Operations Manager. For information about installing Operations Manager on a computer where no previous version of Operations Manager exists, see Deploying System Center 2012 - Operations Manager.

Before you upgrade to System Center 2012 R2 Operations Manager, you must first determine whether all servers in your Operations Manager management group meet the minimum supported configurations. For more information, see System Requirements: System Center 2012 R2 Operations Manager

There are several options for upgrade:

1. If you run upgrade on a single-server management group, you only need to run upgrade one time since all features are installed on a single server. The Operations Manager Upgrade wizard performs system prerequisite checks and provides resolution steps for any issues. Installation will not continue until you resolve all issues.
2. If you are upgrading a distributed management group, you must upgrade certain features before others. For example, you upgrade the management servers first, followed by the gateways, operations consoles, and then agents. Next, you can upgrade any remaining features, such as the web console, reporting and Audit Collection Services (ACS). You must also perform a number of pre-upgrade and post-upgrade tasks.
3. If you want to maintain your Operations Manager 2007 R2 environment you can install System Center 2012 Service Pack 1 (SP1), Operations Manager in parallel and just upgrade your agents.

High Level View of System Center 2012 R2 Operations Manager Upgrade Steps – Upgrading a Distributed Management Group

The following steps outline the process for upgrading a distributed management group:

1. Accomplish Pre-Upgrade Tasks
2. Upgrade the initial management server and then additional management servers (each management server must be upgraded)
3. Upgrade ACS (because the ACS server must be on same machine as a management server, we recommend you perform this step along with the upgrade of the management server on which ACS resides.)

4. *Upgrade Gateway(s)
5. Upgrade Console
6. Push Install to Agent(s) / Upgrading Manually Installed Agents
7. Upgrade Web Console
8. Upgrade Reporting Server
9. Accomplish Post-Upgrade Tasks

* Steps 4 to 8 after Management Server Upgrade can occur in parallel.

High Level View of System Center 2012 R2 Operations Manager Upgrade Steps – Upgrading 2012 SP1 Agents to 2012 R2 and Running Two Environments

The following upgrade path supports customers in an Operations Manager scenario with parallel environments, sharing agents, so that the original System Center 2012 Service Pack 1 (SP1), Operations Manager environment is left intact. After the upgrade, the agents have been upgraded to System Center 2012 R2 Operations Manager and are fully capable of working with native System Center 2012 R2 Operations Manager functionality. The R2 agents are also able to "talk" to the System Center 2012 Service Pack 1 (SP1), Operations Manager management server.

Important

In this parallel environment scenario, we support upgrade of System Center 2012 Service Pack 1 (SP1), Operations Manager agents with the latest cumulative update (Operations Manager 2007 R2 CU6).

1. Retain the original System Center 2012 Service Pack 1 (SP1), Operations Manager environment.
2. Set up an additional, new System Center 2012 R2 Operations Manager environment with management servers, gateway, Operations Manager Database, Operations Manager Data Warehouse, console, web console, and reporting server.
3. Upgrade the System Center 2012 Service Pack 1 (SP1), Operations Manager Agents to 2012 R2.

   a. Push-Install option

   b. Manual / Command Line option

Note

If you are manually upgrading, step 2 is not needed.

Pre-Upgrade Tasks When Upgrading to System Center 2012 R2 Operations Manager

Perform the following pre-upgrade tasks in the order presented before you begin the upgrade process.

1. Review the Operations Manager Event Logs
2. Cleanup the Database (ETL Table)
3. Remove Agents from Pending Management
4. Disable the Notification Subscriptions
5. Stop the Services or Disable any Connectors
6. Verify that the Operational Database Has More Than 50 Percent Free Space
7. Back up the Operations Manager Databases

Review the Operations Manager Event Logs

Review the event logs for Operations Manager on the management servers to look for recurring warning or critical events. Address them and save a copy of the event logs before you perform your upgrade.

Cleanup the Database (ETL Table)

As part of upgrade to System Center 2012 R2 Operations Manager installation (setup) includes a script to cleanup ETL tables, grooming the database. However, in cases where there are a large number of rows (greater than 100,000) to cleanup, we recommend running the script before starting the upgrade to promote a faster upgrade and prevent possible timeout of setup. Performing this pre-upgrade task in all circumstances ensures a more efficient installation.

Run the following query to determine the number of rows that need to be deleted from ETL and cleanup the database:

To Cleanup ETL

1. To determine the number of rows that need to be deleted, run the following query:

```
DECLARE @SubscriptionWatermark bigint = 0;



SELECT @SubscriptionWatermark =
dbo.fn_GetEntityChangeLogGroomingWatermark();

Select COUNT (*)
FROM EntityTransactionLog ETL with(nolock)
WHERE NOT EXISTS (SELECT 1 FROM EntityChangeLog ECL
```

```
with(nolock) WHERE ECL.EntityTransactionLogId =
ETL.EntityTransactionLogId)
AND NOT EXISTS (SELECT 1 FROM RelatedEntityChangeLog RECL
with(nolock) WHERE RECL.EntityTransactionLogId =
ETL.EntityTransactionLogId)
AND EntityTransactionLogId < @SubscriptionWatermark;
```

2. To clean up the ETL Table, run the following SQL script:

```
DECLARE @RowCount int = 1;
DECLARE @BatchSize int = 100000;
DECLARE @SubscriptionWatermark bigint = 0;
DECLARE @LastErr int;

SELECT @SubscriptionWatermark =
dbo.fn_GetEntityChangeLogGroomingWatermark();
WHILE(@RowCount > 0)
BEGIN
DELETE TOP (@BatchSize) ETL
FROM EntityTransactionLog ETL
WHERE NOT EXISTS (SELECT 1 FROM EntityChangeLog ECL WHERE
ECL.EntityTransactionLogId = ETL.EntityTransactionLogId)
AND NOT EXISTS (SELECT 1 FROM RelatedEntityChangeLog RECL
WHERE RECL.EntityTransactionLogId =
ETL.EntityTransactionLogId)
AND ETL.EntityTransactionLogId < @SubscriptionWatermark;

SELECT @LastErr = @@ERROR, @RowCount = @@ROWCOUNT;



END
```

Note

Cleanup of ETL can require several hours to complete.

Remove Agents from Pending Management

Before you upgrade a management server, remove any agents that are in Pending Management.

To remove agents that are in Pending Management

1. Log on to the Operations console by using an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the **Administration pane**, expand **Device Management**, and then click **Pending Management**.
3. Right-click each agent, and then click **Approve** or **Reject**.

Disable the Notification Subscriptions

You should disable notification subscription before you upgrade the management group to ensure that notifications are not sent during the upgrade process.

To disable subscriptions

1. Log on to the Operations console account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, select the **Administration** view.
3. In the navigation pane, expand **Administration**, expand the **Notifications** container, and then click **Subscriptions**.
4. Select each subscription, and then click **Disable** in the **Actions** pane.

Note

Multiselect does not work when you are disabling subscriptions.

Stop the Services or Disable any Connectors

Refer to the non-Microsoft connector documentation for any installed Connectors to determine the services used for each Connector.

To stop a service for Connectors

1. On the **Start** menu, point to **Administrative Tools**, and then click **Services**.
2. In the **Name** column, right-click the Connector that you want to control, and then click **Stop**.

Verify that the Operational Database Has More Than 50 Percent Free Space

You must verify that the operational database has more than 50 percent of free space before you upgrade the management group because the upgrade might fail if there is not enough space. You should also ensure that the transactions logs are 50 percent of the total size of the operational database.

To check how much free space the Operational Database has

1. On the computer that hosts the operational database, open **SQL Server Management Studio**.
2. In the **Object Explorer**, expand **Databases**.
3. Right-click the operational database, point to **Reports**, **Standard Reports**, and then click **Disk Usage**.
4. View the **Disk Usage** report to determine the percentage of free space.

To increase the free space for the operational database and log files

1. On the computer that hosts the operational database, open **SQL Server Management Studio**.
2. In the **Connect to Server** dialog box, in the **Server Type** list, select **Database Engine**.
3. In the **Server Name** list, select the server and instance for your operational database (for example, computer\INSTANCE1).
4. In the **Authentication** list, select **Windows Authentication**, and then click **Connect**.
5. In the **Object Explorer** pane, expand **Databases**, right-click the operational database, and then click **Properties**.
6. In the **Database Properties** dialog box, under **Select a page**, click **Files**.
7. In the results pane, increase the **Initial Size** value for the **MOM_DATA** database by 50 percent.

   Note
   This step is not required if free space already exceeds 50 percent.
8. Set the **Initial Size** value for the **MOM_LOG** to be 50 percent of the total size of the database. For example, if the operational database size is 100 GB, the log file size should be 50 GB. Then click **OK**.

Back up the Operations Manager Databases

Obtain verified recent backups of the operational database and of the data warehouse database before you upgrade the secondary management server. You should also create backups of databases for optional features, such as the Reporting and the Audit Collection Services database before you upgrade them. For more information, see How to: Back up a Database and How to Schedule Backups of System Center 2012 - Operations Manager Databases.

How to Upgrade a Single-Server Management Group to System Center 2012 R2 Operations Manager

When you upgrade a single-server management group to System Center 2012 R2 Operations Manager, all features that are installed on the server are upgraded. Before you begin the upgrade process, make sure that your server meets the minimum supported configurations. For more information, see System Requirements: System Center 2012 R2 Operations Manager.

To upgrade a single-server management group

1. Log on to the server with an account that is a member of the Operations Manager Administrators role for your Operations Manager management group and a local administrator on the computer.
2. On the Operations Manager media, run **Setup.exe**, and then click **Install**.

   Note
   The **Getting Started** page displays information about what will be upgraded. Click **Next** to proceed with the upgrade.
3. On the **Getting Started, Please read the license terms page**, read the Microsoft Software License Terms, click **I have read, understood, and agree with the license terms**, and then click **Next**.
4. On the **Select installation location** page, accept the default value of **C:\Program Files\Microsoft System Center 2012 R2\Operations Manager**, or type in a new location or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify prerequisites again** to recheck the system.

   Note
   Microsoft SQL Server Full Text Search must be enabled.
6. If the Prerequisites checker does not return any other errors or warnings that have to be addressed, click **Next**.
7. On the **Configuration, Configure Operations Manager accounts** page, enter the credentials for a domain account or use Local System, and then click **Next**.

   Important
   If you receive a message about using the wrong version of SQL Server, or experience a problem with the SQL Server Windows Management Instrumentation (WMI) provider, you can resolve this. Open a Command Prompt window by using the **Run as administrator** option. Then run the following command, where <path> is the location of Microsoft SQL Server: `mofcomp.exe "<path>\Microsoft SQL Server\100\Shared\sqlmgmproviderxpsp2up.mof"`.
8. When the **Ready to Upgrade** page appears, review the upgrade summary, and then

click **Upgrade**.

To upgrade a single-server management group by using the Command Prompt window

1. Log on to the server with an account that is a member of the Operations Manager Administrators role for your Operations Manager management group and a local administrator on the computer.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the Operations Manager Setup.exe file is located.

   Important
   Use the `/WebConsoleUseSSL` parameter only if your website has Secure Sockets Layer (SSL) activated. For a default web installation, specify **Default Web Site** for the `/WebSiteName` parameter.

   Important
   The following commands assume that you specified the Local System for the Data Access service (`/UseLocalSystemDASAccount`). To specify a domain\user name for these accounts, you must provide the following parameters instead:`/DASAccountUser: <domain\username> /DASAccountPassword: <password>`
4. Run the following command.

```
Setup.exe /silent /upgrade
/AcceptEndUserLicenseAgreement:1
/UseLocalSystemDASAccount
/DatareaderUser: <domain\username>
/DatareaderPassword: <password>
/DataWriterUser: <domain\username>
/DataWriterPassword: <password>
/ManagementServer: <ManagementServerName>
/WebsiteName: "<WebSiteName>" [/WebConsoleUseSSL]
/WebConsoleAuthorizationMode: [Mixed|Network]
```

   Tip
   If you want to upgrade a specific component, you can add `/components: <component name1> [<, component name2>][ <, component name3>]`

After you have upgraded your single-server management group, you can upgrade the agents.

How to Upgrade a Management Server to System Center 2012 - Operations Manager - Upgrading a Distributed Management Group

When you upgrade a distributed management group to System Center 2012 R2 Operations Manager, you start by upgrading each of the management servers in your management group. There are a number of pre-upgrade tasks that you must perform first. For more information, see Pre-Upgrade Tasks When Upgrading to System Center 2012 R2 Operations Manager.

Important

Between the time that you upgrade the management servers and upgrade the agents, you might experience Application Platform Monitoring (APM)-related event log entries on the agent-managed servers. These event log entries might occur on agent-managed servers that are not APM-enabled. These event log entries will be resolved when you complete the upgrade of the agents. You might have to restart the health service after the agent is upgraded in order to clear the events.

Note

Because the ACS server must be on same machine as a management server, we recommend you perform the steps described in How to Upgrade an ACS Collector to System Center 2012 R2 Operations Manager along with the upgrade of the management server on which ACS resides.

Important

When upgrading multiple management servers in a distributed management group, you must wait to start upgrade of additional management servers until after setup on the first management server completes. Failing to do so can cause a SQL update script that runs early in the set up process to run on multiple management servers and result in database issues. This SQL update script only needs to run on the initial management server being upgraded.

Note

When upgrading multiple management servers in a distributed management group, sequence the upgrades in a manner that best suits your business needs. Upgrade all management servers in the distributed management group as soon as possible after the initial management server is upgraded to verify that your upgraded environment is healthy.

To upgrade a management server

1. Log on to the Operations Manager management server with an account that is a member of the Operations Manager Administrators role for your Operations Manager management group and a local administrator on the computer.
2. From the Operations Manager media, run **Setup.exe**, and then click **Install**. The **Getting**

Started page displays information about which features will be upgraded.

3. On the **Getting Started, System Center 2012 R2 Operations Manager Upgrade** page, click **Next** to proceed with the upgrade.
4. On the **Getting Started, Please read the license terms** page, read the Microsoft Software License Terms, click **I have read, understood, and agree with the terms of the license agreement**, and then click **Next**.
5. On the **Getting Started, Select installation location** page, accept the default value of **C:\Program Files\Microsoft System Center 2012 R2\Operations Manager**, or type in a new location, or browse to one. Then click **Next**.
6. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify prerequisites again** to recheck the system.
7. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites, Proceed with Setup** page appears. Click **Next**.
8. On the **Configuration, Configure Operations Manager accounts** page, enter the credentials for a domain account, and then click **Next**
9. Review the **Configuration, Ready To Upgrade** page, and then click **Upgrade**. The upgrade proceeds and displays the upgrade progress.
10. When the upgrade is finished, the **Upgrade complete** page appears. Click **Close**.

Note

Upgrading a management server is just one phase of the distributed upgrade process. Upgrade is not completed until you have upgraded all of the other features in your management group. The next step is to upgrade any gateways. See How to Upgrade a Gateway Server to System Center 2012 R2 Operations Manager for more information.

To upgrade a management server by using the Command Prompt window

1. Log on to the management server with an account that is a member of the Operations Manager Administrators role for your Operations Manager management group and a local administrator on the computer.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the Operations Manager setup.exe file is located, and run the following command.

Important

The following commands assume that you specified the Local System account for the Data Access service (`/UseLocalSystemDASAccount`). To specify a domain\user name for these accounts, you must provide the following parameters instead.`/DASAccountUser: <domain\username> /DASAccountPassword: <password>`

```
setup.exe /silent /upgrade
```

```
/AcceptEndUserLicenseAgreement:1
/UseLocalSystemDASAccount
/DataReaderUser:<domain\user>
/DataReaderPassword:<password>
```

After you have upgraded all of the management servers in your management group, you should upgrade any gateways, and then upgrade any stand-alone operations consoles.

How to Upgrade an ACS Collector to System Center 2012 R2 Operations Manager

Perform this procedure to upgrade the Audit Collection Services (ACS) Collector to System Center 2012 R2 Operations Manager locally on the ACS Collector. During this procedure, the ACS database is also upgraded without any additional steps.

Warning

A computer that hosts an ACS Collector must also be an Operations Manager management server or gateway server.

Before you begin the upgrade process, make sure that your server meets the minimum supported configurations. For more information, see System Requirements: System Center 2012 R2 Operations Manager

To upgrade an ACS Collector

1. Log on to the computer that hosts the ACS Collector with an Operations Manager Administrators role account for your Operations Manager management group.
2. On the Operations Manager media, run **Setup.exe**.
3. In the **Install** section, click **Audit Collection Services**. The Audit Collection Services Setup wizard starts.
4. On the **Welcome to the Audit Collection Services Collector Setup Wizard** page, click **Next**.
5. On the **Database Installation Options** page, select **Use an existing database**, and then click **Next**.
6. On the **Data Source** page, type the name that you used as the Open Database Connectivity data source name for your ACS database in the **Data source name** box. By default, this name is **OpsMgrAC**. Click **Next**.
7. On the **Database** page, if the database is on a separate server than the ACS Collector, click **Remote Database Server**, and then type the computer name of the database server that will host the database for this installation of ACS. Otherwise, click **Database server running locally**, and then click **Next**.
8. On the **Database Authentication** page, select one authentication method. If the ACS Collector and the ACS database are members of the same domain, you can select

Windows authentication; otherwise, select **SQL authentication**, and then click **Next**.

> **Note**
> If you select **SQL authentication** and click **Next**, the **Database Credentials** page appears. Enter the name of the user account that has access to the SQL Server in the **SQL login name** box and the password for that account in the **SQL password** password box, and then click **Next**.

9. The **Summary** page displays a list of actions that the installation program will perform to upgrade ACS. Review the list, and then click **Next** to begin the installation.

> **Note**
> If a **SQL Server Login** dialog box appears and the database authentication is set to **Windows Authentication**, select the correct database, and then verify that the **Use Trusted Connection** check box is selected. Otherwise, clear it, enter the SQL Server login name and password, and then click **OK**.

10. When the upgrade is finished, click **Finish**.

How to Upgrade a Gateway Server to System Center 2012 R2 Operations Manager

After you upgrade the management servers in your management group, you upgrade any gateway servers. The procedure to upgrade a gateway server to System Center 2012 R2 Operations Manager is performed locally on the gateway server. You can then verify whether the upgrade is successful. Before you begin the upgrade process, make sure that your gateway server meets the minimum supported configurations. For more information, see System Requirements: System Center 2012 R2 Operations Manager

To upgrade a gateway server

1. Log on to a computer that hosts the gateway server with an Operations Manager Administrators role account for your Operations Manager management group.
2. On the Operations Manager media, run **Setup.exe**.
3. In the **Optional Installations** area, click **Gateway management server**.
4. On the **Welcome to the System Center 2012 R2 Operations Manager Gateway Upgrade Wizard** page, click **Next**.
5. On the **The wizard is ready to begin gateway upgrade** page, click **Upgrade**.
6. On the **Completing the System Center 2012 - Operations Manager Gateway Setup wizard** page, click **Finish**.

To upgrade a gateway server by using the Command Prompt window

1. Log on to a computer that is hosting the gateway server with an Operations Manager

Administrators role account for your Operations Manager management group.

2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the directory to the System Center 2012 R2 Operations Manager installation media and change directory again to gateway\AMD64, where the MOMGateway.msi file is located.
4. Run the following command where D:\ is the location for the upgrade log file.

```
msiexec /i MOMgateway.msi /qn /l*v D:\logs\GatewayUpgrade.
log
AcceptEndUserLicenseAgreement=1
```

To verify the gateway server upgrade

1. In the Operations console, in the navigation pane, click the **Administration** button.
2. Under **Device Management**, click **Management Servers**.
3. In the **Management Servers** pane, verify that the value listed in the **Version** column is System Center 2012 R2 Operations Manager 10139 (10xxx), where x is any positive integer.

After you have upgraded all of the gateways in your management group, you can upgrade the stand-alone operations consoles. See How to Upgrade an Operations Console to System Center 2012 R2 Operations Manager for more information.

How to Upgrade an Operations Console to System Center 2012 R2 Operations Manager

This procedure upgrades a stand-alone Operations console to System Center 2012 R2 Operations Manager. Perform this procedure locally on the computer that has a stand-alone Operations console installed. You do not have to perform this procedure to upgrade Operations consoles that are installed locally on a management server.

Before you begin the upgrade process, make sure that your server meets the minimum supported configurations. For more information, see System Requirements: System Center 2012 R2 Operations Manager

To upgrade a stand-alone Operations console

1. Log on to the computer that hosts the Operations console with an Operations Manager Administrators role account for your Operations Manager management group.
2. On the Operations Manager source media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started**, **System Center 2012 R2 Operations Manager Upgrade** page, click **Next**.
4. On the **Getting Started**, **Select installation location** page, accept the default value of **C:\Program Files\Microsoft System Center 2012 R2\Operations Manager**, or type in a

new location or browse to one. Then click **Next**.

5. On the **Prerequisites** page, review and address any warnings or errors that are returned by the Prerequisites checker, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration**, **Ready To Upgrade** page, click **Upgrade**.
8. When the upgrade is finished, the **Upgrade complete** page appears. Click **Close**.

To upgrade a stand-alone Operations console by using the Command Prompt window

1. Log on to the computer that hosts the Operations console with an Operations Manager Administrators role account for your Operations Manager management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change to the path to the Operations Manager source media, and run the following command.

```
Setup.exe /silent / upgrade /AcceptEndUserLicenseAgreement:1
```

To verify the Operations console upgrade

1. On the Windows desktop, click **Start**, and then click **Run**.
2. Type **regedit**, and then click **OK**. The Registry Editor starts.

   Caution
   Incorrectly editing the registry can severely damage your system. Before you make changes to the registry, you should back up any valued data that is on the computer.
3. Browse to the **HKey_Local_Machine\Software\Microsoft\Microsoft Operations Manager\3.0\Setup** key. If the value of the **UIVersion** entry is **10226 (10xxx)**, where **x** is any positive integer, the Operations console was upgraded successfully.

After you have upgraded all of the stand-alone operations consoles in your management group, you can upgrade the agents. See How to Upgrade an Agent to System Center 2012 R2 Operations Manager for more information.

How to Upgrade an Agent to System Center 2012 R2 Operations Manager

Use the following procedures to upgrade to System Center 2012 R2 Operations Manager agents. You should first verify that the agents meet minimum supported configurations. For more information, see System Requirements: System Center 2012 R2 Operations Manager

Note

If before upgrade an agent was installed using the push install method, after upgrade the server the agent will be put into a pending update state and can be upgraded through the Console. Otherwise the agent should be upgraded manually.

When you upgrade an agent, the Operations Manager installer service runs and is not removed until after the completion of the upgrade. If the agent upgrade fails, you might have to re-install the agent because the installer service was not properly removed. If you attempt to upgrade the agent again and it fails, you should re-install the agent after you have completed upgrading all features of Operations Manager.

Note
If you have Audit Collection Services (ACS) enabled for an agent prior to this upgrade, it is disabled as part of the agent upgrade process. ACS must be re-enabled after upgrade completes.

If you are upgrading agents that are deployed to a computer that has other System Center 2012 R2 Operations Manager features installed, you must do the following:

- If the agent is installed on a computer that has System Center 2012 R2 Operations Manager Operations console or web console installed, you must first uninstall the consoles before you upgrade the agents. You can do this by uninstalling System Center 2012 R2 Operations Managerin Programs and Features. You can reinstall these consoles after upgrade is completed.

Note
If UAC is enabled, you must run the agent upgrade from an elevated command prompt.

Note
Information about upgraded agents might not appear in the Operations console for up to 60 minutes after performing the upgrade.

Upgrading Push-Installed Agents

Push-installed agents are agents that were installed by using the **Computer and Device Management Wizard**. Use the following procedures to upgrade these agents.

To upgrade push-installed Windows agents by using the Operations console

1. Log on to the computer hosting the Operations Manager Operations console. Use an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click **Administration**.

   Note
   When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the management server to which you want to connect.
3. In the **Administration** workspace, in the navigation pane under **Device Management**,

click **Pending Management**.

4. In the **Pending Management** pane, under **Type: Agent Requires Update**, right-click each agent-managed computer listed, and then click **Approve**.

   Warning
   You should not approve more than 200 agents at one time.

5. In the **Update Agents** dialog box, enter the administrator account credentials or use a selected Management Server Action Account, and then click **Update**. The upgrade status is displayed in the **Agent Management Task Status** dialog box.
6. When the upgrade is completed, click **Close**.

Upgrading Manually Installed Agents

Manually-installed agents are agents that were installed manually, either by using the Command Prompt window, or by using the MOMAgent.msi Setup Wizard. Use the following procedure to upgrade these agents.

To upgrade a manually installed Windows agent by using the Setup Wizard

1. Log on to the computer that hosts the agent with an Operations Manager Administrators role account for your Operations Manager management group.
2. Run **Setup.exe** from the Operations Manager installation media.
3. On the first page of the Setup Wizard, click **Local agent**. When the **Welcome to the Microsoft Monitoring Agent Upgrade Wizard** page opens, click **Next**.
4. In the **Microsoft Monitoring Agent Setup** dialog box, click **Upgrade**. The status page displays the progress of the upgrade.
5. When the **Completing the Microsoft Monitoring Agent Setup Wizard** page appears, click **Finish**.

To upgrade a manually installed Windows agent by using the Command Prompt window

1. Log on to the computer that hosts the agent with an Operations Manager Administrators role account for your Operations Manager management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Run the following command, where D:\ is the location for the upgrade log file.

```
msiexec /i MOMAgent.msi /qn /l*v D:\logs\AgentUpgrade.log
 AcceptEndUserLicenseAgreement=1
```

Verifying Windows Agent Upgrade

To verify the Windows agent upgrade

1. In the Operations console, in the navigation pane, click the **Administration** button.
2. Under **Device Management**, click **Agent Managed**.
3. In the Agent Managed pane, verify that the value listed in the Version column is 10184 (10xxx), where x is any positive integer.

   Note
   It can take up to one hour for the console to show the updated version of the agent.

Upgrading UNIX and Linux Agents

To upgrade UNIX and Linux agents

- In the Operations console, in the **Administration** pane, run the **UNIX/Linux Upgrade Wizard**.

  Any existing Run As profiles and Run As accounts continue to have valid configurations. For information about changes to Run As profiles and accounts for UNIX and Linux monitoring in Operations Manager, see Accessing UNIX and Linux Computers in Operations Manager

To manually upgrade UNIX and Linux agents

1. Log on to Linux/Unix machines and copy the target agent to machines.
2. Run the commands below on different Systems to upgrade the agents:
   - Suse/Redhat/CentOS/Oracle Linux: `rpm -U <package>`
   - Ubuntu/Debian: `-i <package file>`
   - HP-UX: `swinstall -s <full path to depot> <package name>`
   - Aix: `/usr/sbin/install -X -F -d <package file> scx.rte/`
   - Solaris:
     - Remove the installed package with: `pkgrm MSFTscx`
     - Install the new package version with: `pkgadd`

To verify the UNIX or Linux agent upgrade

1. In the Operations console, in the navigation pane, click **Administration**.
2. Under **Device Management**, click **UNIX/Linux Computers**.
3. Verify that the value listed in the Agent **Version** column is 1.54.0-xxx, where x is any positive integer.

   Note
   It can take up to one hour for the console to show the updated version of the agent.

How to Upgrade a Web Console to System Center 2012 R2 Operations Manager

If you have a stand-alone System Center 2012 Service Pack 1 (SP1), Operations Manager web console server, you can upgrade it to System Center 2012 R2 Operations Manager.

Before you begin the upgrade process, make sure that your server meets the minimum supported configurations. For more information, see System Requirements: System Center 2012 R2 Operations Manager

Note
When you upgrade the web console, any customizations that were made to the web.config file after the web console was installed will be reset.

If you made changes after you set up your web console to either enable or disable Secure Sockets Layer (SSL), the SSL settings will be reset during upgrade. To resolve the issue, you must make changes to the registry key before you upgrade the web console, as follows:

To set the registry to enable or disable SSL on the web console

1. Logon on to the web console with an account that has local administrator rights, and on the desktop, click **Start**, and then click **Run**.
2. Type **regedit**, and then click **OK**. The Registry Editor starts.

   Caution
   Incorrectly editing the registry can severely damage your system. Before you make changes to the registry, you should back up any valued data that is on the computer.
3. Navigate to the **HKey_Local_Machine\Software\Microsoft\System Center Operations Manager\12\Setup\WebConsole** key.
4. To enable SSL, set the following:

   HTTP_GET_ENABLED=0

   BINDING_CONFIGURATION=DefaultHttpsBinding
5. To disable SSL, set the following:

   HTTP_GET_ENABLED=1

   BINDING_CONFIGURATION=DefaultHttpBinding

To upgrade the web console server

1. Log on to the computer that hosts the web console server with an Operations Manager Administrators role account for your Operations Manager management group.
2. On the Operations Manager source media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started**, **System Center 2012 R2 Operations Manager Upgrade** page, review the features that will be upgraded, and then click **Next**.
4. On the **Select installation location** page, accept the default value of **C:\Program**

Files\Microsoft System Center 2012 R2\Operations Manager, or type in a new location or browse to one. Then click **Next**.

5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
7. When the **Ready to Upgrade** page appears, review the upgrade summary, and then click **Upgrade**.

To upgrade the web console server by using the Command Prompt window

1. Log on to the computer that hosts the web console server with an Operations Manager Administrators role account for your Operations Manager management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the Operations Manager Setup.exe file is located, and run the following command.

   Important
   Use the `/WebConsoleUseSSL` parameter only if your website has Secure Sockets Layer (SSL) activated. For a default web installation, specify **Default Web Site** for the `/WebSiteName` parameter.

```
setup.exe /silent /AcceptEndUserLicenseAgreement:1 /upgrade
/WebsiteName: "<WebSiteName>" [/WebConsoleUseSSL]
/WebConsoleAuthorizationMode: [Mixed|Network]
```

How to Upgrade Reporting to System Center 2012 - Operations Manager

Use this procedure to upgrade a stand-alone Reporting server to System Center 2012 R2 Operations Manager. You should not run upgrade on the Reporting server until after you have upgraded the management servers, gateways, operation consoles, and agents.

Before you begin the upgrade process, make sure that your server meets the minimum supported configurations. For more information, see System Requirements: System Center 2012 R2 Operations Manager

To upgrade the Reporting server

1. Log on to the computer that hosts the Reporting server with an account that is a member of the Operations Manager Administrators role for your Operations Manager

management group.

2. On the Operations Manager source media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started**, **System Center 2012 R2 Operations Manager Upgrade** page, review the features that will be upgraded. In this case, it is Operations Manager Reporting. Click **Next**.
4. On the **Select installation location** page, accept the default value of **C:\Program Files\Microsoft System Center 2012 R2\Operations Manager**, or type in a new location or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
7. On the **Ready to Upgrade** page, review the options, and then click **Upgrade**.
8. When upgrade is finished, the **Upgrade complete** page appears. Click **Close**.

To upgrade the Reporting server by using the command prompt

1. Log on to the computer that hosts the Reporting server with an account that is a member of the Operations Manager Administrators role for your Operations Manager management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the Operations Manager Setup.exe file is located, and run the following command:

   Note
   If the Reporting server reports to an unsupported or inaccessible root management server, you must also pass the following parameter: `/ManagementServer: <ManagementServerName>`.

```
setup.exe /silent /AcceptEndUserLicenseAgreement:1 /upgrade
/ManagementServer: <ManagementServerName>
```

Post-Upgrade Tasks When Upgrading to System Center 2012 R2 Operations Manager

After you have completed the upgrade process to System Center 2012 R2 Operations Manager, you must perform a number of post-upgrade tasks.

Post-Upgrade Tasks

Perform the following tasks when you have completed the upgrade process.

1. Re-enable the Notification Subscriptions.
2. Restart or Re-enable the Connector Services (if needed)
3. Re-enable Audit Collection Services (ACS) on agents that were upgraded
4. Verify That the Upgrade Was Successful

Re-enable the Notification Subscriptions

After the upgrade has finished, use the following procedure to re-enable subscriptions.

To re-enable the subscriptions

1. Open the Operations console by using an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, in the navigation pane, click the **Administration** button.

   Note
   When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** text box, type the name of the Operations Manager management server to which you want to connect.
3. In the **Administration** pane, under **Notifications**, click **Subscriptions**.
4. In the **Actions** pane, click **Enable** for each subscription listed.

Restart or Re-enable the Connector Services

Refer to the third-party documentation for any installed connectors to determine if the connectors are supported for System Center 2012 R2 Operations Manager. If you stopped a connector for any reason during upgrade, restart the service.

To restart a connector service

1. On the taskbar, click **Start**, click **Administrative Tools**, and then click **Services**.
2. In the **Name** column, right-click the connector that you want to restart, and then click **Start**.

Re-Enable Audit Collection Services

If you had Audit Collection Services (ACS) enabled for an agent prior to upgrade, it was disabled as part of the agent upgrade process. Re-enable ACS as appropriate.

Verify That the Upgrade Was Successful

Perform the following tasks to verify that the upgrade was successful.

- Check the health state of the management servers and agents in the Health Service Watcher state view. In the **Administration** workspace of the Operations console, ensure that the management servers and agents are healthy. In the **Monitoring** workspace, check if there are any alerts related to the management group health.
- Review the event logs of all the management servers for new errors.
- Sort alerts by the last-modified column to review the new alerts.
- Check the CPU utilization and disk I/O on your database servers to ensure that they are functioning normally.
- If the Reporting feature is installed, click **Reporting**, and then run a generic performance report to ensure that Reporting is functioning correctly.
- Re-deploy any agents that you uninstalled during the upgrade process.

How to Upgrade OM2012 SP1 Agents to OM2012 R2 Parallel Environments

This upgrade path contains an Operations Manager scenario with parallel environments, sharing agents, so that the original System Center 2012 Service Pack 1 (SP1), Operations Manager environment is left intact. After the upgrade, the agents have been upgraded to System Center 2012 R2 Operations Manager and are fully capable of working with native System Center 2012 R2 Operations Manager functionality. The System Center 2012 R2 Operations Manager agents are also able to “talk” to the System Center 2012 Service Pack 1 (SP1), Operations Manager management server.

Upgrading OM2012 SP1 Agents to OM2012 R2 using Parallel Environments

If you want to maintain your System Center 2012 Service Pack 1 (SP1), Operations Manager environment you can install System Center 2012 R2 Operations Manager in parallel and just upgrade your agents using the following process.

1. Retain the original System Center 2012 Service Pack 1 (SP1), Operations Manager environment.
2. Set up an additional, new System Center 2012 R2 Operations Manager environment with management servers, gateway, Operations Manager Database, Operations Manager Data Warehouse, console, web console, and reporting server. See Deploying System Center 2012 - Operations Manager for more information.
3. Upgrade the System Center 2012 Service Pack 1 (SP1), Operations Manager Agents to 2012 R2 using Push-Install or Command Line options as appropriate. See How to Upgrade an Agent to System Center 2012 R2 Operations Manager for more information.

Upgrading System Center 2012 – Operations Manager to System Center 2012 SP1

This Upgrade Guide provides information about how to upgrade from System Center 2012 – Operations Manager to System Center 2012 Service Pack 1 (SP1), Operations Manager.

Warning

If you are planning to upgrade two or more System Center components, it is imperative that you first consult the guide Upgrade Sequencing for System Center 2012 SP1. The order in which you perform component upgrades is important. Failure to follow the correct upgrade sequence might result in component failure for which no recovery options exist. The affected System Center components are:

1. Orchestrator
2. Service Manager
3. Data Protection Manager (DPM)
4. Operations Manager
5. Configuration Manager
6. Virtual Machine Manager
7. App Controller

Warning

The only supported upgrade path to System Center 2012 Service Pack 1 (SP1), Operations Manager is from System Center 2012 – Operations Manager. If you are upgrading from System Center Operations Manager 2007 R2, you must first upgrade to System Center 2012 – Operations Manager. See Upgrading to System Center 2012 - Operations Manager for complete upgrade information.

Important

It is assumed in this guide that you are performing an *upgrade* to System Center 2012 Service Pack 1 (SP1), Operations Manager. For information about installing Operations Manager on a computer where no previous version of Service Manager exists, see Deploying System Center 2012 – Service Manager.

Before you upgrade to System Center 2012 Service Pack 1 (SP1), Operations Manager, you must first determine whether all servers in your Operations Manager management group meet the minimum supported configurations. For more information, see System Requirements: System Center 2012 SP1 - Operations Manager

There are several options for upgrade:

1. If you run upgrade on a single-server management group, you only need to run upgrade one time since all features are installed on a single server. The Operations Manager Upgrade wizard performs system prerequisite checks and provides resolution steps for any issues. Installation will not continue until you resolve all issues.

2. If you are upgrading a distributed management group, you must upgrade certain features before others. For example, you upgrade the management servers first, followed by the gateways, operations consoles, and then agents. Next, you can upgrade any remaining features, such as the web console, reporting and Audit Collection Services (ACS). You must also perform a number of pre-upgrade and post-upgrade tasks.
3. If you want to maintain your Operations Manager 2007 R2 environment you can install System Center 2012 Service Pack 1 (SP1), Operations Manager in parallel and just upgrade your agents.

High Level View of System Center 2012 SP1 - Operations Manager Upgrade Steps – Upgrading a Distributed Management Group

The following steps outline the process for upgrading a distributed management group:

1. Accomplish Pre-Upgrade Tasks
2. Upgrade the initial management server and then additional management servers (each management server must be upgraded)
3. Upgrade ACS (because the ACS server must be on same machine as a management server, we recommend you perform this step along with the upgrade of the management server on which ACS resides.)
4. *Upgrade Gateway(s)
5. Upgrade Console
6. Push Install to Agent(s) / Upgrading Manually Installed Agents
7. Upgrade Web Console
8. Upgrade Reporting Server
9. Accomplish Post-Upgrade Tasks

* Steps 4 to 8 after Management Server Upgrade can occur in parallel.

High Level View of System Center 2012 SP1 - Operations Manager Upgrade Steps – Upgrading 2007 R2 Agents to 2012 SP1 and Running Two Environments

The following upgrade path supports customers in an Operations Manager scenario with parallel environments, sharing agents, so that the original Operations Manager 2007 R2 environment is left intact. After the upgrade, the agents have been upgraded to System Center 2012 Service Pack 1 (SP1), Operations Manager and are fully capable of working with native System Center 2012 Service Pack 1 (SP1) functionality. The SP1 agents are also able to “talk” to the Operations Manager 2007 R2 management server.

Important

In this parallel environment scenario, we support upgrade of Operations Manager 2007 R2 agents with the latest cumulative update (CU6).

1. Retain the original Operations Manager 2007 R2 environment.
2. Set up an additional, new System Center 2012 Service Pack 1 (SP1), Operations Manager environment with management servers, gateway, Operations Manager Database, Operations Manager Data Warehouse, console, web console, and reporting server.
3. Upgrade the Operations Manager 2007 R2 Agents to 2012 SP1.

   a. Push-Install option

   b. Manual / Command Line option

Pre-Upgrade Tasks When Upgrading to System Center 2012 SP1 - Operations Manager

Perform the following pre-upgrade tasks in the order presented before you begin the upgrade process.

1. Review the Operations Manager Event Logs
2. Cleanup the Database (ETL Table)
3. Remove Agents from Pending Management
4. Disable the Notification Subscriptions
5. Stop the Services or Disable any Connectors
6. Verify that the Operational Database Has More Than 50 Percent Free Space
7. Back up the Operations Manager Databases

Review the Operations Manager Event Logs

Review the event logs for Operations Manager on the management servers to look for recurring warning or critical events. Address them and save a copy of the event logs before you perform your upgrade.

Cleanup the Database (ETL Table)

As part of upgrade to System Center 2012 Service Pack 1 (SP1), Operations Manager installation (setup) includes a script to cleanup ETL tables, grooming the database. However, in cases where there are a large number of rows (greater than 100,000) to cleanup, we recommend running the script before starting the upgrade to promote a faster upgrade and prevent possible timeout of setup. Performing this pre-upgrade task in all circumstances ensures a more efficient installation.

Run the following query to determine the number of rows that need to be deleted from ETL and cleanup the database:

To Cleanup ETL

1. To determine the number of rows that need to be deleted, run the following query:

```
DECLARE @SubscriptionWatermark bigint = 0;


SELECT @SubscriptionWatermark =
dbo.fn_GetEntityChangeLogGroomingWatermark();

Select COUNT (*)
FROM EntityTransactionLog ETL with(nolock)
WHERE NOT EXISTS (SELECT 1 FROM EntityChangeLog ECL
with(nolock) WHERE ECL.EntityTransactionLogId =
ETL.EntityTransactionLogId)
AND NOT EXISTS (SELECT 1 FROM RelatedEntityChangeLog RECL
with(nolock) WHERE RECL.EntityTransactionLogId =
ETL.EntityTransactionLogId)
AND EntityTransactionLogId < @SubscriptionWatermark;
```

2. To clean up the ETL Table, run the following SQL script:

```
DECLARE @RowCount int = 1;
DECLARE @BatchSize int = 100000;
DECLARE @SubscriptionWatermark bigint = 0;
DECLARE @LastErr int;

SELECT @SubscriptionWatermark =
dbo.fn_GetEntityChangeLogGroomingWatermark();
WHILE(@RowCount > 0)
BEGIN
DELETE TOP (@BatchSize) ETL
FROM EntityTransactionLog ETL
WHERE NOT EXISTS (SELECT 1 FROM EntityChangeLog ECL WHERE
ECL.EntityTransactionLogId = ETL.EntityTransactionLogId)
AND NOT EXISTS (SELECT 1 FROM RelatedEntityChangeLog RECL
WHERE RECL.EntityTransactionLogId =
```

```
        ETL.EntityTransactionLogId)
        AND ETL.EntityTransactionLogId < @SubscriptionWatermark;

        SELECT @LastErr = @@ERROR, @RowCount = @@ROWCOUNT;


        END
```

Note

Cleanup of ETL can require several hours to complete.

Remove Agents from Pending Management

Before you upgrade a management server, remove any agents that are in Pending Management.

To remove agents that are in Pending Management

1. Log on to the Operations console by using an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the **Administration pane**, expand **Device Management**, and then click **Pending Management**.
3. Right-click each agent, and then click **Approve** or **Reject**.

Disable the Notification Subscriptions

You should disable notification subscription before you upgrade the management group to ensure that notifications are not sent during the upgrade process.

To disable subscriptions

1. Log on to the Operations console account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, select the **Administration** view.
3. In the navigation pane, expand **Administration**, expand the **Notifications** container, and then click **Subscriptions**.
4. Select each subscription, and then click **Disable** in the **Actions** pane.

Note

Multiselect does not work when you are disabling subscriptions.

Stop the Services or Disable any Connectors

Refer to the non-Microsoft connector documentation for any installed Connectors to determine the services used for each Connector.

To stop a service for Connectors

1. On the **Start** menu, point to **Administrative Tools**, and then click **Services**.
2. In the **Name** column, right-click the Connector that you want to control, and then click **Stop**.

Verify that the Operational Database Has More Than 50 Percent Free Space

You must verify that the operational database has more than 50 percent of free space before you upgrade the management group because the upgrade might fail if there is not enough space. You should also ensure that the transactions logs are 50 percent of the total size of the operational database.

To check how much free space the Operational Database has

1. On the computer that hosts the operational database, open **SQL Server Management Studio**.
2. In the **Object Explorer**, expand **Databases**.
3. Right-click the operational database, point to **Reports**, **Standard Reports**, and then click **Disk Usage**.
4. View the **Disk Usage** report to determine the percentage of free space.

To increase the free space for the operational database and log files

1. On the computer that hosts the operational database, open **SQL Server Management Studio**.
2. In the **Connect to Server** dialog box, in the **Server Type** list, select **Database Engine**.
3. In the **Server Name** list, select the server and instance for your operational database (for example, computer\INSTANCE1).
4. In the **Authentication** list, select **Windows Authentication**, and then click **Connect**.
5. In the **Object Explorer** pane, expand **Databases**, right-click the operational database, and then click **Properties**.
6. In the **Database Properties** dialog box, under **Select a page**, click **Files**.
7. In the results pane, increase the **Initial Size** value for the **MOM_DATA** database by 50 percent.

   Note
   This step is not required if free space already exceeds 50 percent.
8. Set the **Initial Size** value for the **MOM_LOG** to be 50 percent of the total size of the

database. For example, if the operational database size is 100 GB, the log file size should be 50 GB. Then click **OK**.

Back up the Operations Manager Databases

Obtain verified recent backups of the operational database and of the data warehouse database before you upgrade the secondary management server. You should also create backups of databases for optional features, such as the Reporting and the Audit Collection Services database before you upgrade them. For more information, see How to: Back up a Database and How to Schedule Backups of System Center 2012 - Operations Manager Databases.

How to Upgrade a Single-Server Management Group to System Center 2012 SP1 - Operations Manager

When you upgrade a single-server management group to System Center 2012 Service Pack 1 (SP1), Operations Manager, all features that are installed on the server are upgraded.Before you begin the upgrade process, make sure that your server meets the minimum supported configurations. For more information, see System Requirements: System Center 2012 SP1 - Operations Manager.

To upgrade a single-server management group

1. Log on to the server with an account that is a member of the Operations Manager Administrators role for your Operations Manager management group and a local administrator on the computer.
2. On the Operations Manager media, run **Setup.exe**, and then click **Install**.

   Note
   The **Getting Started** page displays information about what will be upgraded. Click **Next** to proceed with the upgrade.
3. On the **Getting Started, Please read this license agreement page**, read the Microsoft Software License Terms, click **I have read, understood, and agree with the terms of the license agreement**, and then click **Next**.
4. On the **Select installation location** page, accept the default value of **C:\Program Files\System Center Operations Manager 2012**, or type in a new location or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify prerequisites again** to recheck the system.

   Note
   Microsoft SQL Server Full Text Search must be enabled.
6. If the Prerequisites checker does not return any other errors or warnings that have to be

addressed, click **Next**.

7. On the **Configuration, Configure Operations Manager accounts** page, enter the credentials for a domain account, and then click **Next**.

   Important
   If you receive a message about using the wrong version of SQL Server, or experience a problem with the SQL Server Windows Management Instrumentation (WMI) provider, you can resolve this. Open a Command Prompt window by using the **Run as administrator** option. Then run the following command, where <path> is the location of Microsoft SQL Server: `mofcomp.exe "<path>\Microsoft SQL Server\100\Shared\sqlmgmproviderxpsp2up.mof"`.

8. When the **Ready to Upgrade** page appears, review the upgrade summary, and then click **Upgrade**.

To upgrade a single-server management group by using the Command Prompt window

1. Log on to the server with an account that is a member of the Operations Manager Administrators role for your Operations Manager management group and a local administrator on the computer.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the Operations Manager Setup.exe file is located.

   Important
   Use the `/WebConsoleUseSSL` parameter only if your website has Secure Sockets Layer (SSL) activated. For a default web installation, specify **Default Web Site** for the `/WebSiteName` parameter.

   Important
   The following commands assume that you specified the Local System for the Data Access service (`/UseLocalSystemDASAccount`). To specify a domain\user name for these accounts, you must provide the following parameters instead:`/DASAccountUser: <domain\username> /DASAccountPassword: <password>`

4. Run the following command.

```
Setup.exe /silent /upgrade
/AcceptEndUserLicenseAgreement:1
/UseLocalSystemDASAccount
/DatareaderUser: <domain\username>
/DatareaderPassword: <password>
/DataWriterUser: <domain\username>
/DataWriterPassword: <password>
/ManagementServer: <ManagementServerName>
/WebsiteName: "<WebSiteName>" [/WebConsoleUseSSL]
```

```
/WebConsoleAuthorizationMode: [Mixed|Network]
```

After you have upgraded your single-server management group, you can upgrade the agents.

How to Upgrade a Management Server to System Center 2012 - Operations Manager - Upgrading a Distributed Management Group

When you upgrade a distributed management group to System Center 2012 Service Pack 1 (SP1), Operations Manager, you start by upgrading each of the management servers in your management group. There are a number of pre-upgrade tasks that you must perform first. For more information, see Pre-Upgrade Tasks When Upgrading to System Center 2012 SP1 - Operations Manager.

Important

Between the time that you upgrade the management servers and upgrade the agents, you might experience Application Platform Monitoring (APM)-related event log entries on the agent-managed servers. These event log entries might occur on agent-managed servers that are not APM-enabled. These event log entries will be resolved when you complete the upgrade of the agents. You might have to restart the health service after the agent is upgraded in order to clear the events.

Note

Because the ACS server must be on same machine as a management server, we recommend you perform the steps described in How to Upgrade an ACS Collector to System Center 2012 SP1 - Operations Manager along with the upgrade of the management server on which ACS resides.

Important

When upgrading multiple management servers in a distributed management group, you must wait to start upgrade of additional management servers until after setup on the first management server completes. Failing to do so can cause a SQL update script that runs early in the set up process to run on multiple management servers and result in database issues. This SQL update script only needs to run on the initial management server being upgraded.

Note

When upgrading multiple management servers in a distributed management group, sequence the upgrades in a manner that best suits your business needs. Upgrade all management servers in the distributed management group as soon as possible after the initial management server is upgraded to verify that your upgraded environment is healthy.

To upgrade a management server

1. Log on to the Operations Manager management server with an account that is a member of the Operations Manager Administrators role for your Operations Manager management group and a local administrator on the computer.
2. From the Operations Manager media, run **Setup.exe**, and then click **Install**. The **Getting Started** page displays information about which features will be upgraded.
3. On the **Getting Started, Operations Manager 2012 Upgrade** page, click **Next** to proceed with the upgrade.
4. On the **Getting Started, Please read this license agreement** page, read the Microsoft Software License Terms, click **I have read, understood, and agree with the terms of the license agreement**, and then click **Next**.
5. On the **Getting Started, Select installation location** page, accept the default value of **C:\Program Files\System Center Operations Manager 2012**, or type in a new location, or browse to one. Then click **Next**.
6. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify prerequisites again** to recheck the system.
7. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites, Proceed with Setup** page appears. Click **Next**.
8. On the **Configuration, Configure Operations Manager accounts** page, enter the credentials for a domain account, and then click **Next**
9. Review the **Configuration, Ready To Upgrade** page, and then click **Upgrade**. The upgrade proceeds and displays the upgrade progress.
10. When the upgrade is finished, the **Upgrade complete** page appears. Click **Close**.

Note

Upgrading a management server is just one phase of the distributed upgrade process. Upgrade is not completed until you have upgraded all of the other features in your management group. The next step is to upgrade any gateways. See How to Upgrade a Gateway Server to System Center 2012 SP1 - Operations Manager for more information.

To upgrade a management server by using the Command Prompt window

1. Log on to the management server with an account that is a member of the Operations Manager Administrators role for your Operations Manager management group and a local administrator on the computer.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the Operations Manager setup.exe file is located, and run the following command.

Important

The following commands assume that you specified the Local System account

for the Data Access service (`/UseLocalSystemDASAccount`). To specify a domain\user name for these accounts, you must provide the following parameters instead.`/DASAccountUser: <domain\username> /DASAccountPassword: <password>`

```
setup.exe /silent /upgrade
/AcceptEndUserLicenseAgreement:1
/UseLocalSystemDASAccount
/DataReaderUser:<domain\user>
/DataReaderPassword:<password>
```

After you have upgraded all of the management servers in your management group, you should upgrade any gateways, and then upgrade any stand-alone operations consoles.

How to Upgrade an ACS Collector to System Center 2012 SP1 - Operations Manager

Perform this procedure to upgrade the Audit Collection Services (ACS) Collector to System Center 2012 Service Pack 1 (SP1), Operations Manager locally on the ACS Collector. During this procedure, the ACS database is also upgraded without any additional steps.

Warning
A computer that hosts an ACS Collector must also be an Operations Manager management server or gateway server.

Before you begin the upgrade process, make sure that your server meets the minimum supported configurations. For more information, see System Requirements: System Center 2012 SP1 - Operations Manager.

To upgrade an ACS Collector

1. Log on to the computer that hosts the ACS Collector with an Operations Manager Administrators role account for your Operations Manager management group.
2. On the Operations Manager media, run **Setup.exe**.
3. In the **Install** section, click **Install Audit Collection Server**. The Audit Collection Services Setup wizard starts.
4. On the **Welcome to the Audit Collection Services Collector Setup Wizard** page, click **Next**.
5. On the **Database Installation Options** page, select **Use an existing database**, and then click **Next**.
6. On the **Data Source** page, type the name that you used as the Open Database Connectivity data source name for your ACS database in the **Data source name** box. By default, this name is **OpsMgrAC**. Click **Next**.

7. On the **Database** page, if the database is on a separate server than the ACS Collector, click **Remote Database Server**, and then type the computer name of the database server that will host the database for this installation of ACS. Otherwise, click **Database server running locally**, and then click **Next**.
8. On the **Database Authentication** page, select one authentication method. If the ACS Collector and the ACS database are members of the same domain, you can select **Windows authentication**; otherwise, select **SQL authentication**, and then click **Next**.

   Note
   If you select **SQL authentication** and click **Next**, the **Database Credentials** page appears. Enter the name of the user account that has access to the SQL Server in the **SQL login name** box and the password for that account in the **SQL password** password box, and then click **Next**.
9. The **Summary** page displays a list of actions that the installation program will perform to upgrade ACS. Review the list, and then click **Next** to begin the installation.

   Note
   If a **SQL Server Login** dialog box appears and the database authentication is set to **Windows Authentication**, select the correct database, and then verify that the **Use Trusted Connection** check box is selected. Otherwise, clear it, enter the SQL Server login name and password, and then click **OK**.
10. When the upgrade is finished, click **Finish**.

How to Upgrade a Gateway Server to System Center 2012 SP1 - Operations Manager

After you upgrade the management servers in your management group, you upgrade any gateway servers. The procedure to upgrade a gateway server to System Center 2012 Service Pack 1 (SP1), Operations Manager is performed locally on the gateway server. You can then verify whether the upgrade is successful.Before you begin the upgrade process, make sure that your gateway server meets the minimum supported configurations. For more information, see System Requirements: System Center 2012 SP1 - Operations Manager.

To upgrade a gateway server

1. Log on to a computer that hosts the gateway server with an Operations Manager Administrators role account for your Operations Manager management group.
2. On the System Center 2012 – Operations Manager media, run **Setup.exe**.
3. In the **Optional Installations** area, click **Gateway management server**.
4. On the **Welcome to the System Center 2012 - Operations Manager Gateway Upgrade Wizard** page, click **Next**.
5. On the **The wizard is ready to begin gateway upgrade** page, click **Upgrade**.

6. On the **Completing the System Center 2012 - Operations Manager Gateway Setup wizard** page, click **Finish**.

To upgrade a gateway server by using the Command Prompt window

1. Log on to a computer that is hosting the gateway server with an Operations Manager Administrators role account for your Operations Manager management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the directory to the System Center 2012 – Operations Manager installation media and change directory again to gateway\AMD64, where the MOMGateway.msi file is located.
4. Run the following command where D:\ is the location for the upgrade log file.

```
msiexec /i MOMgateway.msi /qn /l*v D:\logs\GatewayUpgrade.
log
AcceptEndUserLicenseAgreement=1
```

To verify the gateway server upgrade

1. In the Operations console, in the navigation pane, click the **Administration** button.
2. Under **Device Management**, click **Management Servers**.
3. In the **Management Servers** pane, verify that the value listed in the **Version** column is 8925 (89xx), where x is any positive integer.

After you have upgraded all of the gateways in your management group, you can upgrade the stand-alone operations consoles. See How to Upgrade an Operations Console to System Center 2012 SP1 - Operations Manager for more information.

How to Upgrade an Operations Console to System Center 2012 SP1 - Operations Manager

This procedure upgrades a stand-alone Operations console to System Center 2012 Service Pack 1 (SP1), Operations Manager. Perform this procedure locally on the computer that has a stand-alone Operations console installed. You do not have to perform this procedure to upgrade Operations consoles that are installed locally on a management server.

Before you begin the upgrade process, make sure that your server meets the minimum supported configurations. For more information, see System Requirements: System Center 2012 SP1 - Operations Manager.

To upgrade a stand-alone Operations console

1. Log on to the computer that hosts the Operations console with an Operations Manager Administrators role account for your Operations Manager management group.

2. On the Operations Manager source media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started**, **System Center 2012 - Operations Manager Upgrade** page, click **Next**.
4. On the **Getting Started**, **Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager**, or type in a new location or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that are returned by the Prerequisites checker, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration**, **Ready To Upgrade** page, click **Upgrade**.
8. When the upgrade is finished, the **Upgrade complete** page appears. Click **Close**.

To upgrade a stand-alone Operations console by using the Command Prompt window

1. Log on to the computer that hosts the Operations console with an Operations Manager Administrators role account for your Operations Manager management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change to the path to the Operations Manager source media, and run the following command.

```
Setup.exe /silent / upgrade /AcceptEndUserLicenseAgreement:1
```

To verify the Operations console upgrade

1. On the Windows desktop, click **Start**, and then click **Run**.
2. Type **regedit**, and then click **OK**. The Registry Editor starts.

   Caution
   Incorrectly editing the registry can severely damage your system. Before you make changes to the registry, you should back up any valued data that is on the computer.
3. Browse to the **HKey_Local_Machine\Software\Microsoft\Microsoft Operations Manager\3.0\Setup** key. If the value of the **UIVersion** entry is **8925 (89xx)**, where **x** is any positive integer, the Operations console was upgraded successfully.

After you have upgraded all of the stand-alone operations consoles in your management group, you can upgrade the agents. See How to Upgrade an Agent to System Center 2012 SP1 - Operations Manager for more information.

How to Upgrade an Agent to System Center 2012 SP1 - Operations Manager

Use the following procedures to upgrade to System Center 2012 Service Pack 1 (SP1), Operations Manager agents. You should first verify that the agents meet minimum supported configurations. For more information, see System Requirements: System Center 2012 SP1 - Operations Manager.

Note
If before upgrade an agent was installed using the push install method, after the server the agent will be put into a pending update state and can be upgraded through the Console. Otherwise the agent should be upgraded manually.

When you upgrade an agent, the Operations Manager installer service runs and is not removed until after the completion of the upgrade. If the agent upgrade fails, you might have to re-install the agent because the installer service was not properly removed. If you attempt to upgrade the agent again and it fails, you should re-install the agent after you have completed upgrading all features of Operations Manager.

Note
If you have Audit Collection Services (ACS) enabled for an agent prior to this upgrade, it is disabled as part of the agent upgrade process. ACS must be re-enabled after upgrade completes.

If you are upgrading agents that are deployed to a computer that has other System Center 2012 Service Pack 1 (SP1), Operations Manager features installed, you must do the following:

- If the agent is installed on a computer that has System Center 2012 Service Pack 1 (SP1), Operations Manager Operations console or web console installed, you must first uninstall the consoles before you upgrade the agents. You can do this by uninstalling System Center 2012 Service Pack 1 (SP1), Operations Managerin Programs and Features. You can reinstall these consoles after upgrade is completed.

Note
If UAC is enabled, you must run the agent upgrade from an elevated command prompt.

Note
Information about upgraded agents might not appear in the Operations console for up to 60 minutes after performing the upgrade.

Upgrading Push-Installed Agents

Push-installed agents are agents that were installed by using the **Computer and Device Management Wizard**. Use the following procedures to upgrade these agents.

To upgrade push-installed Windows agents by using the Operations console

1. Log on to the computer hosting the Operations Manager Operations console. Use an

account that is a member of the Operations Manager Administrators role for the Operations Manager management group.

2. In the Operations console, click **Administration**.

   Note
   When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the management server to which you want to connect.

3. In the **Administration** workspace, in the navigation pane under **Device Management**, click **Pending Management**.
4. In the **Pending Management** pane, under **Type: Agent Requires Update**, right-click each agent-managed computer listed, and then click **Approve**.

   Warning
   You should not approve more than 200 agents at one time.

5. In the **Update Agents** dialog box, enter the administrator account credentials, and then click **Update**. The upgrade status is displayed in the **Agent Management Task Status** dialog box.
6. When the upgrade is completed, click **Close**.

Upgrading Manually Installed Agents

Manually-installed agents are agents that were installed manually, either by using the Command Prompt window, or by using the MOMAgent.msi Setup Wizard. Use the following procedure to upgrade these agents.

To upgrade a manually installed Windows agent by using the Setup Wizard

1. Log on to the computer that hosts the agent with an Operations Manager Administrators role account for your Operations Manager management group.
2. Run **Setup.exe** from the Operations Manager installation media.
3. On the first page of the Setup Wizard, click **Local agent**. When the **Welcome to the System Center Operations Manager 2012 Agent Upgrade Wizard** page opens, click **Next**.
4. In the **System Center Operations Manager 2012 Agent Setup** dialog box, click **Upgrade**. The status page displays the progress of the upgrade.
5. When the **Completing the System Center Operations Manager 2012 Agent Setup Wizard** page appears, click **Finish**.

To upgrade a manually installed Windows agent by using the Command Prompt window

1. Log on to the computer that hosts the agent with an Operations Manager Administrators role account for your Operations Manager management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.

3. Run the following command, where D:\ is the location for the upgrade log file.

```
msiexec /i MOMAgent.msi /qn /l*v D:\logs\AgentUpgrade.log
 AcceptEndUserLicenseAgreement=1
```

Verifying Windows Agent Upgrade

To verify the Windows agent upgrade

1. In the Operations console, in the navigation pane, click the **Administration** button.
2. Under **Device Management**, click **Agent Managed**.
3. In the Agent Managed pane, verify that the value listed in the Version column is 8925 (89xx), where x is any positive integer.

   Note
   It can take up to one hour for the console to show the updated version of the agent.

Upgrading UNIX and Linux Agents

To upgrade UNIX and Linux agents

- In the Operations console, in the **Administration** pane, run the **UNIX/Linux Upgrade Wizard**.

  Any existing Run As profiles and Run As accounts continue to have valid configurations. For information about changes to Run As profiles and accounts for UNIX and Linux monitoring in System Center 2012 Service Pack 1 (SP1), Operations Manager, see Accessing UNIX and Linux Computers in Operations Manager

To manually upgrade UNIX and Linux agents

1.

To verify the UNIX or Linux agent upgrade

1. In the Operations console, in the navigation pane, click the **Administration** button.
2. Under **Device Management**, click **UNIX/Linux Computers**.
3. Verify that the value listed in the Agent **Version** column is 1.4.0-xxx, where x is any positive integer.

   Note
   It can take up to one hour for the console to show the updated version of the agent.

How to Upgrade a Web Console to System Center 2012 - Operations Manager

If you have a stand-alone System Center 2012 – Operations Manager web console server, you can upgrade it to System Center 2012 Service Pack 1 (SP1), Operations Manager.

Before you begin the upgrade process, make sure that your server meets the minimum supported configurations. For more information, see System Requirements: System Center 2012 SP1 - Operations Manager.

Note

When you upgrade the web console, any customizations that were made to the web.config file after the web console was installed will be reset.

If you made changes after you set up your web console to either enable or disable Secure Sockets Layer (SSL), the SSL settings will be reset during upgrade. To resolve the issue, you must make changes to the registry key before you upgrade the web console, as follows:

To set the registry to enable or disable SSL on the web console

1. Logon on to the web console with an account that has local administrator rights, and on the desktop, click **Start**, and then click **Run**.
2. Type **regedit**, and then click **OK**. The Registry Editor starts.

   Caution

   Incorrectly editing the registry can severely damage your system. Before you make changes to the registry, you should back up any valued data that is on the computer.
3. Navigate to the **HKey_Local_Machine\Software\Microsoft\System Center Operations Manager\12\Setup\WebConsole** key.
4. To enable SSL, set the following:

   HTTP_GET_ENABLED=0

   BINDING_CONFIGURATION=DefaultHttpsBinding
5. To disable SSL, set the following:

   HTTP_GET_ENABLED=1

   BINDING_CONFIGURATION=DefaultHttpBinding

To upgrade the web console server

1. Log on to the computer that hosts the web console server with an Operations Manager Administrators role account for your Operations Manager management group.
2. On the Operations Manager source media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started**, **System Center 2012 - Operations Manager Upgrade** page,

review the features that will be upgraded, and then click **Next**.

4. On the **Select installation location** page, accept the default value of **C:\Program Files\System Center Operations Manager 2012**, or type in a new location or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
7. When the **Ready to Upgrade** page appears, review the upgrade summary, and then click **Upgrade**.

To upgrade the web console server by using the Command Prompt window

1. Log on to the computer that hosts the web console server with an Operations Manager Administrators role account for your Operations Manager management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the Operations Manager Setup.exe file is located, and run the following command.

   Important
   Use the `/WebConsoleUseSSL` parameter only if your website has Secure Sockets Layer (SSL) activated. For a default web installation, specify **Default Web Site** for the `/WebSiteName` parameter.

```
setup.exe /silent /AcceptEndUserLicenseAgreement:1 /upgrade
/WebsiteName: "<WebSiteName>" [/WebConsoleUseSSL]
/WebConsoleAuthorizationMode: [Mixed|Network]
```

How to Upgrade Reporting to System Center 2012 - Operations Manager

Use this procedure to upgrade a stand-alone Reporting server to System Center 2012 Service Pack 1 (SP1), Operations Manager. You should not run upgrade on the Reporting server until after you have upgraded the management servers, gateways, operation consoles, and agents.

Before you begin the upgrade process, make sure that your server meets the minimum supported configurations. For more information, see System Requirements: System Center 2012 SP1 - Operations Manager.

To upgrade the Reporting server

1. Log on to the computer that hosts the Reporting server with an account that is a member of the Operations Manager Administrators role for your Operations Manager management group.
2. On the Operations Manager source media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started**, **System Center 2012 - Operations Manager Upgrade** page, review the features that will be upgraded. In this case, it is Operations Manager Reporting. Click **Next**.
4. On the **Select installation location** page, accept the default value of **C:\Program Files\System Center Operations Manager 2012**, or type in a new location or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
7. On the **Ready to Upgrade** page, review the options, and then click **Upgrade**.
8. When upgrade is finished, the **Upgrade complete** page appears. Click **Close**.

To upgrade the Reporting server by using the command prompt

1. Log on to the computer that hosts the Reporting server with an account that is a member of the Operations Manager Administrators role for your Operations Manager management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the Operations Manager Setup.exe file is located, and run the following command:

   Note
   If the Reporting server reports to an unsupported or inaccessible root management server, you must also pass the following parameter: `/ManagementServer: <ManagementServerName>`.

```
setup.exe /silent /AcceptEndUserLicenseAgreement:1 /upgrade
/ManagementServer: <ManagementServerName>
```

Post-Upgrade Tasks When Upgrading to System Center 2012 SP1 - Operations Manager

After you have completed the upgrade process to System Center 2012 Service Pack 1 (SP1), Operations Manager, you must perform a number of post-upgrade tasks.

Post-Upgrade Tasks

Perform the following tasks when you have completed the upgrade process.

1. Re-enable the Notification Subscriptions.
2. Restart or Re-enable the Connector Services (if needed)
3. Re-enable Audit Collection Services (ACS) on agents that were upgraded
4. Verify That the Upgrade Was Successful

Re-enable the Notification Subscriptions

After the upgrade has finished, use the following procedure to re-enable subscriptions.

To re-enable the subscriptions

1. Open the Operations console by using an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, in the navigation pane, click the **Administration** button.

   Note
   When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** text box, type the name of the Operations Manager management server to which you want to connect.
3. In the **Administration** pane, under **Notifications**, click **Subscriptions**.
4. In the **Actions** pane, click **Enable** for each subscription listed.

Restart or Re-enable the Connector Services

Refer to the third-party documentation for any installed connectors to determine if the connectors are supported for System Center 2012 Service Pack 1 (SP1), Operations Manager. If you stopped a connector for any reason during upgrade, restart the service.

To restart a connector service

1. On the taskbar, click **Start**, click **Administrative Tools**, and then click **Services**.
2. In the **Name** column, right-click the connector that you want to restart, and then click **Start**.

Re-Enable Audit Collection Services

If you had Audit Collection Services (ACS) enabled for an agent prior to upgrade, it was disabled as part of the agent upgrade process. Re-enable ACS as appropriate.

Verify That the Upgrade Was Successful

Perform the following tasks to verify that the upgrade was successful.

- Check the health state of the management servers and agents in the Health Service Watcher state view. In the **Administration** workspace of the Operations console, ensure that the management servers and agents are healthy. In the **Monitoring** workspace, check if there are any alerts related to the management group health.
- Review the event logs of all the management servers for new errors.
- Sort alerts by the last-modified column to review the new alerts.
- Check the CPU utilization and disk I/O on your database servers to ensure that they are functioning normally.
- If the Reporting feature is installed, click **Reporting**, and then run a generic performance report to ensure that Reporting is functioning correctly.
- Re-deploy any agents that you uninstalled during the upgrade process.

How to Upgrade OM2007 R2 Agents to OM2012 SP1 - Parallel Environments

This upgrade path contains an Operations Manager scenario with parallel environments, sharing agents, so that the original Operations Manager 2007 R2 environment is left intact. After the upgrade, the agents have been upgraded to System Center 2012 Service Pack 1 (SP1), Operations Manager and are fully capable of working with native System Center 2012 Service Pack 1 (SP1) functionality. The SP1 agents are also able to “talk” to the Operations Manager 2007 R2 management server.

Important

In this parallel environment scenario, we support upgrade of Operations Manager 2007 R2 agents with the latest cumulative update (CU6).

Upgrading OM 2007 R2 Agents to OM2012 SP1 using Parallel Environments

If you want to maintain your Operations Manager 2007 R2 environment you can install System Center 2012 Service Pack 1 (SP1), Operations Manager in parallel and just upgrade your agents using the following process.

1. Retain the original Operations Manager 2007 R2 environment.
2. Set up an additional, new System Center 2012 Service Pack 1 (SP1), Operations Manager environment with management servers, gateway, Operations Manager Database, Operations Manager Data Warehouse, console, web console, and reporting server. See Deploying System Center 2012 - Operations Manager for more information.
3. Upgrade the Operations Manager 2007 R2 Agents to 2012 SP1 using Push-Install or Command Line options as appropriate. See How to Upgrade an Agent to System Center 2012 SP1 - Operations Manager for more information.

Deploying System Center 2012 - Operations Manager

The Deployment Guide contains information to help you:

1. Plan for and deploy System Center 2012 – Operations Manager
2. Plan for and deploy System Center 2012 Service Pack 1 (SP1), Operations Manager
3. Upgrade from Operations Manager 2007 R2
4. Maintain the Operations Manager infrastructure

Deploying Operations Manager consists of several phases, such as a design phase, testing phase, and a deployment phase. If you already have Operations Manager 2007 R2 implemented and want to move to System Center 2012 – Operations Manager, or have System Center 2012 – Operations Manager implemented and you want to move to System Center 2012 Service Pack 1 (SP1), you will go through several phases of upgrade, depending on your current topology. After you upgrade or deploy the product directly, you might want to make changes to your Operations Manager environment.

Tasks

The following topics introduce the task areas covered in the Deployment Guide:

- Planning the System Center 2012 - Operations Manager Deployment
- Deploying System Center 2012 - Operations Manager
- Upgrading to System Center 2012 - Operations Manager
- Maintaining the System Center 2012 - Operations Manager Infrastructure

For upgrade procedures to System Center 2012 Service Pack 1 (SP1), see the guide Upgrading System Center 2012 – Operations Manager to System Center 2012 SP1.

Downloadable Documentation

You can download a copy of this technical documentation from the Microsoft Download Center. Always use the TechNet library for the most up-to-date information.

Planning the System Center 2012 - Operations Manager Deployment

This section provides information on major concepts to consider in the design and planning phase. This document provides high level scenarios, and points to details found throughout the Deployment Guide for System Center 2012 – Operations Manager as well as the Operations Manager Sizing Helper and specific concepts and procedures found in the Operations Guide for System Center 2012 – Operations Manager.

Before You Begin

Before deploying, there are several sources of information you should read that are helpful for gaining context about Operations Manager functionality and requirements:

- **Getting Started**

  Provides a learning roadmap intended for the operator in a Tier I role

- System Requirements for System Center 2012 - Operations Manager

  Provides information about the supported operating systems, hardware configurations, software requirements, installation combinations, and security configurations - This document focuses on the system requirements and only mentions unsupported configurations when necessary

Designing and Planning for Deployment Scenarios

This document contains the following sections:

- Considerations when Upgrading to System Center 2012 - Operations Manager

  Covers key concepts and considerations for upgrading to System Center 2012 – Operations Manager

- Considerations for a Clean Installation of System Center 2012 – Operations Manager

  Covers key concepts and common configurations for a new, clean installation of System Center 2012 – Operations Manager

- Considerations when Designing a Management Group for Network Monitoring

  Covers key concepts and considerations for discovering and monitoring network routers and switches, including the network interfaces and ports on those devices and the virtual LAN (VLAN) that they participate in

- Considerations for Application Performance Monitoring

  Covers key concepts and considerations for monitoring Internet Information Services (IIS)-hosted .NET applications from server- and client-side perspectives in getting details about application performance and reliability that can help you pinpoint root causes of incidents

- Considerations for High Availability and Disaster Recovery

  Covers key concepts to consider when designing for disaster recovery

Considerations when Upgrading to System Center 2012 - Operations Manager

This section of the Design and Planning material covers key concepts and considerations for upgrading to System Center 2012 – Operations Manager or System Center 2012 Service Pack 1 (SP1), Operations Manager. Complete upgrade scenarios and procedures are found in Upgrading to System Center 2012 - Operations Manager.

The supported upgrade path is from System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager, and then to System Center 2012 Service Pack 1 (SP1), so customers may have to perform multiple upgrades. Considerations when performing multiple

upgrades include system requirements that do or do not overlap between System Center 2012 – Operations Manager and SP1. For example, you will want to consider what versions of SQL Server are supported and how moving across versions of SQL Server will be required as you upgrade across versions of Operations Manager.

If you have not reviewed **Getting Started** or System Requirements for System Center 2012 - Operations Manager, you may want to before continuing. These documents contain key concepts and important configuration details you will find helpful as an upgrading customer.

Note

Unified Installer is a utility designed to perform new, clean installations of System Center 2012 for testing and evaluation purposes only. If you want to upgrade from an existing System Center installation or choose any set up options such as high availability or multi-server component installs, we recommend you refer instead to the procedures detailed in the deployment guides for each individual System Center 2012 component.

RMS Removal and the New RMS Emulator

In Operations Manager, the single largest change impacting design and planning is the removal of the root management server (RMS). All management servers are peers now that there is no RMS. Therefore, the RMS is no longer a single point of failure as all management servers host the services previously hosted only by the RMS. Roles are distributed to all the management servers. If one management server becomes unavailable, its responsibilities are automatically redistributed. An RMS emulator role provides for backwards compatibility for management packs targeting the RMS. If you do not have any management packs that previously targeted the RMS, you will not need to make use of the RMS Emulator.

Preparing for Upgrade

Before upgrade:

Important

Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see Supported Configurations for System Center 2012 – Operations Manager.

In a distributed management group upgrade, you upgrade the secondary management servers, the gateways, and agents. The order of agent upgrade depends on how the agents were deployed. If you installed the agents manually, you upgrade the agents before you upgrade the management servers and gateways.

1. Remove Agents from Pending Management
2. Check the Operations Manager 2007 R2 RMS for Active Connected Console
3. Disable Notification Subscription

4. Stop the Connector Services or Disable any Connector

These procedures are outlined in detail in Pre-Upgrade Tasks for Operations Manager

AD Integration and Agents

If you have any agents reporting to the RMS, move them to secondary management servers to take the agent work. It is important to manually upgrade your agents first. These procedures are outlined in detail in Checklist: Distributed Upgrade (Complex)

Data Warehouse

Data warehouse is now required; this is new for System Center 2012 – Operations Manager and is included in all sizing scenarios in the Operations Manager Sizing Helper

While upgrading, the UI will direct you to add a data warehouse if one does not exist.

Resource Pools

A resource pool is a collection of management servers, or gateway servers, used to distribute work amongst themselves and take over work from a failed member.

Due to the introduction of resource pools, we recommend that all management servers be connected by a low latency network. This means that if you are currently using management servers in multiple datacenters or sites we recommend you move all management servers to a single data center and use gateway servers at the other sites.

You should always have two management servers in ANY environment. A second management server allows for failover and easy restore. All management servers are members of the All Management Servers Resource pool, which balances the monitoring load of your management group as new management servers are added, and provides automatic failover for monitoring. SeeDistributed Deployment of Operations Manager for complete details.

Make sure the SDK Service is running on all management servers and that any SDK client (console, web console, connector, PowerShell) can connect to it. In System Center 2012 – Operations Manager, setup sets this service to automatically start on every management server during installation. We support any SDK client connecting to any management server.

Network Monitoring

See Considerations when Designing a Management Group for Network Monitoring for information regarding management packs and running Network Discovery.

Considerations for a Clean Installation of System Center 2012 – Operations Manager

The Deployment Guide for System Center 2012 - Operations Manager covers the full details of installing Operations Manager, in two installation scenarios:

1. Single-Server Deployment of Operations Manager - for evaluation, testing, and management pack development, usually in nonproduction or preproduction environments
2. Distributed Deployment of Operations Manager - forms the foundation of 99 percent of Operations Manager deployments. It allows for the distribution of features and services across multiple servers to allow for scalability. It can include all Operations Manager server roles and supports the monitoring of devices across trust boundaries through the use of the gateway server

For the purposes of design and planning this topic will focus on design considerations for a distributed deployment making use of multiple management servers and the use of resource pools.

If you have not reviewed **Getting Started** or System Requirements for System Center 2012 - Operations Manager, you may want to before continuing. These documents contain key concepts and important configuration details.

Note

Unified Installer is a utility designed to perform new, clean installations of System Center 2012 for testing and evaluation purposes only. If you want to upgrade from an existing System Center installation or choose any set up options such as high availability or multi-server component installs, we recommend you refer instead to the procedures detailed in the deployment guides for each individual System Center 2012 component.

Common Installations

Use the Operations Guide for Operations Manager for System Center 2012 to determine hardware requirements for each Operations Manager server feature. If you want to install more than one feature on the same computer, use the higher of the recommended hardware requirements for any of the combined features.

The sizing helper is a downloadable tool in spreadsheet format that contains tabs listing general information on supported configurations, as well as sizing examples based on number of agents and number of network devices monitored, information on gateway servers, and more.

For example, a scenario calling for 500 agents monitoring 50 network devices calls for a recommendation of:

1. (1) One management server managing up to 500 agents handling the entire workload, plus (1) one additional management server for HA / failover, managing up to five SDK connections
2. (2) Two management servers in a single resource pool monitoring the 50 network devices
3. (2) Two servers: An Operations Database Server, and an Operations Data Warehouse Server (with an SRS and Web Console Server)

Not included in this scenario is the possible need for a gateway server. They are supported for use in managing network devices, but the gateway server must be in its own resource pool, and not in the same pool as the devices.

Resource Pools

A resource pool is a collection of management servers or gateway servers used to distribute work amongst themselves and to take over work from a failed member.

Due to the introduction of resource pools it is recommended that all management servers be connected by a low latency network. This means that if you are currently using management servers in multiple datacenters or sites we recommend you move all management servers to a single data center and use gateway servers at the other sites.

You should always have two management servers in ANY environment. A second management server allows for failover and easy restore. All management servers are members of the All Management Servers Resource pool, which balances the monitoring load of your management group as new management servers are added, and provides automatic failover for monitoring. See Distributed Deployment of Operations Manager for complete details.

Make sure the SDK Service is running on all management servers and that any SDK client (console, web console, connector, PowerShell) can connect to it. In System Center 2012 – Operations Manager, setup sets this service to automatically start on every management server during installation. Any SDK client can connect to any management server.

Considerations when Designing a Management Group for Network Monitoring

System Center 2012 – Operations Manager provides the ability to discover and monitor network routers and switches, including the network interfaces and ports on those devices and the virtual LAN (VLAN) that they participate in. You can also delete discovered network devices and prevent the deleted network devices from being rediscovered the next time discovery runs. For more information, see Monitoring Networks by Using Operations Manager.

Resource Pools

Network monitoring in System Center 2012 – Operations Manager requires its own separate resource pool.

Create a resource pool dedicated to network management; add dedicated management servers into the newly created resource pool, then remove the dedicated management server from any other resource pool.

1. Each management server or gateway server can run only one discovery rule. You specify a single management server or gateway server to run the discovery rule and a management server resource pool to perform the actual monitoring of the network devices.
2. If you create discovery rules on multiple management servers, you should create a management pool for each and make sure that each discovery defines a different set of devices. If a single device is managed in different pools, it will not be able to be deleted.

For more information see How to Discover Network Devices in Operations Manager and Network Device Discovery Settings.

Performance and Scale

Because network monitoring workflows run on management servers (on the SNMP module), and not on agents, a heavy load is placed on the management servers. Therefore for better performance we recommend using dedicated management servers in dedicated resource pools for network monitoring.

For more information see the Operations Manager Sizing Helper.

Network Device Accessibility

Network devices must be accessible by the management servers during monitoring.

1. Any firewalls between the management servers and the devices must be considered in planning, and when setting up dedicated resource pools.
2. Gateway servers are supported for use in managing network devices, but the gateway server must be in its own resource pool, and not in the same pool as the devices.

Upgrade

If you were monitoring network devices in Operations Manager 2007 R2 and are upgrading toSystem Center 2012 – Operations Manager, the network monitoring you were performing will still function properly. But if you want to take advantage of the additional monitoring capabilities available when upgrading, you will need to rerun network device discovery. However, you must also upgrade any appropriate management packs. See Monitoring Networks by Using Operations Manager for more information. If upgrading management packs is not an option, then do not rerun discovery: continue to operate under the original management packs and the original network monitoring capabilities you had under Operations Manager 2007 R2.

See Also

Security for Servers Performing Network Discovery

Tuning Network Monitoring

Considerations for Application Performance Monitoring

In Operations Manager, you can monitor Internet Information Services (IIS)-hosted .NET applications from server- and client-side perspectives to get details about application performance and reliability that can help you pinpoint root causes of incidents. For more information, see .NET Application Performance Monitoring Template in the Authoring Guide and Monitoring .NET Applications in the Operations Guide.

Operations Database

The primary consideration for application performance monitoring on design and planning is its impact on the database. Since application performance monitoring in Operations Manager is Health Service based, scale and load put on the Operations Manager Database is an important factor to consider.

For example, when monitoring many applications that generate several events (state changes) each per second, it is easy to see how the Health Services can be overloaded if not considered in the design phase. For example, the average application generates 0.3 events per second. With IIS supporting hundreds of applications per host it can result in 30 or more events being raised per second through the Health Service.

For more information see Operations Manager Sizing Helper and **How to Configure Grooming Settings for the Operations Manager Database**.

Agents

Application performance monitoring is not agentless, so using resource pools is not a design option for optimizing performance or scale. The application monitoring agent is installed at the same time as the Operations Manager agent. You do not have to pre-plan where to install the application monitoring service.

Upgrade

For AVIcode 5.7 customers, there are two ways to look at an upgrade:

1. Integrated (AVIcode integrated with Operations Manager), where Operations Manager handles some of the configuration steps
2. Standalone (Continuing to run AVIcode 5.7 as a separate product from Operations Manager)

For more information, see Notes for AVIcode 5.7 Customers in the Operations Guide.

Note: Installation of AVIcode 5.7 integration management packs is NOT supported in System Center 2012 – Operations Manager. If you need to use AVIcode 5.7 with System Center 2012 – Operations Manager, for example to monitor IIS 6 hosts, the management packs must be installed on the System Center Operations Manager 2007 R2 environment before upgrading to System Center 2012 – Operations Manager. Additionally, you need to import an update for the AVIcode 5.7 management packs from the System Center 2012 – Operations Manager installation media.

See Also

Monitoring .NET Applications

Considerations for High Availability and Disaster Recovery

This section describes key concepts to consider when designing for disaster recovery. Using multiple management servers and the concept of resource pools, it is possible to easily set up for successful failover scenarios.

Multiple Management Servers and Distributed Deployment

You should always have two management servers in ANY environment. A second management server allows for failover and easy restore, and a second management server can take on the load if one fails. All management servers are members of the All Management Servers Resource

pool, which balances the monitoring load of your management group as new management servers are added, and provides automatic failover for monitoring. The impact of failure of a management server in a distributed environment is minimized, but it increases the workload on additional management servers in the management group until the failed management server is restored. See Distributed Deployment of Operations Manager in the Deployment Guide for complete details.

You should always keep a backup of your operational database and data warehouse databases. For information about scheduling regular backups of the Operations Manager databases, see How to Schedule Backups of System Center 2012 - Operations Manager Databases.

You must keep SDK services running on all management servers.

See Also

Operations Manager Sizing Helper

Deploying System Center 2012 - Operations Manager

All System Center 2012 – Operations Manager individual management group deployments will either be an "all-in-one" installation, where all features are loaded on a single server, or the deployment will be a distributed installation, where Operations Manager features are distributed across servers. Any number of these can then be combined together to form an overall Operations Manager infrastructure that consists of multiple management groups. These management groups can then relate to each other in a hierarchical fashion as your business needs dictate.

This section of the Deployment Guide describes an individual management group deployment, where you have one management group, but the features of Operations Manager are either installed on a single server or distributed over several servers.

- Single-Server Deployment of Operations Manager
- Distributed Deployment of Operations Manager

For information about connecting management groups, see Connecting Management Groups in Operations Manager.

Before You Begin

Before you begin your deployment, you should read the release notes, and ensure that your server meets the minimum system requirements for Operations Manager. For more information, see:

- Release Notes for System Center 2012 - Operations Manager
- System Requirements for System Center 2012 – Operations Manager

Operations Manager Administrators Role Assignment

Operations Manager handles assignment of the Operations Manager Administrators role differently than previous versions. In System Center 2012 – Operations Manager, Setup automatically assigns the Administrators group on the local computer to the Operations Manager Administrators role. You must be logged on with an account that has local Administrator rights to run Setup on the first management server that you install; this ensures that you can open the Operations console after Setup is completed. When you install additional management servers, you must use a Domain account of which you are a member.

Required Accounts

During setup, you are prompted for two accounts, the **management server action account** and the **System Center Configuration service and System Center Data Access service** account. In Operations Manager, you can use the same account for both services.

If you install Reporting, you are prompted for two additional accounts, **the Data Warehouse Write account** and the **Data Reader account**. These accounts are created as domain user accounts and added to the local Administrators group on the target server.

Note

If you create a specific account for installation, this account must be a member of the **sysadmin** server role for Microsoft SQL Server, but also have access to the master database.

Note

If you install multiple management servers, you are prompted for a **management server action account** and a **System Center Configuration service and System Center Data Access service account** each time you add a management server. You must provide the same accounts for each installation.

Account	Description	Permissions
Management server action account	This account is used to carry out actions on monitored computers across a network connection.	To save time, specify a domain-based account. We recommend that you create an account for this purpose that has local administrative credentials. You should not use an account that has domain administrative credentials.
System Center Configuration service and System Center Data Access service account	This account is one set of credentials that is used to update and read information in the operational database. Operations Manager ensures	This account can be configured as either Local System or as a domain account. The account must have local administrative credentials. For cases where the

Account	Description	Permissions
	that the credentials used for the System Center Data Access service and System Center Configuration service account are assigned to the sdk_user role in the operational database.	operational database is hosted on a remote computer that is not a management server, a domain account must be used. For better security, we recommend that you use an account different from the one used for the management server action account.
Data Warehouse Write account	The Data Warehouse Write account writes data from the management server to the Reporting data warehouse and reads data from the operational database.	This account is assigned write permissions on the Data Warehouse database and read permissions on the operational database. **Note** Ensure that the account you plan to use for the Data Warehouse Write account has SQL Server Logon rights and has logon rights for the computers hosting both the operational database and the reporting data warehouse. Otherwise, Setup fails, and all changes are rolled back. This might leave SQL Server Reporting Services in an inoperable state.
Data Reader account	The Data Reader account is used to define which account credentials SQL Server Reporting Services uses to run queries against the Operations Manager reporting data warehouse.	The account should be configured as a domain account. **Note** Ensure that the account you plan to use for the Data Reader account has SQL Server logon rights and Management Server logon rights.

SQL Server Requirements

System Center 2012 – Operations Manager requires access to an instance of a server running Microsoft SQL Server 2008 SP1, SQL Server 2008 R2, or SQL Server 2008 R2 SP1. This instance can be located on a separate computer from the management servers in a distributed installation or on the first management server in the management group. In either case, the instance of Microsoft SQL Server 2008 SP1, SQL Server 2008 R2, or SQL Server 2008 R2 SP1 must already exist and be accessible before you start your first management server installation. The SQL Server Collation setting must be a supported value, and SQL Full Text Search must be enabled.

System Center 2012 Service Pack 1 (SP1), Operations Manager requires access to an instance of a server running Microsoft SQL Server 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1. This instance can be located on a separate computer from the management servers in a distributed installation or on the first management server in the management group. In either case, the instance of Microsoft SQL Server 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1 must already exist and be accessible before you start your first management server installation. The SQL Server Collation setting must be a supported value, and SQL Full Text Search must be enabled.

During setup, you are prompted for the following:

- The SQL Server database server name and instance name. If you have installed SQL Server by using the default instance, you only have to specify the SQL Server name.

You can accept the default values for or set:

- SQL Server Port number. By default, 1433.
- A new operational database (for first management server installation in the management group) or an existing operational database (for installing additional management servers in an existing management group).
- The database name. By default, OperationsManager.
- The starting database size. By default, 1000 MB.
- The Data file and Log folder locations. By default, these are C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Data or C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log as appropriate to the SQL Server defaults.

Important

If TCP/IP is disabled on a remote server that is hosting the SQL Server database, Setup will not be able to connect to the SQL Server database. To resolve this issue, enable TCP/IP on the remote server.

Ensure that SQL Server Reporting Services has been correctly installed and configured. For more information about how to install and configure SQL Server 2012 Reporting Services, see SQL Server Installation (SQL Server 2008 R2).

See Also

Deploying System Center 2012 - Operations Manager

Environmental Prerequisites for Operations Manager

This section covers the infrastructure that you need to have in place and other factors to consider before you run the Setup for System Center 2012 – Operations Manager or System Center 2012 Service Pack 1 (SP1), Operations Manager.

There are two sets of prerequisites that must be satisfied prior to installing any of the Operations Manager features. One set consists of those items that the Prerequisite checker identifies during Setup. The Prerequisite checker is targeted at the server that Setup is running on and determines if the server has the necessary configuration to host whatever role you have chosen.

The other set consists of those items that are outside the scope of the Prerequisite checker, such as the Active Directory domain or forest functional level, or the availability of a certification authority (CA) to issue the certificates that are necessary for deploying agents and gateway servers across trust boundaries. This section addresses this second set of prerequisites, which are much broader in scope, because they apply to the whole environment that Operations Manager will be functioning in, rather than those that are verified by the Prerequisite checker during Setup. To ensure that Operations Manager deploys smoothly and functions as expected, the environment that it will run in must be properly prepared. Because environmental changes affect more than Operations Manager, ensure that you exercise due caution before making sweeping changes. The prerequisites are presented in a unified format with scenario-specific items called out.

For more information about design and environmental decisions, see Planning the System Center 2012 - Operations Manager Deployment. For more information about supported configurations for System Center 2012 – Operations Manager, see System Requirements for System Center 2012 – Operations Manager.

In This Section

Supporting Infrastructure

Describes prerequisites and issues that you need to be aware of before you install System Center 2012 – Operations Manager.

Security Considerations

Describes high-level security factors that need to be addressed.

Agent and Agentless Monitoring

Describes the environmental prerequisites for deploying agents to monitor devices and for deploying agentless monitoring.

Supporting Infrastructure

This section addresses prerequisites and issues involving Active Directory Domain Services (AD DS) and Domain Name System (DNS) that you need to be aware of before initiating your System Center 2012 – Operations Manager installation.

Active Directory Domain Services

System Center 2012 – Operations Manager relies on AD DS for a number of services, including definition of security principles, rights assignment, authentication, and authorization. Operations Manager queries AD DS when performing computer and service discovery and can use AD DS for storing and distributing agent configuration information. For Operations Manager to function properly, AD DS and its supporting service, DNS, need to be healthy and at certain minimum configuration levels. In addition, certain domain naming conventions must be followed.

Domain Space Naming

An Operations Manager management group cannot be installed into a root Active Directory domain that has a flat DNS namespace. However, you can install the management group into child domains of the root domain. For example, you have a root domain that has a DNS name of "Woodgrove". Because this root domain has a flat DNS namespace, you cannot install an Operations Manager management group into the Woodgrove domain. But, if the Woodgrove domain has a child domain with a DNS name of "National", the fully qualified domain name of the child domain would be national.woodgrove. For more information about configuring Windows for domains with single-label DNS names, see Information about configuring Active Directory domains by using single-label DNS names.

Domain Functional Level

Windows Server Active Directory can operate at different functional levels. These levels are distinguished by the version of the Windows Server operating system that is permitted on the domain controllers present in the domain. System Center 2012 – Operations Manager requires that the domain functional level be Windows 2000 native, Windows Server 2003 interim, Windows Server 2003, or Windows Server 2008. The domain functional level of Windows Server 2008 R2 is also supported (for the SP1 version of System Center 2012 – Operations Manager, Windows Server 2008 R2 SP1 and Windows Server 2012 are supported). For System Center 2012 – Operations Manager to function properly, you must check the domain functional level and raise it to the appropriate version. To do this, see Raise the Domain Functional Level.

Note

Ensure that you exercise due caution prior to raising a domain's functional level because it cannot be reversed, and if there are any down-level domain controllers, their function will be impacted.

Forest Functional Level

The forest functional level is similar to the domain functional level in that it sets a minimum domain controller operating system level across the whole forest. After it is set, domain

controllers with down-level operating systems from lower functional levels cannot be introduced into the forest. Operations Manager does not have a forest functional level requirement; however, if the forest functional level is left at the default Windows 2000 level, there may be domains in your forest that won't meet the minimum domain functional level requirement.

DNS

DNS must be installed and in a healthy state to support AD DS. Beyond the reliance of Operations Manager on AD DS, there are no specific DNS requirements.

See Also

Environmental Prerequisites for Operations Manager

Security Considerations

Most of the work in preparing the environment for System Center 2012 – Operations Manager goes into security-related tasks. This section covers those tasks at a cursory level. For more information, see the Index to Security-related Information for Operations Manager.

Preparing the security-related tasks involves the following:

- Understanding, planning, and preparing for monitoring across trust boundaries.
- Understanding, planning, and preparing for monitoring UNIX or Linux computers.
- Planning and preparing the service accounts, user accounts, and security groups that you will need.
- Understanding and preparing the network ports as required by your design.

Trust Boundaries

Active Directory domains form the basic unit of a Kerberos trust boundary as seen by Operations Manager. This boundary is automatically expanded to other domains in the same name space (the same Active Directory tree), and between domains that are in different Active Directory trees but still in the same Active Directory forest via transitive trusts. The trust boundary can be further expanded between domains in different Active Directory forests through the use of across forest trusts.

Kerberos

The Kerberos authentication protocol, which is supported by Windows 2000 domain controllers and above, can only occur within a trust boundary. Kerberos authentication is the mechanism used to perform the Operations Manager agent/server mutual authentication. Agent/server mutual authentication is mandated in Operations Manager Shell for all agent/server communication.

An Operations Manager management group does have the ability to perform discovery and monitoring outside of the Kerberos trust boundary that it is in. However, because the default authentication protocol for Windows-based computers that are not joined to an Active Directory domain is NTLM, another mechanism must be used to support mutual authentication. This is done through the exchange of certificates between agents and servers.

Certificates

When Operations Manager communication needs to occur across trust boundaries, such as when a server that you want to monitor lies in a different, untrusted, Active Directory domain than the management group that is performing the monitoring, certificates can be used to satisfy the mutual authentication requirement. Through manual configuration, certificates can be obtained and associated with the computers and the Operations Manager services running on them. When a service that needs to communicate with a service on a different computer starts and attempts to authenticate, the certificates will be exchanged and mutual authentication completed.

Important
The certificates used for this purpose must ultimately trust the same root certification authority (CA).

For more information about how to obtain and make use of certificates for mutual authentication, see Deploying a Gateway Server.

Certification Authority

To get the necessary certificates, you will need access to a certification authority (CA). This can be either Microsoft Certificate Services or a third-party certification service such as VeriSign.

Microsoft Certificate Services

There are four types of Microsoft CAs:

- Enterprise root
- Enterprise subordinate
- Stand-alone root
- Stand-alone subordinate
- Both enterprise types of CAs require Active Directory Domain Services; stand-alone CAs do not. Either type of CA can issue the necessary certificates for agent/server mutual authentication across trust boundaries.

Customarily, a CA infrastructure consists of a root CA that signs its own certificates and certifies itself and one or more subordinate CAs, which are certified by the root. The subordinate CA servers are the ones that a service certificate requests, while the root is taken offline and held for safekeeping. For more information about designing certificates, see Infrastructure Planning and Design and Authentication and Data Encryption for Windows Computers.

Monitoring UNIX and Linux computers

System Center 2012 – Operations Manager can monitor UNIX and Linux computers. Because the UNIX and Linux computers are not participating in the Active Directory domain that the management group is in a variation of the certificate method of mutual authentication, discussed before, is used.

Establishing Mutual Authentication with UNIX and Linux computers

You will use the Discovery wizard to find UNIX and Linux computers and add them to the management group as managed objects. During the Discovery wizard process, Operations Manager has the discovered UNIX and Linux computer generate a self-signed certificate which is

used for mutual authentication with the management server. The certificate generation, signing and exchange process works like this when SSH discovery is enabled:

1. The Discovery Wizard process on the management server has the discovered UNIX or Linux computer generate a self-signed certificate.
2. The discovering management server issues a get certificate request to the UNIX or Linux computer.
3. The UNIX or Linux computer returns the certificate to the management server
4. The discovering management server creates a key pair and a self-signed certificate of its own. The management server only generates a key pair and a self-signed certificate when it discovers its first UNIX or Linux computer. The management server then imports its own certificate into its trusted certificate store. The discovering management server then signs the UNIX or Linux certificate with its private key. Any subsequent signing of UNIX or Linux computer certificates by the management server will reuse the management server's private key that was generated on the first signing.
5. The discovering management server then issues a put certificate request which puts the now management server-signed certificate back onto the UNIX or Linux computer that initially generated it. The UNIX or Linux computer WSMAN communication layer is then restarted to make the new UNIX\Linux computer generated certificate active.
6. Now when the management server requests that the UNIX or Linux computer authenticate itself, the UNIX or Linux computer will provide the trusted certificate to the management server and the management server will read the signature on the certificate that it is presented with, see that it trusts this signature (because the signature is its own private key that is stored in its own trusted certificate store) and accept this certificate as proof that the UNIX OR LINUX computer is who the management server thinks it is.
7. The discovering management server will use UNIX or Linux credentials as configured in the appropriate Run As Profile to authenticate itself with the UNIX or Linux computer. See the Planning for UNIX or Linux Run As Profiles section for more details.

Important

The preceding order of operations is for the low security version of UNIX or Linux discovery.

Planning for UNIX or Linux Run As Profiles

After the UNIX or Linux computer is being managed by the discovering management server, the management pack discoveries and workflows begin to run. These workflows require the use of credentials to complete successfully. These credentials, what objects, classes or group they will be applied to and the computers that they will be distributed to are contained in Run As Profiles. There are two Run As Profiles that are imported when the UNIX management packs are imported into your management group; they are:

- Unix Action Account profile – This Run As profile and its associated UNIX or Linux credentials are used for low security activities on the designated UNIX or Linux computers.
- Unix Privileged Account profile – This Run As profile and its associated UNIX or Linux credentials are used for activities that are protected by a higher level of security and therefore

require an account that has higher privileges on the UNIX or Linux computer. This can be (but does not have to be) the root account.

You will need to configure these profiles with the appropriate UNIX or Linux computer credentials for the management pack workflows that use them to function correctly.

Accounts and Groups

Over the lifetime of your Operations Manager deployment, you will potentially need many accounts and security groups. During Operations Manager Setup, you are only prompted for four. You need to consider additional accounts when planning out role-based security assignments, notifications, and alternate credentials to run processes. For guidance on planning role-based security assignments, see Planning the System Center 2012 - Operations Manager Deployment.

Role-Based Security Accounts and Groups

Operations Manager controls access to monitored groups, tasks, views, and administrative functions through the assignment of user accounts to roles. A role in Operations Manager is the combination of a profile type (operator, advanced operator, administrator) and a scope (what data the role has access to). Typically, Active Directory security groups are assigned to roles, and then individual accounts are assigned to those groups. Prior to deploying, plan out Active Directory security groups that can be added to these and any custom-created roles so that you can then add individual user accounts to the security groups.

Operations Manager provides the following role definitions out-of-the-box.

Role name	Profile type	Profile description	Role scope
Operations Manager Administrators: Created at setup; cannot be deleted; must contain one or more global groups	Administrator	Has full privileges to Operations Manager; no scoping of the Administrator profile is supported	Full access to all Operations Manager data, services, administrative, and authoring tools
Operations Manager Advanced Operators: Created at setup; globally scoped; cannot be deleted	Advanced Operator	Has limited change access to Operations Manager configuration; ability to create overrides to rules; monitors for targets or groups of targets within the configured scope	Access to all groups, views, and tasks currently present and those imported in the future
Operations Manager Authors: Created at setup; globally scoped; cannot be deleted	Author	Has ability to create, edit, and delete tasks, rules, monitors, and views within	Access to all groups, views, and tasks currently present and those imported in the

Role name	Profile type	Profile description	Role scope
		configured scope	future
Operations Manager Operators: Created at setup; globally scoped; cannot be deleted	Operator	Has ability to interact with alerts, run tasks, and access views according to configured scope	Access to all groups, views, and tasks currently present and those imported in the future
Operations Manager Read-Only Operators: Created at setup; globally scoped; cannot be deleted	Read-Only Operator	Has ability to view alerts and access views according to configured scope	Access to all groups and views currently present and those imported in the future
Operations Manager Report Operators: Created at setup; globally scoped	Report Operator	Has ability to view reports according to configured scope	Globally scoped
Operations Manager Report Security Administrators: Integrates SQL Server Reporting Services security with Operations Manager user roles; gives Operations Manager administrators the ability to control access to reports; cannot be scoped	Report Security Administrator	Enables integration of SQL Server Reporting Services security with Operations Manager roles	No scope

You can add Active Directory security groups or individual accounts to any of these predefined roles. If you do, those individuals will be able to exercise the given role privileges across the scoped objects.

Note
The predefined roles are globally scoped, giving them access to all groups, views, and tasks (except for Report Security Administrator).

Operations Manager also allows you to create custom roles based on the Operator, Read-Only Operator, Author, and Advanced Operator profiles. When you create the role, you can further narrow the scope of groups, tasks, and views that the role can access. For example, you can create a role entitled "Exchange Operator" and narrow the scope to only Exchange-related

groups, views, and tasks. User accounts assigned to this role will only be able to run Operator-level actions on Exchange-related objects.

Notification Accounts and Groups

Individuals in your company that will interact with Operations Manager frequently, such as an Exchange administrator who has been assigned to the Exchange Operator role, need a way to discover new alerts. This can be done by either watching the Operations console for new alerts or by Operations Manager informing them about the alert via supported communications channels. Operations Manager supports notifications through e-mail, instant messaging, Short Message Service, or pager messages. Notifications on what the role needs to know go out to recipients that you specify in Operations Manager. An Operations Manager recipient is merely an object that has a valid address to receive the notification, such as an SMTP address for e-mail notifications.

Therefore, it is logical to combine role assignment with notification group membership via an e-mail-enabled security group. For example, create an Exchange Administrators security group and populate it with individuals that have the knowledge and permissions to fix things in Exchange. Assign this security group to a custom-created Exchange Administrator role so they have access to the data and are e-mail-enabled. Then, create a recipient by using the SMTP address of the e-mail-enabled security group.

Service Accounts

At the time of deployment, you need to have the following service accounts ready. If you use domain accounts and your domain Group Policy object (GPO) has the default password expiration policy set as required, you will either have to change the passwords on the service accounts according to the schedule, or use low maintenance system accounts, or configure the accounts so that the passwords never expire.

Account name	Requested when	Used for	Low maintenance	High security
Management server Action Account	management server setup	Collecting data from providers, running responses	Local system	Low privilege domain account
Data Access Service and Configuration Service Account	management server setup	Writing to operational database, running services	Local system	Low privilege domain account
Local Administrator Account for target devices	Discovery and push agent install	Installing agents	Domain or local administrator account	Domain or local administrator account
Agent Action Account	Discovery and push agent install	Gathering information and running	Local system	Low privilege domain account

Account name	Requested when	Used for	Low maintenance	High security
		responses on managed computers		
Data Warehouse Write Action Account	Reporting Server setup	Writing to the Reporting Data Warehouse database	Low privilege domain account	Low privilege domain account
Data Reader Account	Reporting Server setup	Querying SQL Reporting Services database	Low privilege domain account	Low privilege domain account

Service Principal Names

When you deploy Operations Manager, you may need to register a Service Principal Name (SPN) in some configurations. SPNs are used by Kerberos authentication for the client to mutually authenticate with the server. For more information, see What Are Service Publication and Service Principal Names?.

When you install Operations Manager, you select an account for the **System Center Configuration service and System Center Data Access service**. For more information, see Deploying System Center 2012 - Operations Manager.

Caution

Do not modify the default Active Directory permissions to allow an account to do unrestricted modifications of its own SPN.

If you select the Local System as the System Center Data Access service account, the account can create the appropriate SPN. No additional configuration is necessary.

If you use a domain account, you must register an SPN for each management server. Use the SETSPN command line tool. For more information about running that tool, see Setspn Overview.

Register both the netbios name and fully qualified domain name of the management server, using the following syntax:

```
setspn –a MSOMSdkSvc/<netbios name> <DAS account domain>\<DAS account name>

setspn –a MSOMSdkSvc/<fqdn> <DAS account domain>\<DAS account name>
```

Tip

You can list the SPNs registered to user account or computer with the following syntax:

```
setspn –l <DAS account name>

setspn –l <fqdn>
```

If you are using Network Load Balancing or using a hardware load balancer, the System Center Data Access service must run under a domain account. In addition to the setup already described, you must also register the load balanced name, using the following syntax:

```
setspn –a MSOMSdkSvc/<load balanced name> <DAS account domain>\<DAS account name>
```

Note

All of the System Center Data Access services running behind the load balancer must be running with the same domain account.

Run As Accounts

Agents on monitored computers can run tasks, modules, and monitors on demand as well as in response to predefined conditions. By default, all tasks run by using the Agent Action account credentials. In some cases, the Agent Action account may have insufficient rights and privileges to run a given action on the computer. Operations Manager supports the running of tasks by agents in the context of an alternate set of credentials called a Run As Account. A Run As Account is an object that is created in Operations Manager, just like a recipient is, and maps to an Active Directory user account. A Run As Profile is then used that maps the Run As Account to a specific computer. When a rule, task, or monitor that has been associated with a Run As Profile at the development time of a management pack needs to run on the targeted computer, it does so by using the specified Run As Account.

Out-of-the-box, Operations Manager provides a number of Run As Accounts and Run As Profiles, and you can create additional ones as necessary. You may also choose to modify the Active Directory credentials that a Run As Account is associated with. This will require planning, creating, and maintaining additional Active Directory credentials for this purpose. You should treat these accounts as service accounts with respect to password expiration, Active Directory Domain Services, location, and security.

You will need to work with management pack authors as they develop requests for Run As Accounts. For more information, see the Index to Security-related Information for Operations Manager.

See Also

Environmental Prerequisites for Operations Manager

Agent and Agentless Monitoring

This section covers the environmental prerequisites for devices that will have agents installed and devices that will be monitored in an agentless fashion.

Clients with Agents Installed

The three main activities involved with agent administration are discovery of target devices, deployment or installation of agents to those devices, and ongoing management of the agents. Agents that lie outside a trust boundary require a few more prerequisites than agents that lie inside a trust boundary.

Agents Inside a Trust Boundary

Discovery

Discovery requires that the TCP 135 (RPC), RPC range, and TCP 445 (SMB) ports remain open and that the SMB service is enabled. For UNIX\Linux computers, default discovery and management occurs over TCP 1270, troubleshooting, and diagnostics discovery occur over SSH, TCP 22. Discovery and deployment over SSH, default TCP 22, can also be enabled to allow Operations Manager to install the WSMAN communication layer on the discovered UNIX/Linux computer.

Installation

After a target device has been discovered, an agent can be deployed to it. Agent installation requires the following:

- Opening Remote procedure call (RPC) ports beginning with endpoint mapper TCP 135 and the Server Message Block (SMB) port TCP/UDP 445.
- Enabling the File and Printer Sharing for Microsoft Networks and the Client for Microsoft Networks services (this ensures that the SMB port is active).
- If enabled, Windows Firewall Group Policy settings for **Allow remote administration exception** and **Allow file and printer sharing exception** must be set to **Allow unsolicited incoming messages from:** to the IP address and subnets for the primary and secondary management servers for the agent.
- An account that has local administrator rights on the target computer.
- Windows Installer 3.1. To install, see Windows Installer 3.1 (article 893803) in the Microsoft Knowledge Base.
- Microsoft Core XML services (MSXML) 6 on the Operations Manager product installation media in the \msxml subdirectory.

Note

Push agent installation will install MSXML 6 on the targeted device if it is not there.

Ongoing Management

Ongoing management of an agent requires that the TCP 135 (RPC), RPC range, and TCP 445 (SMB) ports remain open and that the SMB service remains enabled.

Agents Outside a Trust Boundary

For agents that lie outside the trust boundary of the management servers, the environmental prerequisites are the same as for those that lie inside a trust boundary, plus some additions.

Because the device is going to have an installed agent, the software, service, and port requirements remain the same. However, because there is no underlying infrastructure to support Kerberos authentication, certificates must be used on both sides of the connection.

To simplify the cross trust boundary configuration, you can install an Operations Manager gateway server in the same trust boundary as the devices that you will monitor. The gateway server acts as a proxy so that all communication between the management server and agents is routed through the gateway server. This communication is done over a single port, TCP 5723, and requires certificates on the management server and the gateway server. In addition, the gateway server performs discovery and installation, and relays ongoing administration traffic on

behalf of the management server to the agents. The use of gateway servers also reduces the volume of network traffic and is therefore useful in low bandwidth conditions

Gateway servers can also discover and manage UNIX/Linux computers; this is done over TCP ports 1270 and as needed SSH TCP 22, this port is configurable.

For more information about gateway server configuration, see Deploying a Gateway Server.

Manually Installed Agents

Discovery is not performed for manually installed agents, so there are fewer requirements.

Agentless Monitoring

Agentless monitoring of devices is performed by either a management server or by another device that does have an agent, called a proxy agent. An agentless managed device must not be separated from its management server or proxy agent by a firewall because monitoring is performed over RPC. The action account of the agent that is performing the monitoring must have local administrative rights on the device that is being monitored.

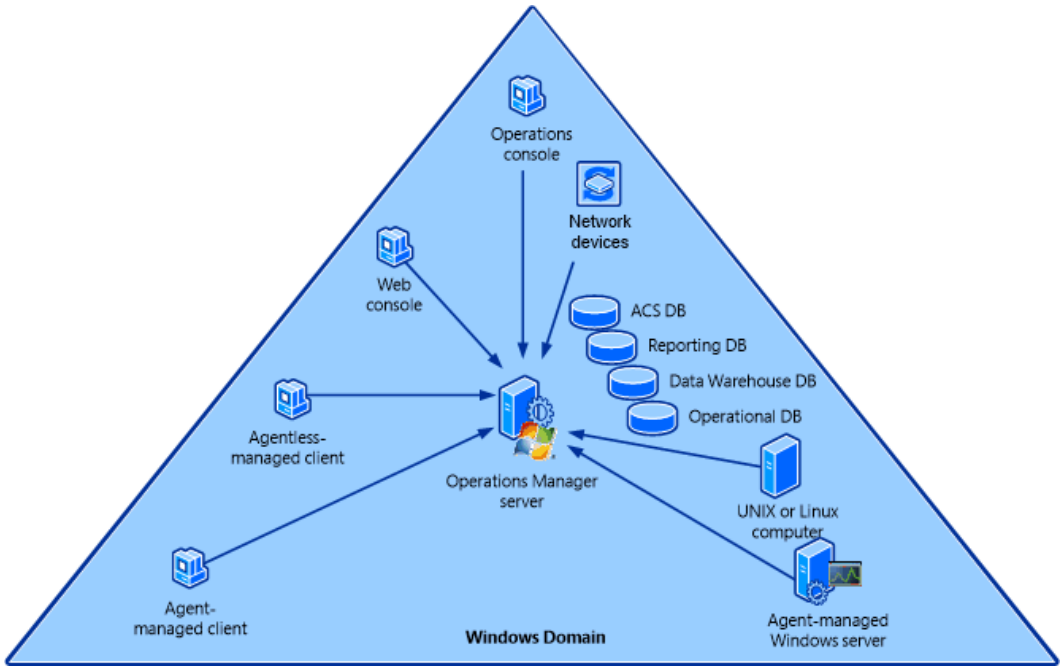
See Also

Environmental Prerequisites for Operations Manager

Single-Server Deployment of Operations Manager

The single-server management group scenario combines all the management group roles that can coexist onto a single instance of the Windows Server 2008 R2 SP1, or Windows Server 2012 operating system running as a member server in an Active Directory domain. This instance can be on dedicated hardware or on a virtual computer. The Operations console can be deployed to computers other than the single server, and the web console is accessed via a browser. Agents are then typically deployed to a limited number of devices depending on the capacity of the server that System Center 2012 – Operations Manager is deployed on.

You deploy Operations Manager in a single-server management group when you want to use it for evaluation, testing, and management pack development, usually in nonproduction or preproduction environments.



Operations Manager Services

The single-server management group configuration supports the following services:

1. Monitoring and alerting
2. Reporting (available in the Operations console but not in the web console)
3. Audit collection
4. Agentless exception management
5. Data (accessed by using the web console and the Operations console)

Operations Manager Features

The single-server management group configuration combines these features:

- Audit Collection Services (ACS) collector
- ACS database
- ACS forwarder
- Operational database
- Operations console
- Reporting data warehouse database
- Reporting database
- Reporting server
- Web console server
- Command Shell

Restrictions

The single-server management group configuration is the easiest to deploy, but there are limitations to its capabilities and therefore limitations to what it is commonly used for.

Gateway Server

This configuration does not include the gateway server role. Because of this, all monitored devices must be in the same Active Directory forest as the management server or you must use certificates on both the managed computer and the management server to provide for mutual authentication.

High Availability and Redundancy

The single server, single management group resides on a single set of hardware. This configuration supports only one instance of each server role and therefore cannot support agent failover between management servers.

Common Uses

This configuration is most commonly used for evaluation, testing, and management pack development purposes, usually in nonproduction or preproduction environments. Single-server management group configurations generally lack the robustness and performance to support anything but the smallest production loads.

Ports Used

In this configuration, you need to make sure that network ports are opened for communication between the agents and the management server, between the Operations console and the management server, and between the web console and the management server. All other inter-service communication occurs on the management server itself. The ports are as follows:

- Operations console to management server: TCP 5724
- Operations console to Reporting server: TCP 80
- Web console to web console server: selected web site port
- Agent to management server: TCP 5723
- ACS forwarder to ACS collector: TCP 51909
- Agentless management: occurs over remote procedure call
- Management server to UNIX\Linux computer: TCP 1270
- Management server to UNIX\Linux computer for special discovery and troubleshooting: TCP 22

For a complete listing of ports used, the direction of the communication, and if the ports can be configured, see Supported Configurations for System Center 2012 – Operations Manager.

To deploy Operations Manager in a single-server management group, see Walkthrough: Installing Operations Manager on a Single Server.

See Also

Deploying System Center 2012 - Operations Manager

Distributed Deployment of Operations Manager

Walkthrough: Installing Operations Manager on a Single Server

This walkthrough guides you through an installation of System Center 2012 – Operations Manager or System Center 2012 Service Pack 1 (SP1), Operations Manager on a single server. The features installed include the following:

- Management server
- Operations console
- Web console
- Reporting server

Prerequisites

You must ensure that your server meets the minimum supported configurations for Operations Manager. For more information, see System Requirements for System Center 2012 – Operations Manager.

Important
Before you follow these procedures, read the Before You Begin section of Deploying System Center 2012 - Operations Manager.

To install the single server management group configuration

1. Log on to the server by using an account that has local administrative credentials.
2. On the Operations Manager installation media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started**, **Select features to install** page select the **Management server**, **Operations console**, **Web console**, and **Reporting server** features. To read more about each feature and its requirements, click **Expand all**, or expand the buttons next to each feature. Then click **Next**.
4. On the **Getting Started**, **Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager** or type in a new location or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and resolve any warnings or errors, and then click **Verify Prerequisites Again** to recheck the system.

   Note
   Installation of the web console requires that ISAPI and CGI Restrictions in IIS be enabled for ASP.NET 4. To enable this, select the web server in IIS Manager, and then double-click **ISAPI and CGI Restrictions**. Select **ASP.NET v4.0.30319**, and then click **Allow**.

   Important

You must install IIS before installing .NET Framework 4. If you installed IIS after installing .NET Framework 4, you must register ASP.NET 4.0 with IIS. Open a Command prompt window by using the **Run As Administrator** option and then run the following command:

%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -r

6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration**, **Specify an installation option** page, select **Create the first Management server in a new management group**, type in a name for your management group and then click **Next**.

   Note
   After the management group name is set, it cannot be changed. The Management Group name cannot contain the following characters:, ( ) ^ ~ : ; . ! ? " , ' ` @ # % \ / * + = $ | & [ ] <>{}, and it cannot have a leading or trailing space. It is recommended that the Management Group name be unique within your organization if you plan to connect several management groups together.
8. On the **Configuration**, **Please read the license terms** page, review the Microsoft Software License Terms, select **I have read, understood, and agree with the license terms**, and then click **Next**.
9. When the **Configuration**, **Configure the operational database** page opens, in the **Server name and instance name** box, type the name of the server and the name of the SQL Server instance for the database server that will host the operational database. If you installed SQL Server by using the default instance, you only have to enter the server name. If you changed the default SQL Server port, you must type in the new port number in the **SQL Server port** box.

   If you type an invalid SQL Server and instance name, you see a red circle with a white **X** in it appear to the left of the **Server name and instance name** and **SQL Server port** boxes.

   The white **X** appears under the following circumstances:

   - You entered an instance of SQL Server or a SQL Server port value that is not valid or that does not exist.
   - The instance of SQL Server that you specified does not have the required configuration or features.
   - You entered a value that is out-of-range (for example, port 999999).
   - You entered an illegal character for that box (for example, server\instance%)

   You can hover the cursor over the **Server name and instance** text box to view additional information about the error.
10. After you type the correct value for the SQL Server database server name, click the **SQL Server port** box so that Setup will attempt to validate the values you typed for the SQL Server name and for the port number.
11. In the **Database name**, **Database size (MB) Data file folder**, and **Log file folder** box,

we recommend that you accept the default values. Click **Next**

Note
These paths do not change if you connect to a different instance of SQL Server.

Important
You might receive a message about having the wrong version of SQL Server, or you might encounter a problem with the SQL Server Windows Management Instrumentation (WMI) provider. To resolve this problem, open a Command Prompt window, select **Run as administrator**, and then run the following command. In the command, replace the *<path>* placeholder with the location of SQL Server:

mofcomp.exe "<path>\Microsoft SQL Server\100\Shared\sqlmgmproviderxpsp2up.mof"

Note
The SQL Server model database size must not be greater than 100 MB. If it is, you might encounter an error in Setup regarding the inability to create a database on SQL due to user permissions. To resolve the issue, you must reduce the size of the model database.

12. When the **Configuration**, **Configure the data warehouse database** page opens, in the **Server name and instance name** box, type the server name and the name of the instance of SQL Server for the database server that will host the data warehouse database.
13. Because this is a single-server installation, accept the default value of **Create a new data warehouse database**.
14. In the **Database name**, **Database size (MB) Data file folder**, and **Log file folder** boxes, we recommend that you accept the default values. Click **Next**.

Important
You might receive a message about having the wrong version of SQL Server, or you might encounter a problem with the SQL Server Windows Management Instrumentation (WMI) provider. To resolve this problem, open a Command Prompt window, select **Run as administrator**, and then run the following command. In the command, replace the *<path>* placeholder with the location of SQL Server:

mofcomp.exe "<path>\Microsoft SQL Server\100\Shared\sqlmgmproviderxpsp2up.mof".

Note
These paths do not change if you connect to a different instance of SQL Server.

15. On the **Configuration**, **SQL Server instance for reporting services** page, select the SQL Server database instance from the drop-down list. This drop-down list contains the SQL Server database instance name that was created when you installed

SQL Server 2008 R2, SQL Server 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1 and should be the name of the server on which you are installing Operations Manager. Click **Next**.

16. On the **Configuration**, **Specify a web site for use with the Web console** page, select **Default Web Site** or the name of an existing website. Select the option **Enable SSL** only if the website has been configured to use SSL, and then click **Next**.
17. On the **Configuration**, **Select an authentication mode for use with the Web console** page, select your option, and then click **Next**.
18. On the **Configuration**, **Configure Operations Manager accounts** page, we recommend that you use **Domain Account** option for the **Management Server Action Account**, **System Center Configuration service and System Center Data Access service**, the **Data Reader account**, and the **Data Writer account**.

    Enter the credentials for a domain account in each field. The error icon will disappear after account validation. Click **Next**.
19. On the **Configuration**, **Help improve System Center 2012 - Operations Manager** page, select your options and click **Next**.
20. If Windows Update is not activated on the computer, the **Configuration**, **Microsoft Update** page appears. Select your options, and then click **Next**.
21. Review the options on the **Configuration**, **Installation Summary** page, and click **Install**. Setup continues.
22. When Setup is finished, the **Setup is complete** page appears. Click **Close** and the Operations console will open.

To install the System Center 2012 - Operations Manager single server management group configuration by using the Command Prompt window

1. Log on to the server by using an account that has local administrative credentials.
2. Open the Command Prompt window by using the **Run as Administrator** option.

   Note
   Setup.exe requires administrator privileges because the Setup process requires access to system processes that can only be used by a local administrator.
3. Change the path to where the Operations Manager setup.exe file is located, and run the following command.

   Important
   Use the `/WebConsoleUseSSL` parameter only if your website has Secure Sockets Layer (SSL) activated.

   For a default web installation, specify **Default Web Site** for the `/WebSiteName` parameter.

   Important
   The following command assumes that you specified the Local System for the Management server action account (`/UseLocalSystemActionAccount`) and Data

Access service (`/UseLocalSystemDASAccount`). To specify a domain\user name for these accounts, you must provide the following parameters instead.

`/ActionAccountUser: <domain\username> /ActionAccountPassword: <password>`

`/DASAccountUser: <domain\username> /DASAccountPassword: <password>`

```
setup.exe /silent /install
/components:OMServer,OMConsole,OMWebConsole,OMReporting
/ManagementGroupName: "<ManagementGroupName>"
/SqlServerInstance: <server\instance>
/DatabaseName: <OperationalDatabaseName>
/DWSqlServerInstance: <server\instance>
/DWDatabaseName: <DWDatabaseName>
/UseLocalSystemActionAccount /UseLocalSystemDASAccount
/DatareaderUser: <domain\username>
/DatareaderPassword: <password>
/DataWriterUser: <domain\username>
/DataWriterPassword: <password>
/AcceptEndUserLicenseAgreement: [0|1]
/WebSiteName: "<WebSiteName>" [/WebConsoleUseSSL]
/WebConsoleAuthorizationMode: [Mixed|Network]
/SRSInstance: <server\instance>
/SendODRReports: [0|1]
/EnableErrorReporting: [Never|Queued|Always]
/SendCEIPReports: [0|1]
/UseMicrosoftUpdate: [0|1]
```

Verifying the Installation

To confirm the health of the management server

1. In the Operations console, select the **Administration** workspace.
2. In **Device Management** select **Management Servers**. In the results pane, you should see the management server that you just installed with a green check mark in the **Health State** column.

To confirm the health of operations manager reports

1. In the Operations console, in the navigation pane, click the **Reporting** button.

   Note

After initial deployment, it can take up to 30 minutes for reports to appear.

2. Click **Microsoft ODR Report Library**, and then double-click any of the reports listed. The selected report is generated and displays in a new window.

   By default, you should see the following reports:

   - **Alerts Per Day**
   - **Instance Space**
   - **Management Group**
   - **Management Packs**
   - **Most Common Alerts**

   Note
   Selecting the management packs report is particularly useful at this point because it provides you with a full inventory of the management packs that have been installed on your server.

3. Close the report window.

Next Steps

Now that you have installed Operations Manager, you can deploy agents and start monitoring your applications, servers, and network devices. For more information, see Managing Discovery and Agents and Operations Manager 2012 Monitoring Scenarios.

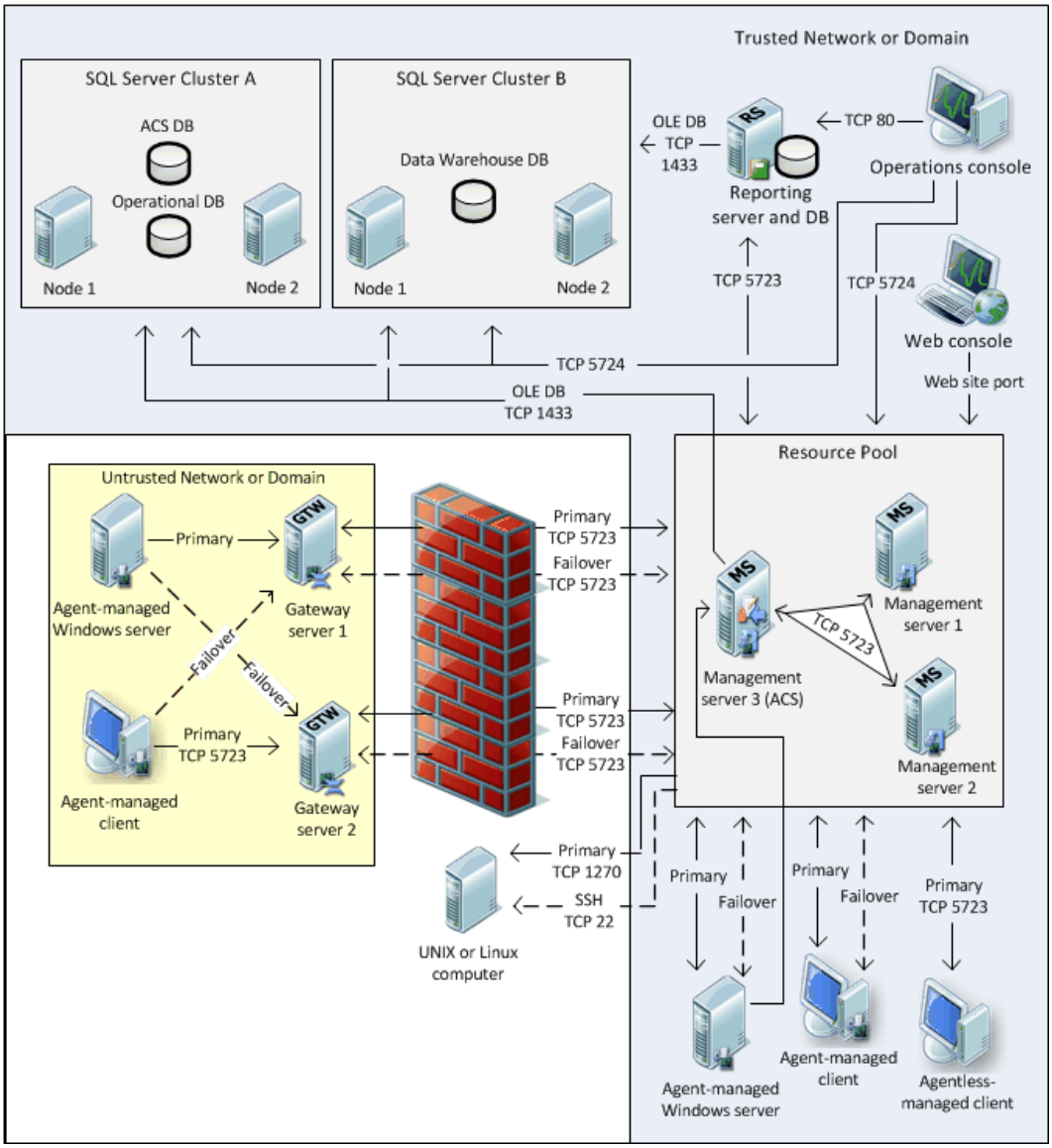
See Also

Distributed Deployment of Operations Manager

Distributed Deployment of Operations Manager

The distributed management group installation will form the foundation of 99 percent of Operations Manager deployments. It allows for the distribution of features and services across multiple servers to allow for scalability. It can include all Operations Manager server roles and supports the monitoring of devices across trust boundaries through the use of the gateway server.

The following diagram presents one possible option for the distributed management group topology.



Note

There is no direct communication between an operations console and the databases. All communication goes to the resource pool through TCP 5724, and then to the database servers using OLE DB on TCP 1433 or another customized port a customer establishes. However, there is direct communication between an Application Diagnostics console (residing with a web console) and databases.

System Center 2012 - Operations Manager Features

This configuration supports all System Center 2012 – Operations Manager and System Center 2012 Service Pack 1 (SP1), Operations Manager features:

- Monitoring and alerting, targeted for up to 15,000 agents
- Monitoring across trust boundaries
- Reporting
- Audit collection
- Agentless exception management
- Agent failover between management servers
- Gateway failover between management servers
- Clustering high availability for database roles

Operations Manager Servers

This configuration supports all Operations Manager server roles:

- Audit Collection Services (ACS) collector
- ACS database
- ACS forwarder (on agent-managed devices)
- Gateway server
- Management server
- Operational database
- Operations console
- For System Center 2012 – Operations Manager: SQL Server 2008 R2, or SQL Server 2008 R2 SP1 Reporting database
- For System Center 2012 Service Pack 1 (SP1), Operations Manager: SQL Server SQL 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, SQL Server 2012 SP1 Reporting database
- Reporting data warehouse database
- Web console server

Restrictions

Single management group configurations do not support partitioning. Partitioning is the separation of management group services across multiple management groups. In Operations Manager, you may want to create multiple management groups for the following reasons.

Installed Languages

Operations Manager management groups support only one installed language. If the overall IT environment that you need to monitor has more than one installed language, a separate management group will be needed per language.

Consolidated Views

Even the largest distributed management group implementation will not be appropriate in every instance. This will lead you to implement multiple management groups, which will split your monitoring and alerting data between management groups. To provide a single, consolidated

view of your environment, data from multiple management groups can be consolidated and viewed in another management group. For more information, see Connecting Management Groups in Operations Manager.

Function

You may need to have separate groups as needed according to function, such as preproduction for testing management packs and new servers, and production for monitoring daily business processes.

Administrative or Other Business Needs

Your company may have other administrative, security, or business needs that require complete separation of monitoring data and administrative teams, which will mandate additional management groups.

Common Uses

Distributed management groups are most commonly used to monitor very large preproduction environments and large production environments that

- Span trust boundaries between domains and workgroups.
- Have multiple network environments segmented by firewalls.
- Have a need for high availability.
- Must have a scalable monitoring solution.

Ports Used

This configuration supports full distribution of features among servers in the management group as well as monitoring of devices across network boundaries, resulting in a longer list of ports that need to be available for communications. For more information, see Connecting Management Groups in Operations Manager.

Distributed Deployment

You deploy either System Center 2012 – Operations Manager or System Center 2012 Service Pack 1 (SP1), Operations Manager in a distributed management group when you want to allow for scalability and high availability of your management servers and gateway servers. By default, all management servers are members of the All Management Servers Resource Pool, which balances the monitoring load of your management group as new management servers are added, and provides automatic failover for monitoring.

A distributed management group distributes the various features of Operations Manager across several servers. For example, you can install the operational database on one server, the web console on a second server, and the Reporting server on a separate server. This differs from the single-server management group installation, where all features are installed on one server. For more information, see Single-Server Deployment of Operations Manager.

You can install a web console on a stand-alone server or on an existing management server, but you cannot install the management server feature on a server that has an existing web console. If you want to install the management server and web console on the same server, you must either install both features simultaneously, or install the management server before you install the web console.

This section of the Deployment Guide contains the following topics:

- How to Install the First Management Server in a Management Group
- How to Install Additional Management Servers
- How to Install the Operations Console
- How to Configure the Operations Console to Use SSL When Connecting to a Reporting Server
- How to Install the Operations Manager Web Console
- Web Console Security in Operations Manager
- How to Install the Operations Manager Reporting Server
- Deploying a Gateway Server
- Deploying ACS and ACS Reporting
- Using SQL Server 2012 Always On Availability Groups with System Center 2012 SP1 - Operations Manager

See Also

Deploying System Center 2012 - Operations Manager

How to Install the First Management Server in a Management Group

In System Center 2012 – Operations Manager, and System Center 2012 Service Pack 1 (SP1), Operations Manager the first feature that is installed is the management server. The operational database and data warehouse database are created during this setup. This procedure assumes that you have already installed a supported version of Microsoft SQL Server locally on the same server that you are going to install the first management server. However, you can specify an instance of SQL Server that is installed on a separate server.

You must ensure that your server meets the minimum system requirements for System Center 2012 – Operations Manager. For more information, see System Requirements for System Center 2012 – Operations Manager.

Important
Before you follow these procedures, read the Before You Begin section of Deploying System Center 2012 - Operations Manager.

To install the first management server in the management group

1. Log on to the server by using an account that has local administrative credentials.
2. On the Operations Manager installation media, run **Setup.exe**, and then click **Install**.

3. On the **Getting Started**, **Select features to install** page, select the **Management server** feature. You can also select any of the additional features listed. For example, to also install the Operations console, select **Operations console**. To read more about each feature and its requirements, click **Expand all**, or expand the buttons next to each feature, and then click **Next**.
4. On the **Getting Started**, **Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager**. Or, type a new location or browse to one, and then click **Next**.
5. On the **Prerequisites** page, review and resolve any warnings or errors, and then click **Verify Prerequisites Again** to recheck the system.

   Important
   You might receive a message that indicates that ASP.NET 4 is not registered with Internet Information Services (IIS). To resolve this problem, open a Command Prompt window, select **Run as administrator**, and then run the following command:

   %WINDIR%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -r
6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration**, **Specify an installation option** page, select **Create the first Management server in a new management group**, type a name for your management group, and then click **Next**.

   Note
   After the management group name is set, it cannot be changed. The Management Group name cannot contain the following characters:, ( ) ^ ~ : ; . ! ? " , ' ` @ # % \ / * + = $ | & [ ] <>{}, and it cannot have a leading or trailing space. It is recommended that the Management Group name be unique within your organization if you plan to connect several management groups together.
8. On the **Configuration**, **Please read the license terms** page, review the Microsoft Software License Terms, select **I have read, understood and agree with the license terms**, and then click **Next**.
9. When the **Configuration**, **Configure the operational database** page opens, in the **Server name and instance name** box, type the name of the server and the name of the SQL Server instance for the database server that will host the operational database. If you installed SQL Server by using the default instance, you only have to type the server name. If you changed the default SQL Server port, you must type the new port number in the **SQL Server port** box.

   As you type the values for the SQL Server and instance names, you see a red circle with a white **X** in it appear to the left of the **Server name and instance name** and **SQL Server port** boxes. The white **X** indicates that the values have not yet been validated, and the black text indicates that you have not entered any illegal characters. If you enter illegal characters, the text itself turns red.

The white **X** appears under the following circumstances:

- You entered an instance of SQL Server or a SQL Server port value that is not valid or that does not exist.
- The instance of SQL Server that you specified does not have the required configuration or features.
- You entered a value that is out-of-range (for example, port 999999).
- You entered an illegal character for that box (for example, server\instance%)

You can hover the cursor over the **Server name and instance name** text box to view additional information about the error.

10. After you type the correct value for the SQL Server database server name, click the **SQL Server port** box so that Setup will attempt to validate the values you typed for the SQL Server name and for the port number.
11. In the **Database name**, **Database size (MB)**, **Data file folder**, and **Log file folder** boxes, we recommend that you accept the default values. Click **Next**.

    Note
    These paths do not change if you connect to a different instance of SQL Server.

    Important
    You might receive a message about having the wrong version of SQL Server, or you might encounter a problem with the SQL Server Windows Management Instrumentation (WMI) provider. To resolve this problem, open a Command Prompt window, select **Run as administrator**, and then run the following command. In the command, replace the *<path>* placeholder with the location of SQL Server.

    mofcomp.exe "<path>\Microsoft SQL Server\100\Shared\sqlmgmproviderxpsp2up.mof".

    Note
    The SQL Server model database size must not be greater than 100 MB. If it is, you might encounter an error in Setup regarding the inability to create a database on SQL due to user permissions. To resolve the issue, you must reduce the size of the model database.
12. When the **Configuration**, **Configure the data warehouse database** page opens, in the **Server name and instance name** box, type the server name and the name of the instance of SQL Server for the database server that will host the data warehouse database.
13. Because this is the first management server installation, accept the default value of **Create a new data warehouse database**.
14. In the **Database name**, **Database size (MB)**, **Data file folder**, and **Log file folder** boxes, we recommend that you accept the default values. Click **Next**.

    Important

You might receive a message about having the wrong version of SQL Server, or you might encounter a problem with the SQL Server Windows Management Instrumentation (WMI) provider. To resolve this problem, open a Command Prompt window, select **Run as administrator**, and then run the following command. In the command, replace the <*path*> placeholder with the location of SQL Server.

mofcomp.exe "<path>\Microsoft SQL Server\100\Shared\sqlmgmproviderxpsp2up.mof".

Note
These paths do not change if you connect to a different instance of SQL Server.

15. On the **Configuration**, **Configure Operations Manager accounts** page, we recommend that you use the **Domain Account** option for the **Management server action account**, the **System Center Configuration service and System Center Data Access service** account, the **Data Reader account**, and the **Data Writer account**. None of them should have domain administrator credentials. Click **Next**.
16. On the **Configuration**, **Help improve System Center 2012 - Operations Manager** page, select your options, and then click **Next**.
17. If Windows Update is not enabled on the computer, the **Configuration**, **Microsoft Update** page appears. Select your options, and then click **Next**.
18. Review the options on the **Configuration**, **Installation Summary** page, and then click **Install**. Setup continues.
19. When Setup is finished, the **Setup is complete** page appears. Click **Close**.
20. Open the Operations console.
21. In the Operations console, in the navigation pane, click the **Administration** button, and then expand **Device Management**.
22. In **Device Management**, select **Management Servers**. In the results pane, you should see the management server that you just installed with a green check mark in the **Health State** column.

To install the first management server in the management group by using the Command Prompt window

1. Log on to the server by using an account that has local administrative credentials.
2. Open the Command Prompt window by using the **Run as Administrator** option.

   Note
   Setup.exe requires administrator privileges because the Setup process requires access to system processes that can only be used by a local administrator.
3. Change the path to where the Operations Manager setup.exe file is located, and run the following command.

   Important
   The following command assumes that you specified the Local System for the

Management server action account (`/UseLocalSystemActionAccount`) and Data Access service (`/UseLocalSystemDASAccount`). To specify a domain\user name for these accounts, you must provide the following parameters instead.

`/ActionAccountUser: <domain\username> /ActionAccountPassword: <password>`

`/DASAccountUser: <domain\username> /DASAccountPassword: <password>`

```
setup.exe /silent /install /components:OMServer
/ManagementGroupName: "<ManagementGroupName>"
/SqlServerInstance: <server\instance>
/DatabaseName: <OperationalDatabaseName>
/DWSqlServerInstance: <server\instance>
/DWDatabaseName: <DWDatabaseName>
/UseLocalSystemActionAccount /UseLocalSystemDASAccount
/DatareaderUser: <domain\username>
/DatareaderPassword: <password>
/DataWriterUser: <domain\username>
/DataWriterPassword: <password>
/EnableErrorReporting: [Never|Queued|Always]
/SendCEIPReports: [0|1]
/UseMicrosoftUpdate: [0|1]
/AcceptEndUserLicenseAgreement: [0|1]
```

See Also

Distributed Deployment of Operations Manager

How to Install Additional Management Servers

After you have installed System Center 2012 – Operations Manager, you can add additional management servers and join them to your existing management group.

Important

If you install a stand-alone web console on a server, you will not be able to add the management server feature to this server. If you want to install the management server and web console on the same server, you must either install both features simultaneously, or install the management server before you install the web console.

You must ensure that your server meets the minimum system requirements for System Center 2012 – Operations Manager. For more information, see System Requirements for System Center 2012 – Operations Manager.

Important

Before you follow these procedures, read the Before You Begin section of Deploying System Center 2012 - Operations Manager.

To install additional management servers

1. Log on to the server with an account that has local administrative credentials.
2. On the Operations Manager installation media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started**, **Select features to install** page, select **Management server**.

   You can also additional features, such as the Operations console. Select **Operations console**. To read more about each feature and its requirements, click **Expand all**, or expand the buttons next to each feature, and then click **Next**.
4. On the **Getting Started**, **Select installation location** page, accept the default location of **C:\Program Files\System Center 2012\Operations Manager**, or type in a new location or browse to one, and then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration**, **Specify an installation option** page, select **Add a Management server to an existing management group**, and then click **Next**.
8. When the **Configuration**, **Configure the operational database** page opens, type the name of the SQL Server database server and instance for the database server that hosts the operational database in the **Server name and instance name** box. If you installed SQL Server by using the default instance, you only have to enter the server name. If you changed the default SQL Server port, you must type in the new port number in the **SQL Server port** box.

   As you type the values for SQL Server and instance name, you see a red circle with a white **X** in it appear to the left of the **Server name and instance name** and **SQL Server port** boxes. The white **X** indicates that the values have not yet been validated. The black text indicates that you have not entered any illegal characters. If you enter illegal characters, the text itself turns red.
9. After you have typed the correct values for the name of the SQL Server database server, click the **SQL Server port** box. Setup attempts to validate the values that you have typed for the SQL Server name and the port number.
10. Select the database name from the **Database name** drop-down list, and then click **Next**.
11. On the **Configuration**, **Configure Operations Manager accounts** page, we recommend that you use the **Domain Account** option for the **Management server action account** and the **System Center Configuration service and System Center Data Access service** account. Neither of them should have domain administrator credentials. Click **Next**.

    Important

You must provide the same credentials for the Management server action account and the System Center Configuration Service and System Center Data Access service that you provided when you created the first management server in your management group.

12. If Windows Update is not enabled on the computer, the **Configuration**, **Microsoft Update** page appears. Select your options, and then click **Next**.
13. Review the options on the **Configuration**, **Installation Summary** page, and then click **Install**. Setup continues.
14. When setup is finished, the **Setup is complete** page appears. Click **Close**.
15. Open the Operations console.
16. In the Operations console, select the **Administration** workspace, and then expand **Device Management**.
17. In **Device Management**, select **Management Servers**. In the results pane, you should see the management server that you just installed with a green check mark in the **Health State** column.

To install additional management servers by using the Command Prompt window

1. Log on to the server by using an account that has local administrative credentials.
2. Open the Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the Operations Manager setup.exe file is located, and run the following command.

Important

The following command assumes that you specified the Local System for the Management server action account (`/UseLocalSystemActionAccount`) and Data Access service (`/UseLocalSystemDASAccount`). To specify a domain\user name for these accounts, you must provide the following parameters instead.

`/ActionAccountUser: <domain\username> /ActionAccountPassword: <password>`

`/DASAccountUser: <domain\username> /DASAccountPassword: <password>`

```
setup.exe /silent /install /components:OMServer
/SqlServerInstance: <server\instance>
/DatabaseName: <OperationalDatabaseName>
/UseLocalSystemActionAccount /UseLocalSystemDASAccount
/DataReaderUser: <domain\username>
/DataReaderPassword: <password>
/DataWriterUser: <domain\username>
/DataWriterPassword: <password>
/EnableErrorReporting: [Never|Queued|Always]
/SendCEIPReports: [0|1]
```

```
/UseMicrosoftUpdate: [0|1]
```

See Also

Distributed Deployment of Operations Manager

How to Install the Operations Console

After you install System Center 2012 – Operations Manager or System Center 2012 Service Pack 1 (SP1), Operations Manager, you can install the Operations console on other servers and computers. For example, you might want to view monitoring data from your desktop computer. Before you install an System Center 2012 – Operations Manager Operations console, you must install Microsoft .NET Framework 3.5 SP1 hotfix.

You must ensure that the computer that will host the Operations console meets the minimum system requirements. For more information, see System Requirements for System Center 2012 – Operations Manager.

Important

Before you follow these procedures, read the Before You Begin section of Deploying System Center 2012 - Operations Manager.

To install the Operations console

1. Log on to the computer that will host the Operations console with an account that has local administrative credentials.
2. On the Operations Manager installation media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started**, **Select features to install** page, select **Operations console**. To read more about what each feature provides and its requirements, click **Expand all**, or expand the buttons next to each feature, and then click **Next**.
4. On the **Getting Started**, **Select installation location** page, accept the default location of **C:\Program Files\System Center 2012\Operations Manager**, or type a new location or browse to one, and then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again**.
6. If the Prerequisite checker returns no warnings or errors, the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration**, **Help improve System Center - Operations Manager** page, select your options, and then click **Next**.
8. If Windows Update is not enabled on the computer, the **Configuration**, **Microsoft Update** page appears. Select your options, and then click **Next**.
9. Review the options on the **Configuration**, **Installation Summary** page, and then click **Install**. Setup continues.
10. When Setup is finished, the **Setup is complete** page appears. Click **Close**, and the Operations console opens.
11. In the Operations console, on the **Connect to Server** page, type the name of the first

management server that you installed in the management group in the **Server name** box, and then click **Connect**.

Important

If you are going to edit company knowledge on this computer, you also have to install the Microsoft Visual Studio 2005 Tools for Office Second Edition Runtime.

Important

Company knowledge cannot be edited with the x64 version of Microsoft Word 2010. You must install the x86 version of Microsoft Office 2010 or an earlier version to edit knowledge.

To install the Operations console by using the Command Prompt window

1. Log on to the server by using an account that has local administrative credentials.
2. Open the Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the Operations Manager setup.exe file is located, and run the following command.

```
setup.exe /silent /install /components:OMConsole
/EnableErrorReporting:[Never|Queued|Always]
/SendCEIPReports:[0|1] /UseMicrosoftUpdate: [0|1]
```

See Also

Distributed Deployment of Operations Manager

How to Configure the Operations Console to Use SSL When Connecting to a Reporting Server

Before you can configure the Operations Manager Operations console to use SSL when connecting to a Reporting Server, you must first install an SSL certificate on IIS. You then configure the Operations console to use SSL.

On the Reporting Server, start Internet Information Services (IIS) Manager to request and install an SSL certificate. For more information about how to implement SSL in IIS, see the Knowledge Base article How to implement SSL in IIS.

Use the following procedure to configure the Operations console to use SSL.

To configure the Operations Console to use SSL

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click the **Administration** button.

Note

When you run the Operations console on a computer that is not a management

server, the **Connect To Server** dialog box displays. In the **Server name** text box, type the name of the Operations Manager management server that you want the Operations console to connect to.

3. In the Administration pane, expand **Administration**, expand **Device Management**, and then click **Settings**.
4. In the Settings pane, right-click **Reporting**, and then click **Properties**.
5. In the **General** tab, under **Reporting Server Settings**, click the **Reporting server URL** drop-down list and select **https://**.
6. Edit the URL by replacing **:80** with **:443**, and then click **OK**.

See Also

Distributed Deployment of Operations Manager

How to Install the Operations Manager Web Console

You can install the web console when you install Operations Manager, or you can install it separately. You can install a stand-alone web console or install it on an existing management server that meets the prerequisites. For information about the prerequisites, see System Requirements for System Center 2012 – Operations Manager. After you install the web console, you must configure permissions inheritance to allow users to view performance and diagram views. For instructions, see To configure permissions inheritance for the web console.

Important

If you install a stand-alone web console on a server, you will not be able to add the management server feature to this server. If you want to install the management server and web console on the same server, you must either install both features simultaneously, or install the management server before you install the web console.

When you install the web console, three components are installed: the Operations Manager web console itself, Application Diagnostics console, and Application Advisor console.

Note

If Application Diagnostics console is not installed, when viewing APM alerts, you will not be able to use the link embedded in the alert description to launch the APM event details. To use this feature, install the web console within the management group.

If you plan to use network load balancing with Application Diagnostics console and Application Advisor console, be sure to use sticky sessions. This ensures that the same instance of the console is used for the entire session. For more information about network load balancing, see Network Load Balancing. For more information about sessions, see Support for Sessions.

Security

The web console operates with sensitive data, such as clear text user credentials, server names, IP addresses, and so on. If these are exposed on the network, they can represent a significant security risk. If Internet Information Services (IIS) does not have Secure Sockets Layer (SSL) configured, you are advised to configure it manually.

Important

Before you follow these procedures, read the Before You Begin section of Deploying System Center 2012 - Operations Manager.

If the web console does not have sufficient access to the operational database or the data warehouse database, you will receive a warning during the web console configuration step. You can proceed with Setup, but the web console will not be configured correctly for .NET Application monitoring. To resolve this issue, you can have your database administrator run the following SQL Server statement on both the operational database and data warehouse database:

```
EXEC [apm].GrantRWPermissionsToComputer N'[LOGIN]'
```

The local and remote parameters are as follows:

- For local installation, the LOGIN is: IIS APPPOOL\OperationsManagerAppMonitoring
- For remote installation, the LOGIN is: Domain\MachineName$

Note

If you run **Repair** on the web console after installation, the settings that were selected during installation will be restored. Any changes that you manually make to the web console configuration after the installation will be reset.

To install a stand-alone web console

1. Log on to the computer that will host the web console with an account that has local administrative credentials.
2. On the Operations Manager installation media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started**, **Select features to install** page, select **Web console**. To read more about what each feature provides and its requirements, click **Expand all**, or expand the buttons next to each feature, and then click **Next**.
4. On the **Getting Started**, **Select installation location** page, accept the default location of **C:\Program Files\System Center 2012\Operations Manager**, or type in a new location or browse to one, and then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.

   Note

   Installation of the web console requires that ISAPI and CGI Restrictions in IIS be enabled for ASP.NET 4. To enable this, select the web server in IIS Manager, and then double-click **ISAPI and CGI Restrictions**. Select **ASP.NET v4.0.30319**, and then click **Allow**.

   Important

   You must install IIS before installing .NET Framework 4. If you installed IIS after installing .NET Framework 4, you must register ASP.NET 4.0 with IIS. Open a Command prompt window by using the **Run As Administrator** option and then

run the following command:

%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -r

6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration**, **Specify a management server** page, enter the name of a management server that only the web console uses, and then click **Next**.
8. On the **Configuration**, **Specify a web site for use with the Web console** page, select the **Default Web Site**, or the name of an existing website. Select **Enable SSL** only if the website has been configured to use Secure Sockets Layer (SSL), and then click **Next**.

   Warning
   Installing the web console on a computer that has SharePoint installed is not supported.
9. On the **Configuration**, **Select an authentication mode for use with the Web console** page, select your options, and then click **Next**.

   Note
   If you install the management server on a server using a domain account for System Center Configuration service and System Center Data Access service, and then install the web console on a different server and select Mixed Authentication, you may need to register Service Principal Names and configure constraint delegations, as described in Running the Web Console Server on a standalone server using Windows Authentication.
10. If Microsoft Update is not enabled on the computer, the **Configuration**, **Microsoft Update** page appears. Select your options, and then click **Next**.
11. Review your selections on the **Configuration**, **Installation Summary** page, and then click **Install**. Setup continues.
12. When Setup is finished, the **Setup is complete** page appears. Click **Close**.

To install the web console on an existing management server

1. Log on to the computer that is hosting a management server with an account that has local administrative credentials.
2. On the Operations Manager installation media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started**, **What do you want to do?** page, click **Add a feature**.
4. On the **Getting Started, Select features to install** page, select **Web console**, and then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors, and then click **Verify Prerequisites Again** to recheck the system.

   Note
   Installation of the web console requires that ISAPI and CGI Restrictions in IIS be enabled for ASP.NET 4. To enable this, select the web server in IIS Manager, and then double-click **ISAPI and CGI Restrictions**. Select **ASP.NET**

v4.0.30319, and then click **Allow**.

Important
You must install IIS before installing .NET Framework 4. If you installed IIS after installing .NET Framework 4, you must register ASP.NET 4.0 with IIS. Open a Command prompt window by using the **Run As Administrator** option and then run the following command:

%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -r

6. If the Prerequisite checker returns no warnings or errors, the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration**, **Specify a web site for use with the Web console** page, select the **Default Web Site**, or the name of an existing website. Select **Enable SSL** only if the website has been configured to use Secure Sockets Layer (SSL), and then click **Next**.
8. On the **Configuration**, **Select an authentication mode for use with the Web console** page, select your options, and then click **Next**.
9. If Windows Update is not activated on the computer, the **Configuration**, **Microsoft Update** page appears. Select your options, and then click **Next**.
10. Review your selections on the **Configuration**, **Installation Summary** page, and click **Install**. Setup continues.
11. On the **Setup is complete** page, click **Close**.

Important
The Default website must have an http or https binding configured.

To install a web console by using the Command Prompt window

1. Log on to the computer with an account that has local administrative credentials.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the Operations Manager setup.exe file is located, and run the following command.

Important
Use the `/WebConsoleSSL` parameter only if your website has Secure Sockets Layer (SSL) activated.

For a default web installation, specify **Default Web Site** for the `/WebSiteName` parameter.

Note
The /ManagementServer parameter is only required when you are installing the web console on a server that is not a management server.

```
setup.exe /silent /install /components:OMWebConsole
/ManagementServer: <ManagementServerName>
/WebSiteName: "<WebSiteName>" [/WebConsoleUseSSL]
```

```
/WebConsoleAuthorizationMode: [Mixed|Network]
/UseMicrosoftUpdate: [0|1]
```

To configure permissions inheritance for the web console

1. In Windows Explorer, navigate to the MonitoringView folder in the installation directory for the web console (by default, C:\Program Files\System Center 2012\Operations Manager\WebConsole\MonitoringView), right-click the TempImages folder, and click **Properties**.
2. On the **Security** tab, click **Advanced**.
3. On the **Permissions** tab, click **Change Permissions**.
4. Select the **Include inheritable permissions from this object's parent** checkbox.
5. In **Permission entries**, click **Administrators**, and then click **Remove**. Repeat for the **SYSTEM** entry, and then click **OK**.
6. Click **OK** to close **Advanced Security Settings for TempImages**, and then click **OK** to close **TempImages Properties**.

All information and content at http://blogs.technet.com/b/momteam/archive/2008/01/31/running-the-web-console-server-on-a-standalone-server-using-windows-authentication.aspx is provided by the owner or the users of the website. Microsoft makes no warranties, express, implied or statutory, as to the information at this website.

See Also

Distributed Deployment of Operations Manager

Web Console Security in Operations Manager

The web console server provides a browser-based alternative to the Monitoring pane of the Operations Manager Operations console. The web console server is commonly used when you want to access Operations Manager management group monitoring data in the following ways:

- From the Internet
- Without installing the Operations console
- From a location with low-bandwidth connectivity
- When notifications are configured to contain hyperlinks to the relevant alerts in the web console

When you install the web console, you must specify a web site for use with the web console. The default port for accessing the web console from a browser using Windows-based authentication is the same port as the web site that is selected when the web console was installed. If the web site chosen has been configured to use Secure Sockets Layer (SSL), then you must also select **Enable SSL**.

You must also select an authentication mode for use with the web console. Use mixed authentication for intranet scenarios and network authentication for extranet scenarios.

Note

The best practice for accessing the web console from the Internet is to use network authentication with SSL with the web console.

The web console uses two encryption algorithms:

1. SHA256
2. HMACSHA256

These algorithms may not be sufficient to meet compliance standards. For instance, they do not meet the Federal Information Processing Standard (FIPS). In order to meet a compliance standard, you need to map these names, in the appropriate configuration files, to appropriate encryption algorithms.

The next section uses FIPS compliant algorithms as an example.

How to Use FIPS Compliant Algorithms

System Center 2012 – Operations Manager can use Federal Information Processing Standard (FIPS) compliant algorithms. A FIPS compliant algorithm is included on your installation media. After you install it, you need to manually edit several configuration files.

In order to use algorithms that are FIPS compliant, follow these steps for all Operations Manager server components.

- Install Microsoft.EnterpriseManagement.Cryptography.dll.
- Edit several instances of the machine.config file.

For systems that host a web console, also do the following steps.

- Edit the WebHost\web.config file.
- Edit the MonitoringView\web.config file.

You need the Global Assembly Cache Tool, gacutil.exe. This utility is part of the Windows SDK. For more information, see Gacutil.exe (Global Assembly Cache Tool).

To install the cryptography DLL

1. On the system hosting the web console, use the **Run as Administrator** option to open a Command Prompt window.
2. Change directories to the SupportTools directory of your installation media, and then change directory as appropriate to your platform: AMD64 or i386.
3. Run the following gacutil command:

```
gacutil.exe –i
Microsoft.EnterpriseManagement.Cryptography.dll
```

To edit the machine.config files

1. Use a plain text editor to open the following machine.config file:

   %WinDir%\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config

2. Add the following content:

```
<mscorlib>
    <cryptographySettings>
        <cryptoNameMapping>
            <cryptoClasses>
                <cryptoClass
SHA256CSP="System.Security.Cryptography.SHA256CryptoServicePr
ovider, System.Core, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089"/>
                <cryptoClass HMACSHA256CSP
="Microsoft.EnterpriseManagement.Cryptography.HMACSHA256,
Microsoft.EnterpriseManagement.Cryptography,
Version=7.0.5000.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35"/>
            </cryptoClasses>
            <nameEntry name="SHA256" class="SHA256CSP"/>
            <nameEntry name="HMACSHA256"
class="HMACSHA256CSP"/>
        </cryptoNameMapping>
    </cryptographySettings>
</mscorlib>
```

   Save and close the file when finished.
3. Repeat the preceding step on the following files:

   %WinDir%\Microsoft.NET\Framework\v4.0.30319\Config\machine.config

   %WinDir%\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config

To edit the web.config file in WebHost

1. Use a plain text editor to open the following web.config file:

   C:\Program Files\System Center 2012\Operations Manager\WebConsole\WebHost\web.config
2. In the `<encryption>` element, add the following element:

```
<symmetricAlgorithm  iv="SHA256"/>
```

3. In the `<connection autoSignIn="true" autoSignOutInterval="30">` element, in the `<session>` tag, add the following attribute: `tokenAlgorithm="SHA256"`.

```
<connection autoSignIn="True" autoSignOutInterval="30">
<session encryptionKey="SessionEncryptionKey"
tokenAlgorithm="SHA256">
```

4. Save and close the file.

To edit the web.config file in MonitoringView

1. Use a plain text editor to open the following web.config file:

   C:\Program Files\System Center 2012\Operations Manager\WebConsole\MonitoringView\web.config
2. In the `<encryption>` element, add the following element:

   ```
   <symmetricAlgorithm  iv="SHA256"/>
   ```

3. In the `<connection autoSignIn="true" autoSignOutInterval="30">` element, in the `<session>` tag, add the following attribute: `tokenAlgorithm="SHA256"`.

   ```
   <connection autoSignIn="True" autoSignOutInterval="30">
   <session encryptionKey="SessionEncryptionKey"
   tokenAlgorithm="SHA256">
   ```
4. In the `<system.web>` element, add the following element:

   ```
   <machineKey validationKey="AutoGenerate,IsolateApps"
   decryptionKey="AutoGenerate,IsolateApps" validation="3DES"
   decryption="3DES"/>
   ```

5. Save and close the file.

How to Install the Operations Manager Reporting Server

In this procedure, the Reporting server is installed on a stand-alone server that is hosting the SQL Server database and SQL Server Reporting Services.

Warning

Although SQL Server Reporting Services is installed on the stand-alone server, Operations Manager reports are not accessed on this server; instead, they are accessed in the **Reporting** workspace in the Operations console. If you want to access published reports via the web console, you must install the Operations Manager web console on the same computer as Operations Manager Reporting server.

You must ensure that your server meets the minimum system requirement for Operations Manager. For more information, see System Requirements for System Center 2012 – Operations Manager.

Important

Before you follow these procedures, read the Before You Begin section of Deploying System Center 2012 - Operations Manager.

Installing Operations Manager Reporting

No other applications that are using SQL Server Reporting Services can be installed on this instance of SQL Server.

Ensure that SQL Server Reporting Services has been correctly installed and configured. For more information about how to install and configure SQL Server Reporting Services, see SQL Server Installation (SQL Server 2012 R2).

Note

Before you continue with this procedure, ensure that the account you plan to use for the Data Warehouse Write account has SQL Server logon rights and is an Administrator on the computers hosting both the operational database and the Reporting data warehouse database. Otherwise, Setup fails, and all changes are rolled back, which might leave SQL Server Reporting Services in an inoperable state.

To verify that Reporting Services is configured correctly

1. Verify that the **ReportServer** and **ReportServerTempDB** databases in SQL Server Management Studio are located on the stand-alone server. Click **Start**, point to **All Programs**, point to **Microsoft SQL Server 2008 R2**, point to **SQL Server Management Studio**, and then connect to the default database instance. Open the **Databases** node and verify that the two Reporting Services databases exist under this node.
2. Verify the correct configuration of SQL Server Reporting Services. Click **Start**, point to **Programs**, point to the appropriate offering of Microsoft SQL Server, point to **Configuration Tools**, and then click **Reporting Services Configuration Manager**. Connect to the instance on which you installed Reporting Services.
3. In the navigation pane, select the <servername>\SQLinstance. This displays the Report Server status in the results pane. Ensure that the **Report Server Status** is **Started**.
4. In the navigation pane, select **Scale-out Deployment**, and then ensure that the **Status** column has the value of **Joined**.
5. If **Report Server** is not started and the **Scale out Deployment** is not joined, check the configuration of **Service Account**, **Web Service URL**, and **Database**.
6. Confirm that the SQL Server Reporting Services service is running. On the taskbar, click **Start**, point to **Administrative Tools**, and then click **Services**.
7. In the **Name** column, find the **SQL Server Reporting Services** instance service and verify that its status reads **Started** and that the **Startup Type** is **Automatic**.
8. In the **Name** column, find the **SQL Server Agent** service and verify that its status reads **Started** and that its **Startup Type** is **Automatic**.
9. Verify that the Report Server website is functioning and available by browsing to **http://servername/reportserver<$instance>**. You should see a page with the

<servername>/ReportServer<$INSTANCE> and the text, **Microsoft SQL Server Reporting Services Version** ##.#.####.## where the # is the version number of your SQL Server installation.

10. Verify that the Report Manager website is configured correctly by opening **Internet Explorer** and browsing to **http://<servername>/reports<instance>**.
11. In the Report Manager website, click **New Folder** to create a new folder. Enter a name and description, and then click **OK**. Ensure that the new, created folder is visible on the Report Manager website.

To install Operations Manager Reporting

1. Log on to the computer with an account that has local administrative credentials.
2. On the Operations Manager installation media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started**, **Select features to install** page, select the **Reporting server** feature. To read more about each feature and its requirements, click **Expand all**, or expand the buttons next to each feature, and then click **Next**.
4. On the **Getting Started**, **Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager** or type a new location or browse to one, and then click **Next**.
5. On the **Prerequisites** page, review and resolve any warnings or errors, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, continue to the **Prerequisites**, **Proceed with Setup** page. Click **Next**.
7. On the **Configuration**, **Specify a Management server** page, enter the name of a management server that is used by the Reporting features only. Then click **Next**.
8. On the **Configuration**, **SQL Server instance for reporting services** page, select the instance of SQL Server that hosts SQL Server Reporting Services, and then click **Next**.
9. On the **Configuration**, **Configure Operations Manager accounts** page, enter the credentials for the **Data Reader account**, and then click **Next**.
10. On the **Configuration**, **Help improve System Center - Operations Manager** page, select your options, and then click **Next**.
11. If Windows Update is not activated on the computer, the **Configuration**, **Microsoft Update** page appears. Select your options, and then click **Next**.
12. Review the options on the **Configuration**, **Installation Summary** page, and then click **Install**. Setup continues.
13. When Setup is finished, the **Setup is complete** page appears. Click **Close**.

To install Operations Manager Reporting by using the Command Prompt window

1. Log on to the server by using an account that has local administrative credentials.
2. Open the Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the Operations Manager setup.exe file is located, and run the following command.

Note

The /ManagementServer parameter is only required when you are installing reporting on a server that is not a management server.

```
setup.exe /silent /install /components:OMReporting
/ManagementServer: "<ManagementServerName>"
/SRSInstance: <server\instance>
/DataReaderUser: <domain\username>
/DataReaderPassword: <password>
/SendODRReports: [0|1]
/UseMicrosoftUpdate: [0|1]
```

To confirm the health of Operations Manager reports

1. Open the Operations console, and select the **Reporting** workspace.

   Note

   After initial deployment, reports can require up to 30 minutes to appear.
2. Click **Microsoft ODR Report Library**, and then double-click any of the reports listed. The selected report is then generated and displayed in a new window.

   By default, you should see the following reports:

   - **Alerts Per Day**
   - **Instance Space**
   - **Management Group**
   - **Management Packs**
   - **Most Common Alerts**
3. Close the report window.

See Also

Distributed Deployment of Operations Manager

Deploying a Gateway Server

Gateway servers are used to enable agent-management of computers that are outside the Kerberos trust boundary of management groups, such as in a domain that is not trusted. The gateway server acts as a concentration point for agent-to-management server communication. Agents in domains that are not trusted communicate with the gateway server and the gateway server communicates with one or more management servers. Because communication between the gateway server and the management servers occurs over only one port (TCP 5723), that port is the only one that has to be opened on any intervening firewalls to enable management of multiple agent-managed computers. Multiple gateway servers can be placed in a single domain so that the agents can failover from one to the other if they lose communication with one of the

gateway servers. Similarly, a single gateway server can be configured to failover between management servers so that no single point of failure exists in the communication chain.

Because the gateway server resides in a domain that is not trusted by the domain that the management group is in, certificates must be used to establish each computer's identity, agent, gateway server, and management server. This arrangement satisfies the requirement of Operations Manager for mutual authentication.

Deploying a gateway topics

- How to Deploy a Gateway Server
- How to Chain Gateways

How to Deploy a Gateway Server

To monitor computers that lie outside the trust boundary of a management server without the use of a gateway server, you need to install and manually maintain certificates on the management servers and the computers to be monitored. When this configuration is used instead of using a gateway server, additional ports must be opened for agent-to-management server communication. For a listing of all ports that are necessary, see System Requirements for System Center 2012 – Operations Manager.

Procedure overview

1. Request certificates for any computer in the agent, gateway server, management server chain.
2. Import those certificates into the target computers by using the MOMCertImport.exe tool.
3. Distribute the Microsoft.EnterpriseManagement.GatewayApprovalTool.exe to the management server.
4. Run the Microsoft.EnterpriseManagement.GatewayApprovalTool.exe tool to initiate communication between the management server and the gateway
5. Install the gateway server.

Preparing for Installation

Before You Start

1. Deployment of gateway servers requires certificates. You need to have access to a certification authority (CA). This can be a public CA such as VeriSign, or you can use Microsoft Certificate Services. This procedure provides the steps to request, obtain, and import a certificate from Microsoft Certificate Services.
2. Reliable name resolution must exist between the agent-managed computers and the gateway server and between the gateway server and the management servers. This name resolution is typically done through DNS. However, if it is not possible to get proper name resolution through DNS, it might be necessary to manually create entries in each computer's hosts file.

Note

The hosts file is located in the \Windows\system32\drivers\ directory, and it contains directions for configuration.

Obtaining Computer Certificates from Microsoft Certificate Services

For more information, see Authentication and Data Encryption for Windows Computers.

Distributing the Microsoft.EnterpriseManagement.GatewayApprovalTool

The Microsoft.EnterpriseManagement.GatewayApprovalTool.exe tool is needed only on the management server, and it only has to be run once.

To copy Microsoft.EnterpriseManagement.GatewayApprovalTool.exe to management servers

1. From a target management server, open the Operations Manager installation media \SupportTools directory.
2. Copy the Microsoft.EnterpriseManagement.GatewayApprovalTool.exe from the installation media to the Operations Manager installation directory.

Registering the Gateway with the Management Group

This procedure registers the gateway server with the management group, and when this is completed, the gateway server appears in the Discovered Inventory view of the management group.

To run the gateway Approval tool

1. On the management server that was targeted during the gateway server installation, log on with the Operations Manager Administrator account.
2. Open a command prompt, and navigate to the Operations Manager installation directory or to the directory that you copied the Microsoft.EnterpriseManagement.gatewayApprovalTool.exe to.
3. At the command prompt, run `Microsoft.EnterpriseManagement.gatewayApprovalTool.exe /ManagementServerName=<managementserverFQDN> /GatewayName=<GatewayFQDN> /Action=Create`
4. If the approval is successful, you will see `The approval of server <GatewayFQDN> completed successfully.`
5. If you need to remove the gateway server from the management group, run the same command, but substitute the `/Action=Delete` flag for the `/Action=Create` flag.
6. Open the Operations console to the Monitoring view. Select the Discovered Inventory view to see that the gateway server is present.

Installing Gateway Server

This procedure installs the gateway server. The server that is to be the gateway server should be a member of the same domain as the agent-managed computers that will be reporting to it.

Tip

An installation will fail when starting Windows Installer (for example, installing a gateway server by double-clicking MOMGateway.msi) if the local security policy User Account Control: Run all administrators in Admin Approval Mode is enabled.

To run Operations Manager Gateway Windows Installer from a Command Prompt window

1. On the Windows desktop, click **Start**, point to **Programs**, point to **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
2. In the **Administrator: Command Prompt** window, navigate to the local drive that hosts the Operations Manager installation media.
3. Navigate to the directory where the .msi file is located, type the name of the .msi file, and then press ENTER.

To install the gateway server

1. Log on to the gateway server with Administrator rights.
2. From the Operations Manager installation media, start **Setup.exe**.
3. In the **Install** area, click the **Gateway management server** link.
4. On the **Welcome** screen, click **Next**.
5. On the **Destination Folder** page, accept the default, or click **Change** to select a different installation directory, and then click **Next**.
6. On the **Management Group Configuration** page, type the target management group name in the **Management Group Name** field, type the target management server name in the **Management Server** field, check that the **Management Server Port** field is **5723**, and then click **Next**. This port can be changed if you have enabled a different port for management server communication in the Operations console.
7. On the **Gateway Action Account** page, select the **Local System** account option, unless you have specifically created a domain-based or local computer-based gateway Action account. Click **Next**.
8. On the **Microsoft Update** page, optionally indicate if you want to use Microsoft Update, and then click **Next**.
9. On the **Ready to Install** page, click **Install**.
10. On the **Completing** page, click **Finish**.

To Install the gateway server by using the Command Prompt window

1. Log on to the gateway server with Administrator rights.
2. Open the Command Prompt window by using the **Run as Administrator** option.
3. Run the following command, where *path\Directory* is the location of the Momgateway.msi, and *path\Logs* is the location where you want to save the log file. Momgateway.msi can be found in the Operations Manager installation media.

```
%WinDir%\System32\msiexec.exe /i
path\Directory\MOMGateway.msi /qn /l*v
```

```
path\Logs\GatewayInstall.log
ADDLOCAL=MOMGateway
MANAGEMENT_GROUP="<ManagementGroupName>"
IS_ROOT_HEALTH_SERVER=0
ROOT_MANAGEMENT_SERVER_AD=<ParentMSFQDN>
ROOT_MANAGEMENT_SERVER_DNS=<ParentMSFQDN>
ACTIONS_USE_COMPUTER_ACCOUNT=0
ACTIONSDOMAIN=<DomainName>
ACTIONSUSER=<ActionAccountName>
ACTIONSPASSWORD=<Password>
ROOT_MANAGEMENT_SERVER_PORT=5723
[INSTALLDIR=<path\Directory>]
```

Importing Certificates with the MOMCertImport.exe Tool

Perform this operation on each gateway server, management server, and computer that will be agent-managed and that is in a domain that is not trusted.

To import computer certificates by using MOMCertImport.exe

1. Copy the MOMCertImport.exe tool from the installation media \SupportTools\<platform> (x86 or ia64) directory to the root of the target server or to the Operations Manager installation directory if the target server is a management server.
2. As an administrator, open a Command Prompt window and change the directory to the directory where MOMCertImport.exe is, and then run `momcertimport.exe /SubjectName <certificate subject name>`. This makes the certificate usable by Operations Manager.

Configuring Gateway Servers for Failover Between Management Servers

Although gateway servers can communicate with any management server in the management group, this must be configured. In this scenario, the secondary management servers are identified as targets for gateway server failover.

Use the Set-ManagementServer-gatewayManagementServer command in Operations Manager Shell, as shown in the following example, to configure a gateway server to failover to multiple management servers. The commands can be run from any Command Shell in the management group.

To configure gateway server failover between management servers

1. Log on to the management server with an account that is a member of the Administrators role for the management group.
2. On the Windows desktop, click **Start**, point to **Programs**, point to **System Center**

Operations Manager, and then click **Command Shell**.

3. In Command Shell, follow the example that is described in the next section.

Description

The following example can be used to configure gateway server failover to multiple management servers.

Code

```
$GatewayServer = Get-SCOMGatewayManagementServer –Name “ComputerName.Contoso.com”

$FailoverServer = Get-SCOMManagementServer –Name

“ManagementServer.Contoso.com”,”ManagementServer2.Contoso.com”

Set-SCOMParentManagementServer -GatewayServer $GatewayServer -FailoverServer

$FailoverServer
```

See Also

Deploying a Gateway Server

How to Chain Gateways

It is sometimes necessary to chain multiple gateways together in order to monitor across multiple untrusted boundaries. This topic describes how to chain multiple gateways together.

Note

You should install one gateway at a time and verify that each newly installed gateway is configured correctly before adding another gateway in the chain.

To chain multiple gateway servers

1. On the management server that was targeted during the gateway server installation, run the Microsoft.EnterpriseManagement.GatewayApprovalTool.exe tool to initiate communication between the management server and the gateway.
2. Open a command prompt, and navigate to the Operations Manager installation directory or, and then run the following: `Microsoft.EnterpriseManagement.gatewayApprovalTool.exe /ManagementServerName=<managementserverFQDN> /GatewayName=<GatewayFQDN> /Action=Create`
3. Install the gateway server on a new server. For more information, see Installing Gateway Server.
4. Configure the certificates between gateways in the same way that you would configure certificates between a gateway and a management server. For more information, see Importing Certificates with the MOMCertImport.exe Tool. The Health Service can only load and use a single certificate. Therefore, the same certificate is used by the parent and child of the gateway in the chain.

See Also

Deploying a Gateway Server

Authentication and Data Encryption for Windows Computers

System Center 2012 – Operations Manager consists of features such as the management server, gateway server, Reporting server, Operational database, Reporting data warehouse, agent, web console, and Operations console. This section explains how authentication is performed and identifies connection channels where the data is encrypted.

Certificate-Based Authentication

When an Operations Manager agent and management server are separated by either an untrusted forest or workgroup boundary, certificate-based authentication will need to be implemented. The following sections provide information about these situations and specific procedures for obtaining and installing certificates from Windows-based certification authorities.

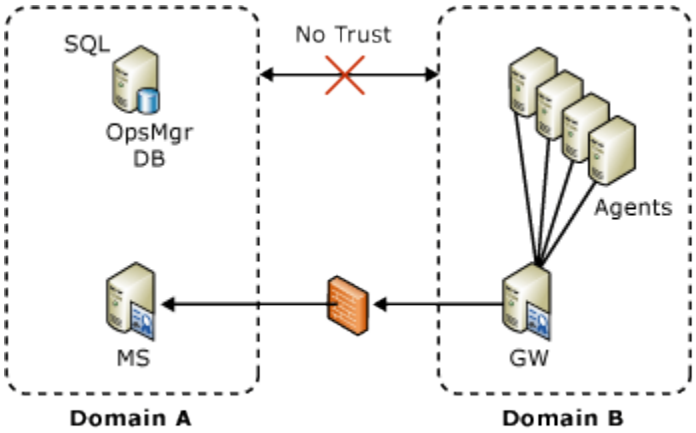
Setting Up Communication Between Agents and Management Servers Within the Same Trust Boundary

An agent and the management server use Windows authentication to mutually authenticate with each other before the management server accepts data from the agent. The Kerberos version 5 protocol is the default method for providing authentication. In order for Kerberos-based mutual authentication to function, the agents and management server must be installed in an Active Directory domain. If an agent and a management server are in separate domains, full trust must exist between the domains. In this scenario, after mutual authentication has taken place, the data channel between the agent and the management server is encrypted. No user intervention is required for authentication and encryption to take place.

Setting Up Communication Between Agents and Management Servers Across Trust Boundaries

An agent (or agents) might be deployed into a domain (domain B) separate from the management server (domain A), and no two-way trust might exist between the domains. Because there is no trust between the two domains, the agents in one domain cannot authenticate with the management server in the other domain using the Kerberos protocol. Mutual authentication between the Operations Manager features within each domain still occurs.

A solution to this situation is to install a gateway server in the same domain where the agents reside, and then install certificates on the gateway server and the management server to achieve mutual authentication and data encryption. The use of the gateway server means you need only one certificate in domain B and only one port through the firewall, as shown in the following illustration.

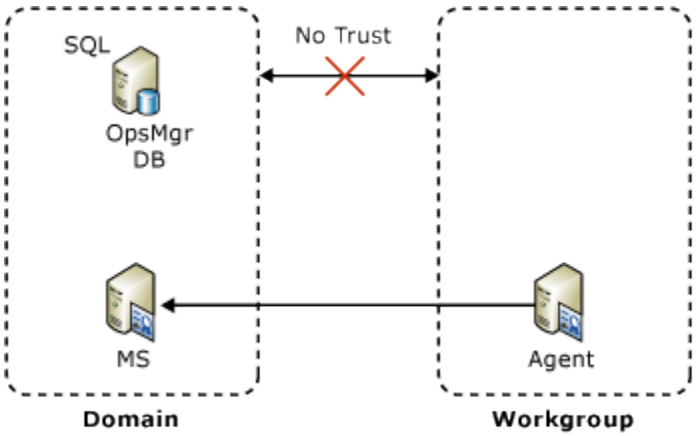


Setting Up Communication Across a Domain – Workgroup Boundary

In your environment, you may have one or two agents deployed to a workgroup inside your firewall. The agent in the workgroup cannot authenticate with the management server in the domain using the Kerberos protocol. A solution to this situation is to install certificates on both the computer hosting the agent and the management server that the agent connects to, as shown in the following illustration.

Note

In this scenario, the agent must be manually installed.



Perform the following steps on both the computer hosting the agent and the management server using the same certification authority (CA) for each:

- Request certificates from the CA.
- Approve the certificate requests on the CA.
- Install the approved certificates in the computer certificate stores.
- Use the MOMCertImport tool to configure Operations Manager.

These are the same steps for installing certificates on a gateway server, except you do not install or run the gateway approval tool.

Confirming Certificate Installation

If you have properly installed the certificate, the following event is written into the Operations Manager event log.

Type	Source	Event ID	General
Information	OpsMgr Connector	20053	The OpsMgr Connector has loaded the specified authentication certificate successfully.

During the setup of a certificate, you run the MOMCertImport tool. When the MOMCertImport tool has finished, the serial number of the certificate that you imported is written to the registry at the following subkey.

Caution

Incorrectly editing the registry can severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Machine Settings

Authentication and Data Encryption Between Management Server, Gateway Server, and Agents

Communication among these Operations Manager features begins with mutual authentication. If certificates are present on both ends of the communications channel, then certificates will be used for mutual authentication; otherwise, the Kerberos version 5 protocol is used. If any two features are separated across an untrusted domain, mutual authentication must be performed using certificates.

Normal communications, such as events, alerts, and deployment of a management pack, occur over this channel. The previous illustration shows an example of an alert being generated on one of the agents that is routed to the management server. From the agent to the gateway server, the Kerberos security package is used to encrypt the data, because the gateway server and the agent are in the same domain. The alert is decrypted by the gateway server and re-encrypted using certificates for the management server. After the management server receives the alert, the management server decrypts the message, re-encrypts it using the Kerberos protocol, and sends it to the management server where the management server decrypts the alert.

Some communication between the management server and the agent may include credential information; for example, configuration data and tasks. The data channel between the agent and the management server adds another layer of encryption in addition to the normal channel encryption. No user intervention is required.

Management Server and Operations Console, Web Console Server, and Reporting Server

Authentication and data encryption between the management server and the Operations console, web console server, or Reporting Server is accomplished by using Windows Communication

Foundation (WCF) technology. The initial attempt at authentication is made by using the user's credentials. The Kerberos protocol is attempted first. If the Kerberos protocol does not work, another attempt is made using NTLM. If authentication still fails, the user is prompted to provide credentials. After authentication has taken place, the data stream is encrypted as a function of either the Kerberos protocol or SSL, if NTLM is used.

In the case of a Reporting Server and a management server, after authentication has occurred, a data connection is established between the management server and SQL Server Reporting Server. This is accomplished by strictly using the Kerberos protocol; therefore, the management server and Reporting Server must reside in trusted domains. For more information about WCF, see the MSDN article What Is Windows Communication Foundation.

Management Server and Reporting Data Warehouse

Two communication channels exist between a management server and the Reporting data warehouse:

- The monitoring host process spawned by the health service (System Center Management service) in a management server
- The System Center Data Access services in the management server

Monitoring Host Process and Reporting Data Warehouse

By default, the monitoring host process spawned by the Health Service, which is responsible for writing collected events and performance counters to the data warehouse, achieves Windows Integrated Authentication by running as the Data Writer Account specified during Reporting Setup. The account credential is securely stored in a Run As Account called Data Warehouse Action Account. This Run As Account is a member of a Run As Profile called Data Warehouse Account (which is associated with the actual collection rules).

If the Reporting data warehouse and the management server are separated by a trust boundary (for example, each resides in different domains with no trust), then Windows Integrated Authentication will not work. To work around this situation, the monitoring host process can connect to the Reporting data warehouse using SQL Server Authentication. To do this, create a new Run As Account (of Simple Account type) with the SQL account credential and make it a member of the Run As Profile called Data Warehouse SQL Server Authentication Account, with the management server as the target computer.

Important

By default, the Run As Profile, Data Warehouse SQL Server Authentication Account was assigned a special account through the use of the Run As Account of the same name. Never make any changes to the account that is associated with the Run As Profile, Data Warehouse SQL Server Authentication Account. Instead, create your own account and your own Run As Account and make the Run As Account a member of the Run As Profile, Data Warehouse SQL Server Authentication Account when configuring SQL Server Authentication.

The following outlines the relationship of the various account credentials, Run As Accounts, and Run As Profiles for both Windows Integrated Authentication and SQL Server Authentication.

Default: Windows Integrated Authentication

Run As Profile: Data Warehouse Account

Run As Account: Data Warehouse Action Account

Credentials: Data Writer Account (specified during setup)

Run As Profile: Data Warehouse SQL Server Authentication Account

Run As Account: Data Warehouse SQL Server Authentication Account

Credentials: Special account created by Operations Manager (do not change)

Optional: SQL Server Authentication

Run As Profile: Data Warehouse SQL Server Authentication Account

Run As Account: A Run As Account you create.

Credentials: An account you create.

The System Center Data Access Service and Reporting Data Warehouse

By default, the System Center Data Access service, which is responsible for reading data from the Reporting data warehouse and making it available in the Report Parameter Area, achieves Windows Integrated Authentication by running as the Data Access Service and Config Service account that was defined during setup of Operations Manager.

If the Reporting data warehouse and the management server are separated by a trust boundary (for example, each resides in different domains with no trust), then Windows Integrated Authentication would not work. To work around this situation, the System Center Data Access service can connect to the Reporting data warehouse using SQL Server Authentication. To do this, create a new Run As Account (of Simple Account type) with the SQL account credential and make it a member of the Run As Profile called Reporting SDK SQL Server Authentication Account with the management server as the target computer.

Important

By default, the Run As Profile, Reporting SDK SQL Server Authentication Account was assigned a special account through the use of the Run As Account of the same name. Never make any changes to the account that is associated with the Run As Profile, Reporting SDK SQL Server Authentication Account. Instead, create your own account and your own Run As Account, and make the Run As Account a member of the Run As Profile, Reporting SDK SQL Server Authentication Account when configuring SQL Server Authentication.

The following outlines the relationship of the various account credentials, Run As Accounts, and Run As Profiles for both Windows Integrated Authentication and SQL Server Authentication.

Default: Windows Integrated Authentication

Data Access Service and Config Service Account (defined during setup of Operations Manager)

Run As Profile: Reporting SDK SQL Server Authentication Account

Run As Account: Reporting SDK SQL Server Authentication Account

Credentials: Special account created by Operations Manager (do not change)

Optional: SQL Server Authentication

Run As Profile: Data Warehouse SQL Server Authentication Account

Run As Account: A Run As Account you create.

Credentials: An account you create.

Operations Console and Reporting Server

The Operations console connects to Reporting Server on port 80 using HTTP. Authentication is performed by using Windows Authentication. Data can be encrypted by using the SSL channel. For more information about using SSL between the Operations console and Reporting Server, see How to Configure the Operations Console to Use SSL When Connecting to a Reporting Server.

Reporting Server and Reporting Data Warehouse

Authentication between Reporting Server and the Reporting data warehouse is accomplished using Windows Authentication. The account that was specified as the Data Reader Account during setup of Reporting becomes the Execution Account on Reporting Server. If the password for the account should change, you will need to make the same password change using the Reporting Services Configuration Manager in SQL Server. For more information about resetting this password, see How to Change the Reporting Server Execution Account Password. The data between the Reporting Server and the Reporting data warehouse is not encrypted.

How to Obtain a Certificate Using Windows Server 2008 Enterprise CA

Use the procedures in this topic to obtain a certificate from Windows Server 2008 R2, or Windows Server 2008 R2 SP1 computer hosting Enterprise Root Active Directory Certificate Services (AD CS). You use the CertReq command-line utility to request and accept a certificate, and you use a Web interface to submit and retrieve your certificate.

It is assumed that you have AD CS installed, an HTTPS binding has been created, and its associated certificate has been installed. Information about creating an HTTPS binding is available in the topic How to Configure an HTTPS Binding for a Windows Server 2008 CA.

Important

The content for this topic is based on the default settings for Windows Server 2008 AD CS; for example, setting the key length to 2048, selecting Microsoft Software Key Storage Provider as the CSP, and using Secure Hash Algorithm 1 (SHA1). Evaluate these selections against the requirements of your company's security policy.

The high-level process to obtain a certificate from an Enterprise certification authority (CA) is as follows:

1. Download the Trusted Root (CA) certificate.
2. Import the Trusted Root (CA) certificate.
3. Create a certificate template.
4. Add the template to the Certificate Templates folder.
5. Create a setup information file for use with the CertReq command-line utility.
6. Create a request file.
7. Submit a request to the CA.

8. Import the certificate into the certificate store.
9. Import the certificate into Operations Manager using MOMCertImport.

Download the Trusted Root (CA) certificate

To download the Trusted Root (CA) certificate

1. Log on to the computer where you want to install a certificate; for example, the gateway server or management server.
2. Start Internet Explorer, and connect to the computer hosting Certificate Services; for example, https://<servername>/certsrv.
3. On the **Welcome** page, click **Download a CA Certificate, certificate chain, or CRL**.
4. On the **Download a CA Certificate, Certificate Chain, or CRL** page, click **Encoding method**, click **Base 64**, and then click **Download CA certificate chain**.
5. In the **File Download** dialog box, click **Save** and save the certificate; for example, **Trustedca.p7b**.
6. When the download has finished, close Internet Explorer.

Import the Trusted Root (CA) certificate

To import the Trusted Root (CA) Certificate

1. On the Windows desktop, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **mmc**, and then click **OK**.
3. In the **Console1** window, click **File**, and then click **Add/Remove Snap-in**.
4. In the **Add/Remove Snap-in** dialog box, click **Add**.
5. In the **Add Standalone Snap-in** dialog box, click **Certificates**, and then click **Add**.
6. In the **Certificates snap-in** dialog box, select **Computer account**, and then click **Next**.
7. In the **Select Computer** dialog box, ensure that **Local computer: (the computer this console is running on)** is selected, and then click **Finish**.
8. In the **Add Standalone Snap-in** dialog box, click **Close**.
9. In the **Add/Remove Snap-in** dialog box, click **OK**.
10. In the **Console1** window, expand **Certificates (Local Computer)**, expand **Trusted Root Certification Authorities**, and then click **Certificates**.
11. Right-click **Certificates**, select **All Tasks**, and then click **Import**.
12. In the Certificate Import Wizard, click **Next**.
13. On the **File to Import** page, click **Browse** and select the location where you downloaded the CA certificate file, for example, TrustedCA.p7b, select the file, and then click **Open**.
14. On the **File to Import** page, select **Place all certificates in the following store** and ensure that **Trusted Root Certification Authorities** appears in the **Certificate store** box, and then click **Next**.
15. On the **Completing the Certificate Import Wizard** page, click **Finish**.

Create a certificate template

To create a certificate template

1. On the computer that is hosting your enterprise CA, on the Windows desktop, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Certification Authority**.
2. In the navigation pane, expand the CA name, right-click **Certificate Templates**, and then click **Manage**.
3. In the **Certificate Templates** console, in the results pane, right-click **IPsec (Offline request)**, and then click **Duplicate Template**.
4. In the **Duplicate Template** dialog box, select **Windows Server 2008 Enterprise Edition**, and then click **OK**.
5. In the **Properties of New Template** dialog box, on the **General** tab, in the **Template display name** text box, type a new name for this template; for example, **OperationsManagerCert**.
6. On the **Request Handling** tab, select **Allow private key to be exported**.
7. Click the **Extensions** tab, and in **Extensions included in this template**, click **Application Policies**, and then click **Edit**.
8. In the **Edit Application Policies Extension** dialog box, click **IP security IKE intermediate,** and then click **Remove**.
9. Click **Add**, and in the **Application policies list**, hold down the CTRL key to multi-select items from the list, click **Client Authentication** and **Server Authentication**, and then click **OK**.
10. In the **Edit Application Policies Extension** dialog box, click **OK**.
11. Click the **Security** tab and ensure that the **Authenticated Users** group has **Read** and **Enroll** permissions, and then click **OK**.
12. Close the Certificate Templates console.

Add the template to the Certificate Templates folder

To add the template to the Certificate Templates folder

1. On the computer that is hosting your Enterprise CA, in the Certification Authority snap-in, right-click the **Certificate Templates** folder, point to **New**, and then click **Certification Template to Issue**.
2. In the **Enable Certificate Templates** box, select the certificate template that you created; for example, click **OperationsManagerCert**, and then click **OK**.

Create a setup information file for use with the CertReq command-line utility

To create a setup information (.inf) file

1. On the computer hosting the Operations Manager feature for which you are requesting a certificate, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **Notepad**, and then click **OK**.

3. Create a text file containing the following content:

   [NewRequest]

   Subject="CN=<FQDN of computer you are creating the certificate, for example, the gateway server or management server.>"

   Exportable=TRUE

   KeyLength=2048

   KeySpec=1

   KeyUsage=0xf0

   MachineKeySet=TRUE

   [EnhancedKeyUsageExtension]

   OID=1.3.6.1.5.5.7.3.1

   OID=1.3.6.1.5.5.7.3.2
4. Save the file with an .inf file name extension; for example, RequestConfig.inf.
5. Close Notepad.

Create a request file

To create a request file to use with an enterprise CA

1. On the computer hosting the Operations Manager feature for which you are requesting a certificate, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. In the command window, type **CertReq –New –f RequestConfig.inf CertRequest.req**, and then press ENTER.
4. Using Notepad, open the resulting file (for example, CertRequest.req), and copy the contents of this file into the clipboard.

Submit a request to the CA

To submit a request to an enterprise CA

1. On the computer hosting the Operations Manager feature for which you are requesting a certificate, start Internet Explorer, and then connect to the computer hosting Certificate Services; for example, https://<servername>/certsrv.

   Note
   If an HTTPS binding has not been configured on the Certificate Services Web site, the browser will fail to connect. See the topic **How to Configure an HTTPS Binding for a Windows Server 2008 CA** in this guide.
2. On the **Microsoft Active Directory Certificate Services Welcome** screen, click **Request a certificate**.
3. On the **Request a Certificate** page, click **advanced certificate request**.
4. On the **Advanced Certificate Request** page, click **Submit a certificate request by**

using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

5. On the **Submit a Certificate Request or Renewal Request** page, in the **Saved Request** text box, paste the contents of the CertRequest.req file that you copied in step 4 in the previous procedure.
6. In the **Certificate Template** select the certificate template that you created, for example, OperationsManagerCert, and then click **Submit**.
7. On the **Certificate Issued** page, select **Base 64 encoded**, and then click **Download certificate**.
8. In the **File Download – Security Warning** dialog box, click **Save**, and save the certificate; for example, save as NewCertificate.cer.
9. Close Internet Explorer.

Import the certificate into the certificate store

To import the certificate into the certificate store

1. On the computer hosting the Operations Manager feature for which you are configuring the certificate, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. In the command window, type **CertReq –Accept NewCertifiate.cer**, and then press ENTER.

Import the certificate into Operations Manager using MOMCertImport

To import the certificate into Operations Manager using MOMCertImport

1. Log on to the computer where you installed the certificate with an account that is a member of the Administrators group.
2. On the Windows desktop, click **Start**, and then click **Run**.
3. In the **Run** dialog box, type **cmd**, and then click **OK**.
4. At the command prompt, type **<***drive_letter***>:** (where <*drive_letter*> is the drive where the Operations Manager installation media is located), and then press ENTER.
5. Type **cd\SupportTools\i386**, and then press ENTER.

   Note
   On 64-bit computers, type **cd\SupportTools\amd64**
6. Type the following:

   MOMCertImport /SubjectName <Certificate Subject Name>
7. Press ENTER.

See Also

Authentication and Data Encryption for Windows Computers

How to Obtain a Certificate Using Windows Server 2008 Stand-Alone CA

Use the procedures in this topic to obtain a certificate from a stand-alone Windows Server 2008 R2, or Windows Server 2008 R2 SP1–based computer hosting Active Directory Certificate Services (AD CS). You use the CertReq command-line utility to request and accept a certificate, and you use a Web interface to submit and retrieve your certificate.

It is assumed that you have AD CS installed, an HTTPS binding is being used, and its associated certificate has been installed. Information about creating an HTTPS binding is available in the topic How to Configure an HTTPS Binding for a Windows Server 2008 CA.

Important

The content for this topic is based on the default settings for Windows Server 2008 AD CS; for example, setting the key length to 2048, selecting Microsoft Software Key Storage Provider as the CSP, and using Secure Hash Algorithm 1 (SHA1). Evaluate these selections against the requirements of your company's security policy.

The high-level process to obtain a certificate from a stand-alone certification authority (CA) is as follows:

1. Download the Trusted Root (CA) certificate.
2. Import the Trusted Root (CA) certificate
3. Create a setup information file to use with the CertReq command-line utility.
4. Create a request file.
5. Submit a request to the CA using the request file.
6. Approve the pending certificate request.
7. Retrieve the certificate from the CA.
8. Import the certificate into the certificate store.
9. Import the certificate into Operations Manager using MOMCertImport.

Download the Trusted Root (CA) certificate

To download the Trusted Root (CA) certificate

1. Log on to the computer where you want to install a certificate; for example, the gateway server or management server.
2. Start Internet Explorer, and connect to the computer hosting Certificate Services; for example, https://<servername>/certsrv.
3. On the **Welcome** page, click **Download a CA Certificate, certificate chain, or CRL**.
4. On the **Download a CA Certificate, Certificate Chain, or CRL** page, click **Encoding method**, click **Base 64**, and then click **Download CA certificate chain**.
5. In the **File Download** dialog box, click **Save** and save the certificate; for example, **Trustedca.p7b**.
6. When the download has finished, close Internet Explorer.

Import the Trusted Root (CA) certificate

To import the Trusted Root (CA) Certificate

1. On the Windows desktop, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **mmc,** and then click **OK**.
3. In the **Console1** window, click **File**, and then click **Add/Remove Snap-in**.
4. In the **Add/Remove Snap-in** dialog box, click **Add**.
5. In the **Add Standalone Snap-in** dialog box, click **Certificates**, and then click **Add**.
6. In the **Certificates snap-in** dialog box, select **Computer account**, and then click **Next**.
7. In the **Select Computer** dialog box, ensure that **Local computer: (the computer this console is running on)** is selected, and then click **Finish**.
8. In the **Add Standalone Snap-in** dialog box, click **Close**.
9. In the **Add/Remove Snap-in** dialog box, click **OK**.
10. In the **Console1** window, expand **Certificates (Local Computer)**, expand **Trusted Root Certification Authorities**, and then click **Certificates**.
11. Right-click **Certificates**, select **All Tasks**, and then click **Import**.
12. In the Certificate Import Wizard, click **Next**.
13. On the **File to Import** page, click **Browse** and select the location where you downloaded the CA certificate file, for example, TrustedCA.p7b, select the file, and then click **Open**.
14. On the **File to Import** page, select **Place all certificates in the following store** and ensure that **Trusted Root Certification Authorities** appears in the **Certificate store** box, and then click **Next**.
15. On the **Completing the Certificate Import Wizard** page, click **Finish**.

Create a setup information file

To create a setup information (.inf) file

1. On the computer hosting the Operations Manager feature for which you are requesting a certificate, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **Notepad**, and then click **OK**.
3. Create a text file containing the following content:

   [NewRequest]

   Subject="CN=<FQDN of computer you are creating the certificate, for example, the gateway server or management server.>"

   Exportable=TRUE

   KeyLength=2048

   KeySpec=1

   KeyUsage=0xf0

   MachineKeySet=TRUE

   [EnhancedKeyUsageExtension]

   OID=1.3.6.1.5.5.7.3.1

   OID=1.3.6.1.5.5.7.3.2

4. Save the file with an .inf file name extension, for example, RequestConfig.inf.
5. Close Notepad.

Create a request file

To create a request file to use with a stand-alone CA

1. On the computer hosting the Operations Manager feature for which you are requesting a certificate, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. In the command window, type **CertReq –New –f RequestConfig.inf CertRequest.req**, and then press ENTER.
4. Open the resulting file (for example, CertRequest.req) with Notepad. Copy the contents of this file onto the clipboard.

Submit a request to the CA using the request file

To submit a request to a stand-alone CA

1. On the computer hosting the Operations Manager feature for which you are requesting a certificate, start Internet Explorer, and then connect to the computer hosting Certificate Services (for example, https://<servername>/certsrv).

   Note
   If an HTTPS binding has not been configured on the Certificate Services Web site, the browser will fail to connect. For more information, see How to Configure an HTTPS Binding for a Windows Server 2008 CA.
2. On the **Microsoft Active Directory Certificate Services Welcome** screen, click **Request a certificate**.
3. On the **Request a Certificate** page, click **advanced certificate request**.
4. On the **Advanced Certificate Request** page, click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.**
5. On the **Submit a Certificate Request or Renewal Request** page, in the **Saved Request** text box, paste the contents of the CertRequest.req file that you copied in step 4 in the previous procedure, and then click **Submit**.
6. Close Internet Explorer.

Approve the pending certificate request

To approve the pending certificate request

1. Log on as a certification authority administrator to the computer hosting Active Directory Certificate Services.
2. On the Windows desktop, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Certification Authority**.

3. In **Certification Authority**, expand the node for your certification authority name, and then click **Pending Requests**.
4. In the results pane, right-click the pending request from the previous procedure, point to **All Tasks**, and then click **Issue**.
5. Click **Issued Certificates**, and confirm the certificate you just issued is listed.
6. Close Certification Authority.

Retrieve the certificate from the CA

To retrieve the certificate

1. Log on to the computer where you want to install a certificate; for example, the gateway server or management server.
2. Start Internet Explorer, and connect to the computer hosting Certificate Services (for example, https://<servername>/certsrv).
3. On the **Microsoft Active Directory Certificate Services Welcome** page, click **View the status of a pending certificate request**.
4. On the **View the Status of a Pending Certificate Request** page, click the certificate you requested.
5. On the **Certificate Issued** page, select **Base 64 encoded**, and then click **Download certificate**.
6. In the **File Download – Security Warning** dialog box, click **Save**, and save the certificate; for example, as NewCertificate.cer.
7. On the **Certificate Installed** page, after you see the message that **Your new certificate has been successfully installed,** close the browser.
8. Close Internet Explorer.

Import the certificate into the certificate store

To import the certificate into the certificate store

1. On the computer hosting the Operations Manager feature for which you are configuring the certificate, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. In the command window, type **CertReq –Accept NewCertifiate.cer**, and then press ENTER.

Import the certificate into Operations Manager using MOMCertImport

To import the certificate into Operations Manager using MOMCertImport

1. Log on to the computer where you installed the certificate with an account that is a member of the Administrators group.
2. On the Windows desktop, click **Start**, and then click **Run**.
3. In the **Run** dialog box, type **cmd**, and then click **OK**.

4. At the command prompt, type **<***drive_letter***>:** (where <*drive_letter*> is the drive where the Operations Manager installation media is located), and then press ENTER.
5. Type **cd\SupportTools\i386**, and then press ENTER.

   Note
   On 64-bit computers, type **cd\SupportTools\amd64**
6. Type the following:

   MOMCertImport /SubjectName <Certificate Subject Name>
7. Press ENTER.

See Also

Authentication and Data Encryption for Windows Computers

How to Configure an HTTPS Binding for a Windows Server 2008 CA

If you are setting up a new certification authority (CA) for the first time for use with System Center 2012 – Operations Manager, use the following procedure to configure an HTTPS binding for the CA.

To configure an HTTPS binding

1. On the computer hosting your CA, on the Windows desktop, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In the **Internet Information Services (IIS) Manager** dialog box, in the **Connections** pane, expand your computer name, expand **Sites**, and then click **Default Web Site**.
3. In the **Actions** pane, click **Bindings**.
4. In the **Site Bindings** dialog box, click **Add**.
5. In the **Add Site Binding** dialog box, on the **Type** menu, select **https**.
6. In the **SSL Certificate** list, select the entry that matches the name of your computer, and then click **OK**.
7. In the **Site Bindings** dialog box, click **Close**.
8. In the **Connections** pane, under **Default Web Site**, click **CertSrv**.
9. In the **/CertSrv Home** pane, right-click **SSL Settings**, and then click **Open Feature**.
10. In the **SSL Settings** pane, click **Require SSL**.
11. In the **Actions** pane, click **Apply**, and then close Internet Information Services (IIS) Manager.

Deploying ACS and ACS Reporting

In System Center 2012 – Operations Manager, Audit Collection Services (ACS) provides a means to collect records generated by an audit policy and store them in a centralized database. Using ACS, organizations can consolidate individual Security logs into a centrally managed database and can filter and analyze events using the data analysis and reporting tools provided

by Microsoft SQL Server. For more information, see Collecting Security Events Using Audit Collection Services in Operations Manager 2012

Audit Collection Services (ACS) reporting can be installed in two configurations.

- A supported version of Microsoft SQL Server Reporting Services (SSRS) instance with Operations Manager Reporting already installed. A benefit of this is the ability to view ACS Reports in the Operations console.
- An SSRS instance without Operations Manager Reporting installed.

The installation procedures for ACS Reporting do not differ, but the application of access control is different. By deploying ACS Reporting on the same SQL Server Reporting Services instance as your Operations Manager Reporting, the same role-based security applies to all reports. This means that ACS Reporting users need to be assigned to the Operations Manager Report Operator Role to access the ACS reports.

In addition to membership in the Operations Manager Reporting Role, ACS report users must also be assigned db_datareader role on the ACS database (OperationsManagerAC) to run ACS reports. This requirement is independent of the presence of Operations Manager Reporting

If you choose to install ACS Reporting independently of Operations Manager Reporting, you can also use SSRS security to secure the reports. For more information, see the SQL Server Books Online tutorial Tutorial: Setting Permissions in Reporting Services.

Preparing for installation

Deploy ACS as described in the following topics prior to installing ACS Reporting.

- How to Install Audit Collection Services (ACS)
- How to Deploy ACS on a Secondary Management Server
- How to Install an Audit Collection Services (ACS) Collector and Database
- How to Deploy Audit Collection Services for UNIX/Linux

Before you start

1. A management server for your management group must be installed and ACS must be configured on the management server. For more information, see Collecting Security Events Using Audit Collection Services in Operations Manager .
2. An instance of a supported version of Microsoft SQL Server Reporting Services must be installed on the target computer.
3. During the procedure, you need to be logged on as member of Operations Manager Report Operator user role.
4. IIS must be installed on the hosting system. IIS will have already been installed if you are co-locating with a Reporting server.
5. You need to have access to the ACS database.
6. You need the Operations Manager installation media.

The following content will help you install ACS on a secondary management server, and install ACS Reporting.

- How to Deploy ACS on a Secondary Management Server
- How to Deploy ACS Reporting

How to Install Audit Collection Services (ACS)

The following procedure provides the general steps needed to install the System Center 2012 – Operations Manager Audit Collection Services (ACS) feature within your organization.

Note

To uninstall Operations Manager from the management server that functions as your ACS Collector, you must first uninstall ACS.

See Collecting Security Events Using Audit Collection Services in Operations Manager in the Operations Guide for information on minimum and recommended system requirements for ACS.

To install Audit Collection Services

1. Plan an audit policy for your organization. For more information on setting up an audit policy, see Advanced Security Audit Policy Step-by-Step Guide.
2. Plan your ACS server deployment. This includes deciding which server will act as the ACS database and which management server will act as the ACS collector. Ensure that the computers selected for these roles meet the minimum system requirements. See Collecting Security Events Using Audit Collection Services in Operations Manager in the Operations Guide for more information about ACS and the system requirements for each feature.
3. Plan which Operations Manager agents will be ACS forwarders. All computers that you want to collect security events from must be ACS forwarders.
4. Install and configure prerequisites for ACS features.
5. (Optional) Separate administrator and auditor roles by doing the following:
    a. Create a local group just for users who access and run reports on the data in the ACS database. For step-by-step instructions for creating a local group, see the “To create a group account in Active Directory” section of the "Creating user and group accounts" topic at http://go.microsoft.com/fwlink/?LinkId=74159.
    b. Grant the newly created local group access to the SQL database by creating a new SQL Login for the group and assigning that login the db_datareader permission. For step-by-step instructions for creating a SQL Login, go to Set up a user account on a SQL server.
    c. Add the user accounts of users who will act as auditors to the local group.
6. Deploy the ACS Database and ACS Collector(s). See How to Install an Audit Collection Services (ACS) Collector and Database.
7. Run the **Enable Audit Collection** task to start the ACS Forwarder service on the ACS forwarders. For more information, see How to Enable Audit Collection Services (ACS) Forwarders.
8. Implement your audit policy within your organization.

See Also

Deploying ACS and ACS Reporting

How to Install an Audit Collection Services (ACS) Collector and Database

How to Deploy ACS on a Secondary Management Server

How to Deploy ACS Reporting

How to Install an Audit Collection Services (ACS) Collector and Database

Use the following procedures in System Center 2012 – Operations Manager to install an Audit Collection Services (ACS) collector and database and to start the service for the ACS collector computer. Both procedures are performed on the computer that is designated as your ACS collector.

The ACS database runs on a supported version of Microsoft SQL Server. The Audit Collection Services Collector Setup wizard creates the ACS database on an existing installation of Microsoft SQL Server. To complete the installation procedure, you must be a member of the local Administrators group on both the ACS collector and the ACS database computers as well as a database administrator on the ACS database. As a best practice for security, consider using Run As to perform this procedure.

For information about system requirements and best practices for performance, see Collecting Security Events Using Audit Collection Services in Operations Manager and Audit Collection Services Capacity Planning in the Operations Guide.

To install an ACS collector and an ACS database

1. Log on to the server by using an account that has local administrative credentials.
2. On the Operations Manager installation media, run **Setup.exe**, and then click **Audit collection services**.

   For monitoring UNIX and Linux computers, click **Audit collection services for UNIX/Linux**.

   The **Audit Collection Services Collector Setup** wizard opens.
3. On the **Welcome** page, click **Next**.
4. On the **License Agreement** page, read the licensing terms, click **I accept the agreement**, and then click **Next**.
5. On the **Database Installation Options** page, click **Create a new database**, and then click **Next**.
6. On the **Data Source** page, in the **Data source name** box, type a name that you want to use as the Open Database Connectivity (ODBC) data source name for your ACS database. By default, this name is **OpsMgrAC**. Click **Next**.
7. On the **Database** page, if the database is on a separate server than the ACS collector, click **Remote Database Server**, and then type the computer name of the database server that will host the database for this installation of ACS. Otherwise, click **Database server running locally**.
8. In the **Database server instance name** field, type the name of the database that will be created for ACS. If you leave this field blank, the default name is used. In the **Database**

name field, the default database name of **OperationsManagerAC** is automatically entered. You can select the text and type in a different name or leave the default name. Click **Next**.

> **Note**
> To display a list of SQL Server Instances, on the database computer click **Start**, point to **Programs** and open **SQL Server** (the appropriate version of SQL Server is dependent on the version of Operations Manager – see System Requirements for System Center 2012 – Operations Manager), and then click **SQL Server Management Studio**. On the **Server name** list, click **Browse for more** and then expand **Database Engine**. All databases are listed as server name\database name.

9. On the **Database Authentication** page, select one of the authentication methods. If the ACS collector and the ACS database are members of the same domain, you can select **Windows authentication**, otherwise select **SQL authentication**, and then click **Next**.

> **Note**
> If you select **SQL authentication** and click **Next**, the **Database Credentials** page displays. In the **SQL login name** box, enter the name of the user account that has access to the SQL Server and the password for that account in the **SQL password** box, and then click **Next**.

10. On the **Database Creation Options** page, click **Use SQL Server's default data and log file directories** to use SQL Server's default folders. Otherwise, click **Specify directories** and enter the full path, including drive letter, to the location you want for the ACS database and log file, for example C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data. Click **Next**.
11. On the **Event Retention Schedule** page, click **Local hour of day to perform daily database maintenance**. Choose a time when the number of expected security events is low. During the database maintenance period, database performance will be impacted. In the **Number of days to retain events** box type the number of days ACS should keep events in the ACS database before the events are removed during database grooming. The default value is 14 days. Click **Next**.
12. On the **ACS Stored Timestamp Format** page, choose **Local** or **Universal Coordinated Time**, formerly known to as Greenwich Mean Time, and then click **Next**
13. The **Summary** page displays a list of actions that the installation program will perform to install ACS. Review the list, and then click **Next** to begin the installation.

> **Note**
> If a **SQL server login** dialog box displays and the database authentication is set to **Windows authentication**, click the correct database and verify that the **Use Trusted Connection** check box is checked. Otherwise click to remove the check and enter the SQL login name and password. Click **OK**.

14. When the installation is complete, click **Finish**.

See Also

Deploying ACS and ACS Reporting

How to Install Audit Collection Services (ACS)

How to Deploy ACS on a Secondary Management Server

How to Deploy ACS Reporting

How to Deploy ACS on a Secondary Management Server

In this procedure, the Audit Collection Services Collector and the Audit Collection Services (ACS) databases are installed on different servers, with the ACS Collector on a stand-alone management server and the ACS database on a separate database. The Operations Manager ACS Collector service must be installed on an existing management server. You can also choose to create a database for ACS to use or you can let the setup program create one for you. In this procedure, an already existing stand-alone secondary management server is used for the ACS Collector and a new ACS Database is created by the ACS setup. For an overview of ACS, see Collecting Security Events Using Audit Collection Services in Operations Manager 2012.

When you are done with this procedure, you must enable the ACS forwarder function on all Operations Manager Agents that you want to collect Windows Security Event Log events from. For more information about enabling ACS forwarders, see How to Enable ACS Forwarders.

To install ACS on a secondary management server

1. Log on to the secondary management server that is to host the ACS Collector with the domain-based Operations Manager Administrator account. This account should already have local administrative rights.
2. On the Operations Manager installation media, start **Setup.exe**.
3. Under the **Install** heading, click the **Audit collection services** link. The **Audit Collection Services Collector Setup** wizard opens.
4. On the **Welcome** page, click **Next**.
5. On the **License Agreement** page, select the **I accept the agreement** option and click **Next**.
6. On the **Database Installation Options** page, select the **Create a new database** option. This creates the ACS database on the designated instance of SQL Server with the necessary tables and stored procedures and the SQL login and database user for the collector. Click **Next**.
7. On the **Data Source** page, in the **Data Source name** field, accept the default value of **OpsMgrAC**, and then click **Next**.

   Note
   The ACS Collector uses an Open Database Connectivity (ODBC) Data Source Name (DSN) to communicate with the ACS database.
8. On the **Database** page, select the **Remote database server** option. In the **Remote database server machine name** field, enter the value in the name field of the SQL Server network. Leave the **Database server instance name** field blank, unless you have installed a SQL Server cluster in a named instance of SQL Server, and then enter that

value. In the **Database name** field, accept the default of **OperationsManagerAC**, but if you plan to host multiple ACS databases in the same instance of SQL Server, enter a unique name. Click **Next**.

9. On the **Database Authentication** page, select **Windows authentication**, and then click **Next**. By selecting Windows authentication, the ACS Collector services will use the local machine account to write to the ACS database during normal operations.
10. On the **Database Creation Options** page, select the **Use SQL Server default data and log file directories** option, and then click **Next**.
11. On the **Event Retention Schedule** page, set the **Local hour of day to perform daily maintenance** and **Number of days an event is retained in database** options to the appropriate values, and then click **Next**.
12. On the **ACS Stored Timestamp Format** page, select either the **Local** or **Universal Coordinated Time (UTC)** option, and then click **Next**.
13. On the **Summary** page, review the installation options, and then click **Next**.
14. During the installation, you might be prompted for a SQL Server Login. If you are logged on with an account that has SQL Server Administrator rights, then accept the default or otherwise provide credentials that have the SQL Server Administrator rights.

    Note
    This account is used by the setup process to create the ACS database.
15. Click **Finish** to complete the installation.
16. Open the **SQL Server Management Studio** tool, open the **Databases** folder, and confirm the presence of the **OperationsManagerAC** database.
17. On the ACS management server, open **Server Manager** tool, expand the **Configuration** container and select **Services**, and confirm that the **Operations Manager Audit Collection Service** is present, that it is started, and that the **Startup Type** is set to **Automatic**.
18. You can now enable the ACS forwarders. For more information, see How to Enable ACS Forwarders.

See Also

Deploying ACS and ACS Reporting

How to Install an Audit Collection Services (ACS) Collector and Database

How to Install Audit Collection Services (ACS)

How to Deploy ACS Reporting

How to Deploy ACS Reporting

You deploy Audit Collection Services (ACS) Reporting on a supported version of Microsoft SQL Server Reporting Services (SSRS) instance. If System Center 2012 – Operations Manager Reporting has also been installed on the same SSRS instance, you can view the ACS Reports in the Operations console. Before you deploy ACS, there are a number of prerequisite steps you must perform, such as ensuring that a ACS is configured on management server within your management group. For more information, see Deploying ACS and ACS Reporting.

To deploy ACS Reporting

1. Log on to the server that will be used to host ACS reporting as a user that is an administrator of the SSRS instance.
2. Create a temporary folder, such as **C:\acs**.
3. On your installation media, go to **\ReportModels\acs** and copy the directory contents to the temporary installation folder.

   There are two folders (**Models** and **Reports**) and a file named **UploadAuditReports.cmd**.
4. On your installation media, go to **\SupportTools** and copy the file **ReportingConfig.exe** into the temporary **acs** folder.
5. Open a Command Prompt window by using the **Run as Administrator** option, and then change directories to the temporary **acs** folder.
6. Run the following command.
   UploadAuditReports "<AuditDBServer\Instance>" "<Reporting Server URL>" "<path of the copied acs folder>"
   For example: **UploadAuditReports "myAuditDbServer\Instance1" "http://myReportServer/ReportServer$instance1" "C:\acs"**

   This example creates a new data source called **Db Audit**, uploads the reporting models **Audit.smdl** and **Audit5.smdl**, and uploads all reports in the **acs\reports** directory.

   Note
   The reporting server URL needs the reporting server virtual directory (**ReportingServer_<InstanceName>**) instead of the reporting manager directory (**Reports_<InstanceName>**).
7. Open Internet Explorer and enter the following address to view the **SQL Reporting Services Home** page. **http://<yourReportingServerName>/Reports_<InstanceName>**
8. Click **Audit Reports** in the body of the page and then click **Show Details** in the upper right part of the page.
9. Click the **Db Audit** data source.
10. In the **Connect Using** section, select **Windows Integrated Security** and click **Apply**.

See Also

Deploying ACS and ACS Reporting

How to Install an Audit Collection Services (ACS) Collector and Database

How to Deploy ACS on a Secondary Management Server

How to Install Audit Collection Services (ACS)

How to Deploy Audit Collection Services for UNIX/Linux

This procedure describes the steps to deploy Audit Collection Services for UNIX/Linux to enable security event collection and reporting for monitored UNIX and Linux computers.

In this Topic

- Prerequisite Configuration
- Installing Audit Collection Services for UNIX/Linux
- Importing UNIX and Linux ACS Management Packs
- Installing ACS Reports for UNIX/Linux
- How to Enable Audit Collection Services for UNIX/Linux

Prerequisite Configuration

Before deploying Audit Collection Services for UNIX/Linux, ACS and ACS Reporting must be deployed and configured. See the following topic for information on deploying and configuring Audit Collection Services.

- Deploying ACS and ACS Reporting

Installing Audit Collection Services for UNIX/Linux

ACS for UNIX and Linux must be installed on each Management Server that manages UNIX or Linux computers. Complete this procedure for each required management server.

1. From a command prompt or the **Run** menu, launch **Services.msc**. Find the **System Center Audit Forwarding** service, and set the service start to **Automatic**. Start the service.
2. From the Operations Manager setup splash screen, select **Audit Collection Services for UNIX/Linux** from the **Optional Installations** section.
3. On the first page of the ACS for UNIX/Linux setup wizard, click **Next**.
4. Accept the terms of service, and then click **Next**.
5. Select **Audit Data Time Zone**, and then click **Next**.
6. On the Ready page, click **Install**.
7. On the ACS Audit Events page, click **Next**.
8. Click **Finish**.

Note

By default, events cannot be written directly to the Windows Security Event log. During installation, a local group policy is modified to allow the Cross Platform Audit Collection Services module to write to the Windows Security Event log.

The policy is found at **Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Audit Policy -> Audit object access {Success, Failure}**. If group policy is overriding the local policy, it may be necessary to modify this group policy setting on the domain.

Importing UNIX and Linux ACS Management Packs

Audit Collection Services Management Packs for each required UNIX or Linux operating system must be imported for UNIX/Linux ACS event collection. To import UNIX and Linux ACS Management Packs, follow this procedure:

1. In the **Operations** console, click the **Administration** node.
2. Right-click **Management Packs**, and then click **Import Management Packs**.
3. In the Import Management Packs Wizard, select **Add**.
4. Select **Add from Disk**.

5. Browse to the **\ManagementPacks** folder of the Operations Manager installation media.
6. Select ACS management packs appropriate for the UNIX-based and Linux-based computers you are monitoring. The ACS management packs have file names that begin with: **Microsoft.ACS**.
7. Select **Open**.
8. Select **Install** to start the import process.
9. When the import is complete, click **Close**.

Installing ACS Reports for UNIX/Linux

1. Log on to the server that will be used to host ACS reporting as a user that is an administrator of the SSRS instance.
2. Create a temporary folder, such as **C:\acs**.
3. From a server with Audit Collection Services for UNIX/Linux installed, copy the ACS reports to your temporary folder. The ACS reports can be found in the Program Files directory. For example: **C:\Program Files\System Center Operations Manager Cross Platform ACS\Cross Platform Audit Repo**rts.
4. Open a Command Prompt window by using the **Run as Administrator** option, and then change directories to the temporary **acs** folder.
5. Run the following command.

```
UploadCrossPlatformAuditReports "<AuditDBServer\Instance>"
"<Reporting Server URL>" "<path of the copied ACS folder>"
```

For example:

```
UploadCrossPlatformAuditReports "myAuditDbServer\Instance1"
"http://myReportServer/ReportServer$instance1" "C:\acs"
```

How to Enable Audit Collection Services for UNIX/Linux

After Audit Collection Services for UNIX/Linux has been installed, it must be enabled in order for events to be collected.

1. In the Operations Console, click **Authoring**.
2. Click **Object Discoveries**.
3. Search for **ACS**.
4. Right-click **Discover UNIX/Linux ACS Endpoint**.
5. Select **Overrides -> Override the Object Discovery -> For all objects of class -> UNIX/Linux Computer**.

   Note
   As an alternative to enabling for all UNIX/Linux Computers, you can select individual computers and groups.
6. Select the **Enabled** check box.
7. In the Enabled Value list, select **True**.
8. In the **Management Pack** list, verify that the custom override management pack you created is selected.

9. Click **OK**.

See Also

Deploying ACS and ACS Reporting

Collecting Security Events Using Audit Collection Services in Operations Manager

Using SQL Server 2012 Always On Availability Groups with System Center 2012 SP1 - Operations Manager

System Center 2012 Service Pack 1 (SP1), Operations Manager supports SQL Server 2012 AlwaysOn functionality.

The procedures explained here are not intended to provide detailed instructions on how to configure a SQL 2012 AlwaysOn Availability Group, but instead provide tasks that need to be exercised in order for Operations Manager to work effectively when using availability groups, and also emphasizes specific SQL Server AlwaysOn functionality that SP1 supports.

For more information on SQL Server 2012 AlwaysOn Availability Groups, see AlwaysOn Availability Groups (SQL Server). A Word document describing SQL Server 2012 AlwaysOn Multisite Failover Cluster Instances can be found at SQL Server 2012 AlwaysOn: Multisite Failover Cluster Instance.

Important

We do not support a topology where the reporting FCI (the instance hosting the reporting services database only) is configured as part of the AlwaysOn Availability Group.

Note

Operations Manager does not support setting the MultiSubnetFailover parameter. This parameter is not used in Operations Manager connection strings.

SQL 2012 AlwaysOn supported Operations Manager databases

SQL 2012 AlwaysOn supports the following Operations Manager databases.

- Operations Manager Operational database
- Operations Manager Data Warehouse
- Operations Manager Audit Collection Services (ACS) database

Important

For the Operations Manager Data Warehouse and the Operations Manager Audit Collection Services (ACS) database, see the procedures in How to Move the Data Warehouse Database, but replace the new SQL server in the procedure with the <name,port> of the Availability group listener.

Note

A common deployment pattern prescribes using separate SQL Server instances for the Operations Manager, Operations Manager Data Warehouse, and Operations Manager ACS databases. If you are using this pattern, then ensure that all SQL Server instances are added to the availability group.

New Management Group Installation

Use the following series of tasks when installing a new management group with a SQL 2012 AlwaysOn Availability Group.

Before Installing Operations Manager on an availability group

1. Make sure to use the Group listener Name and port when installing Operations Manager for the databases that are going to be added to the availability databases.
2. The first management server will use the Group listener to get the primary SQL instance, and will install the databases on that instance.

After installing the first management server

1. Ensure that the recovery model of the database is full: open SQL Server Management Studio and connect to the instance where the database(s) are installed. Right click on the targeted database, and select its **properties** and select **Options**. If the recovery model is not listed as “Full”, select **Full** from the drop down list.
2. Make a full back up the databases.
3. Use SQL Server Management Studio to add the databases to the availability databases. Notice that when adding the databases to the availability databases under **Select Data Synchronization**, three choice are possible: **Full**, **Join only** and **Skip initial data synchronization**. Choose the option that is most appropriate for you. We recommend selecting **Full** and allowing the **Add Database wizard** create a full backup and restore of the databases on the secondary replicas. More steps might or might not be needed depending on which choice you made. See Manually Prepare a Secondary Database for an Availability Group (SQL Server) for more information.
4. On the new server hosting the operational database, expand **Security**, then expand **Logins**, and add the data writer account name. For more information on how to create a SQL Server login, see Create a Login.
5. Under **Logins**, add the action account.
6. Under **Logins**, add the Data Access Service (DAS) computer account, using the form “**domain\computername$**”.
7. For the DAS computer account, add the following user mappings:
    a. ConfigService
    b. db_accessadmin
    c. db_datareader
    d. db_datawriter
    e. db_ddladmin
    f. db_securityadmin

g. sdk_users
h. sql_dependency_subscriber

8. On the new server hosting the data warehouse database, expand **Security**, then expand **Logins**, and then add the data writer account. For more information on how to create a SQL Server login, see Create a Login.
9. Under **Logins**, add the data reader account.
10. Under **Logins**, add the Data Access Service computer account, using the form "**domain\computername$**".
11. For the DAS computer account, add the following user mappings:
    a. db_datareader
    b. OpsMgrReader
    c. apm_datareader

Known Issues

When you open the Operations Manager console after failing from one node to the other you might encounter the following issue:

Execution of user code in the .NET Framework is disabled. Enable "clr enabled" configuration option. Could not use view or function 'dbo.fn_ModuleTypeView' because of binding errors.

To resolve this issue, please run the following SQL command on the database of the new primary replica SQL instance.

```
sp_configure 'show advanced options', 1;

GO

RECONFIGURE;

GO

sp_configure 'clr enabled', 1;

GO

RECONFIGURE;

GO
```

Existing Management Group

Use the following series of tasks when using an existing management group with a SQL 2012 AlwaysOn Availability Group.

Tasks to perform with the existing management group

1. Make sure that all SQL machines hosting your Operations Manager databases are part of the availability group replicas, or add them to it if they are not.
2. Open Management Studio on the SQL Machine hosting the Operations Manager

databases, right click on each database that is going to be part of the availability databases, and for each select its **properties** and select **Options** to change the recovery model to **Full** from the drop down list.

3. Note the name and the port of the availability group listner.
4. On each management server run `regedit` from an elevated CMD, then edit HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\System Center\2010\Common\Database.

   Change the DatabaseServerName to <AvailabilityGroupListnerName,portNumber>
5. On each management server, edit the following file:

   %ProgramFiles%\System Center 2012\Operations Manager\Server\ConfigService.config

   In the <Category> tag named “Cmdb”, change the value for **ServerName** to the name of the availability group listener and change the **PortNumber** to the availability group listener port.
6. Update the Operations Manager database with the group listener name and port by following these steps:
   a. Open SQL Server Management Studio.
   b. Expand Databases, Operations Manager, and Tables.
   c. Right-click dbo. MT_Microsoft$SystemCenter$ManagementGroup, and then click **Edit Top 200 Rows**.
   d. Change the value in the SQLServerName_<GUID> column to reflect the <name,port> of the availability group listner.
   e. Save the change.
7. Update the Operations Manager database with the availability group listener to specify the location of the application performance monitoring tables.
   a. Open SQL Server Management Studio.
   b. Expand Databases, Operations Manager, and Tables.
   c. Right-click dbo. MT_Microsoft$SystemCenter$OpsMgrDB$AppMonitoring, and then click **Edit Top 200 Rows**.
   d. Change the value in the MainDatabaseServerName_<GUID> column to reflect <name,port> of the availability group listener and its port.
   e. Save the change.
8. Right click each database, and under **Task** select **Back up** (Full Back up).
9. Navigate to the **Availability Group** node and expand it. Right click **Availability database**, and select **Add database**.

   On the Select Initial Data Synchronization page, select a data synchronization preference. We recommend selecting **Full**. Full data synchronization has the benefit of creating a full backup and restore of the databases on the secondary replicas.

   At the end of this task all databases will be added to the availability database, and restored on all availability replica nodes.
10. Use SQL Server Management Studio to add the databases to the availability databases. Notice that when adding the databases to the availability databases under **Select Data**

Synchronization, three choice are possible: **Full**, **Join only** and **Skip initial data synchronization**. Choose the option that is most appropriate for you. We recommend selecting **Full** and allowing the **Add Database wizard** create a full backup and restore of the databases on the secondary replicas. More steps might or might not be needed depending on which choice you made. See Manually Prepare a Secondary Database for an Availability Group (SQL Server) for more information.

11. For each of the secondary replicas, open **build_mom_db_admin.sql** in notepad. The file is located under <installationMedisFolder>\Setup\AMD64). Then search for the MOMv3 messages section. Copy this section into SQL Server Management Studio, starting and running a new query.

How to Upgrade from the Evaluation Version of Operations Manager

The System Center 2012 – Operations Manager evaluation version expires 180 days after you install it.

To upgrade from an evaluation version of Operations Manager to a licensed version, you must obtain a valid product key from Microsoft. For information about Operations Manager licensing, see System Center 2012 Licensing.

Note

To check whether Operations Manager is licensed, in Operations console, click **Help**, and then click **About**. The version is displayed.

To upgrade from the evaluation version of Operations Manager to a licensed version

1. On a management server, click **Start**, click **All Programs**, click **Microsoft System Center 2012**, click **Operations Manager**, and then click **Operations Manager Command Shell**.
2. In the Operations Manager Command Shell, type the following command:

   Set-SCOMLicense <license_key>
3. Restart the System Center Data Access Service. You can use the Microsoft Management Console to restart services.
4. Restart the System Center Data Access Service on all management servers in the management group.

For more information about Set-SCOMLicense, type the following in the Operations Manager Command Shell:

get-help Set-SCOMLicense

For current information about your license, you can use the Get-SCOMLicense cmdlet. For more information, type the following in the Operations Manager Command Shell:

get-help Get-SCOMLicense

Installing Operations Manager by Using the Command Prompt Window

You can install features of Operations Manager by using the **setup.exe** command in the Command Prompt window. Gateway and agent installations require the use of MOMGateway.msi and MOMAgent.msi. You must ensure that all servers meet the minimum supported configuration requirements for System Center 2012 – Operations Manager. For more information, see System Requirements for System Center 2012 - Operations Manager.

Command-line Parameters

The following table lists the command-line parameters for installing features of Operations Manager.

Note

If the parameter contains a colon, a value is required. Otherwise, it is simply a switch.

Parameter	Value
/silent	Does not display the installation wizard.
/install	Runs an installation. Use **/components** to indicate specific features to install.
/InstallPath	Runs an installation specifying an alternative location, to Change the default path for install to another drive. For example: `/InstallPath: "D:\Program Files\System Center Operations Manager 2012"` to change from the default location of drive C.
/components	OMServer: install a management server. OMConsole: install an Operations console. OMWebConsole: install a web console. OMReporting: install a Reporting server.
/ManagementGroupName:	The name of the management group
/ManagementServicePort:	Change the Management Server port on install
/SqlServerInstance:	The SQL server and instance (<server\instance>).
/DatabaseName:	The name of the Operational database.
/DWSqlServerInstance:	The data warehouse server and instance (<server\instance>).
/DWDatabaseName:	The name of the data warehouse database.

Parameter	Value
/UseLocalSystemActionAccount	Used to specify the Local System for the Management server action account.
/ActionAccountUser:	The domain and user name of the Management server action account. Used if you do not want to specify the Local System
/ActionAccountPassword:	The password for the Management server action account. Used if you do not want to specify the Local System.
/UseLocalSystemDASAccount	Used to specify the Local System for the Data Access service account.
/DASAccountUser:	The domain and user name of the Data Access service account. Used if you do not want to specify the Local System.
/DASAccountPassword:	The password for the Data Access service account. Used if you do not want to specify the Local System.
/DataReaderUser:	The domain and user name of the data reader account.
/DataReaderPassword:	The password for the data reader account.
/DataWriterUser:	The domain and user name of the data writer account.
/DataWriterPassword:	The password for the data writer account.
/EnableErrorReporting:	Never: Do not opt in to sending automatic error reports. Queued: Opt in to sending error reports, but queue the reports for review before sending. Always: Opt in to automatically send error reports.
/SendCEIPReports:	0 : Do not opt in to the Customer Experience Improvement Program (CEIP).

Parameter	Value
	1 : Opt in to CEIP.
/UseMicrosoftUpdate:	0 : Do not opt in to Microsoft Update. 1 : Opt in to Microsoft Update.
/AcceptEndUserLicenseAgreement:	0 : Do not accept the End User License Agreement (EULA). 1 : Accept the End User License Agreement (EULA). When performing a clean installation of System Center 2012 SP1 - Operations Manager, this switch is needed for all management servers. It is also needed for other scripted installations.
/ManagementServer	Used to specify the name of the management server associated with a web console and/or Reporting server that is not installed on a management server.
/WebSiteName:	The name of the website. For default web installation, specify "**Default Web Site**". Used for web console installations.
/WebConsoleUseSSL	Specify only if your website has Secure Sockets Layer (SSL) activated. Used for web console installations.
/WebConsoleAuthorizationMode:	Mixed: Used for intranet scenarios. Network: Used for extranet scenarios. Used for web console installations.
/SRSInstance	The reporting server and instance (<server\instance>). Used for Reporting Server installations.
/SendODRReports:	0: Do not opt in to sending operational data reports. 1: opt in to sending operational data reports. Used for Reporting Server Installations.
/uninstall	Uninstalls Operations Manager. Use **/components** to indicate specific features to uninstall. If **/components** is not specified, it will uninstall all features of Operations Manager on

Parameter	Value
	the server.

For examples of command lines for installing the various features of Operations Manager see the following:

- Walkthrough: Installing Operations Manager on a Single Server
- How to Install the First Management Server in a Management Group
- How to Install Additional Management Servers
- How to Install the Operations Console
- How to Install the Operations Manager Web Console
- How to Install the Operations Manager Reporting Server
- How to Deploy a Gateway Server

See Also

Deploying System Center 2012 - Operations Manager

How to Enable High Availability for the Data Access Service

By default if your Operations Manager Operations console is connected to the Data Access service of one management server and the connection fails, it does not automatically failover to another management server in your management group. To enable high availability for your Operations Manager Data Access service, you can use Network Load Balancing (NLB). By configuring NLB, and connecting to the NLB cluster, if the connection fails, it will automatically be redirected to another management server.

To configure NLB

1. First, you must set up a virtual IP address. You must configure a static IP address for all nodes participating in the cluster and set up DNS. For more information, see. Configure a Static IP Address.
2. You must enable NLB on each management server in your management group. For more information, see
   - Installing Network Load Balancing
   - Create a New Network Load Balancing Cluster
   - Add a Host to the Network Load Balancing Cluster

Using a Firewall

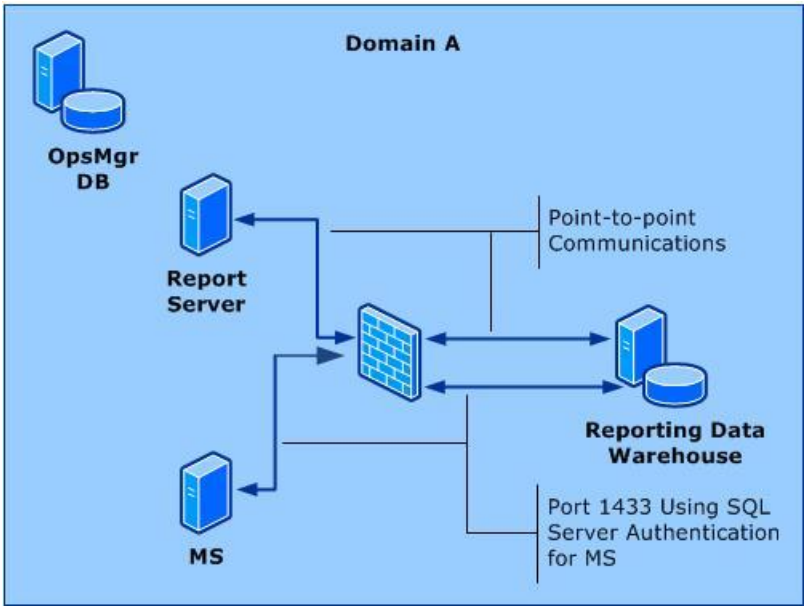
Connecting to the Reporting Data Warehouse Across a Firewall

This section describes how to configure your environment to support the placing of a Report data warehouse behind a firewall.

Note

Separating the Operations console, management server, or Reporting Server by either a firewall or across a trust boundary is not supported.

In an environment where the Reporting data warehouse is separated from the management server and Reporting Server by a firewall, Windows Integrated Authentication cannot be used. You need to take steps to configure SQL Server Authentication. The following sections explain how to enable SQL Server Authentication between the management server (or management server), the Reporting Server, and the Reporting data warehouse, as shown in the following illustration.



Management Server and Reporting Data Warehouse

The following steps are necessary to enable SQL Server Authentication:

1. On the computer hosting the Reporting data warehouse, create a SQL Server Login in the proper role for reader and writer. The credentials you supply for this account must be made a member of the following roles in the data warehouse database on the computer running SQL Server:
   a. OpsMgrWriter
   b. db_owner (only for the owning management group in the database)
2. On the computer hosting the management server, create a Run As Account (of type Simple) with the credentials from the previous step.

3. Associate this Run As Account with the Run As Profile called Data Warehouse SQL Server Authentication Account, targeting this Run As Profile to each management server. For more information, see How to Change the Run As Account Associated with a Run As Profile in this guide.

If there is a firewall between the management server and the Reporting data warehouse, you will have to open port 1433.

Reporting Server and Reporting Data Warehouse

If there is a firewall or trust boundary between the Reporting Server and the Reporting data warehouse, point-to-point communications will need to be established.

The account that was specified as the Data Reader Account during setup of Reporting becomes the Execution Account on Reporting Server, and it is this account that will be used to connect to the Reporting data warehouse.

You should determine what port number the computer running SQL Server on the Reporting data warehouse is using and enter this number into the dbo.MT_DataWarehouse table in the Operations Manager database. See How to Configure the Reporting Data Warehouse to Listen on a Specific TCP/IP Port.

Reporting Server and Management Server Separated by a Firewall

A "Could not verify if current user is in sysadmin Role" error message might display when installing Reporting if the reporting server and the management server are separated by a firewall. This error message might display even if the proper firewall ports have been opened. This error occurs after entering the computer name for the management server and clicking **Next**. This error might also display because Reporting Setup was unable to connect to the operational database on the management server. In this environment you must determine what port number is being used by the computer running SQL Server and configure the Operations Manager database to use the port number. See the topic How to Configure the Operations Manager Database to Listen on a Specific TCP/IP Port.

Port Assignments

The following table shows Operations Manager feature interaction across a firewall, including information about the ports used for communication between the features, which direction to open the inbound port, and whether the port number can be changed.

Operations Manager Feature A	Port Number and Direction	Operations Manager Featuret B	Configurable	Note
management server	1433 --->	Operations Manager database	Yes (Setup)	
management server	5723, 5724 ---	management	No	Port 5724 must be

Operations Manager Feature A	Port Number and Direction	Operations Manager Featuret B	Configurable	Note
	>	server		open to install this feature and can be closed after this feature has been installed.
gateway server	5723 --->	management server	No	
management server	1433 --->	Reporting data warehouse	No	
Reporting server	5723, 5724 --->	management server	No	Port 5724 must be open to install this feature and can be closed after this feature has been installed.
Operations console	5724 --->	management server	No	
Connector framework source	51905 --->	management server	No	
web console server	Web site port --->	management server	No	
web console browser	51908 --->	web console server	Yes (IIS Admin)	Port 51908 is the default port used when selecting Windows Authentication. If you select Forms Authentication, you will need to install an SSL certificate and configure an available port for https functionality for the Operations Manager web console web site.

Operations Manager Feature A	Port Number and Direction	Operations Manager Featuret B	Configurable	Note
connected management server (Local)	5724 --->	connected management server (Connected)	No	
Agent installed using MOMAgent.msi	5723 --->	management server	Yes (Setup)	
Agent installed using MOMAgent.msi	5723 --->	management server	Yes (Setup)	
Agent installed using MOMAgent.msi	5723 --->	gateway server	Yes (Setup)	
gateway server	5723 --->	management server	Yes (Setup)	
Agent (Audit Collection Services forwarder)	51909 --->	management server Audit Collection Services collector	Yes (Registry)	
Agentless Exception Monitoring data from client	51906 --->	management server Agentless Exception Monitoring file share	Yes (Client Monitoring Wizard)	
Customer Experience Improvement Program data from client	51907 --->	management server (Customer Experience Improvement Program End) Point	Yes (Client Monitoring Wizard)	
Operations console (reports)	80 --->	SQL Reporting Services	No	The Operations console uses Port 80 to connect to the SQL Reporting Services web site.

Operations Manager Feature A	Port Number and Direction	Operations Manager Featuret B	Configurable	Note
Reporting server	1433 --->	Reporting data warehouse	Yes	
management server (Audit Collection Services collector)	1433 --->	Audit Collection Services database	Yes	

How to Configure the Operations Manager Database to Listen on a Specific TCP/IP Port

Perform the following steps to configure a static port for the operational database:

- Use the SQL Server Configuration Manager to disable dynamic port addressing, specify a static port, disable and stop the SQL Server Browser service, and then restart the SQL Server <*Instance*> service.
- Edit the dbo.MT_ManagementGroup table with the static port number.
- Edit the registry to configure the static port number on the management server.

Caution
Incorrectly editing the registry can severely damage your system. Before making changes to the registry, you should back up any important data.

To configure the operational database port number

1. Log on to the computer hosting the operational database.
2. On the Windows desktop, click **Start**, point to **Programs**, point to the appropriate offering of Microsoft SQL Server, point to **Configuration Tools**, and then click **SQL Server Configuration Manager**.
3. In the **SQL Server Configuration Manager** dialog box, expand **SQL Server Network Configuration**, and then click **Protocols for <INSTANCE>**.
4. In the results pane, right-click **TCP/IP**, and then click **Properties**.
5. In the **TCP/IP Properties** dialog box, click the **IP Addresses** tab.
6. Several IP addresses appear in the format **IP1**, **IP2**, up to **IPAll**. One of these is for the IP address of the loopback adapter, 127.0.0.1. Additional IP addresses appear for each IP address on the computer. Expand **IP1**, **IP2**, up to **IPAll**.
7. For the **IP***n* areas, if the **TCP Dynamic Ports** dialog box contains a **0**, indicating the Database Engine is listening on dynamic ports, delete the **0**.
8. In the **IPAll** area, if the **TCP Dynamic Ports** dialog box contains a port number (which indicates the dynamic port number that was assigned), delete the port number.
9. In the **IPAll** area, in the **TCP Port** dialog box, enter the static port number you want to

use, and then click **OK**.

10. In the **SQL Server Configuration Manager** dialog box, click **SQL Server Services**.
11. In the **SQL Server Configuration Manager** results pane, right-click **SQL Server Browser**, and select **Properties**.
12. In the **SQL Server Browser Properties** dialog box, click the **Service** tab.
13. In the Service tab, click **Start Mode**. In the **Start Mode** list, click **Disabled**, and then click **OK**.
14. In the SQL Server Configuration Manager results pane, right-click **SQL Server Browser**, and then click **Stop**.
15. In the results pane, right-click **SQL Server (<instance name>)**, and then click **Restart**.
16. Close the **SQL Server Configuration Manager**.

To enter the SQL Server port number into the dbo.MT_ManagementGroup table

1. On the computer hosting the operational database, on the Windows desktop, click **Start**, point to **Programs**, point to **Microsoft SQL Server 2008**, and then click **SQL Server Management Studio**.
2. In the **Connect to Server** dialog box, in the **Server type** list, select **Database Engine**.
3. In the **Server name** list, type the server name, instance, and port number for your operational database (for example, computer\<instance>).
4. In the **Authentication** list, select **Windows Authentication**, and then click **Connect**.
5. In the Object Explorer pane, expand **Databases**, expand the operational database (for example, **OperationsManager**), expand **Tables**, right-click **dbo.MT_ManagementGroup**, and then click **Open Table**.
6. In the results pane, scroll to the right to the column titled **SQLServerName_<guid>**.
7. In the first row, enter computer\<instance> followed by a comma, a space, and then the SQL Server port number (for example, **computer\INSTANCE1, <port>**).
8. Click **File**, and then click **Exit**.

To edit the registry on the management server

1. Log on to the computer hosting the management server.
2. On the Windows desktop, click **Start**, click **Run**, type **regedit**, and then click **OK**.
3. On the **Registry Editor** page, expand **HKEY_LOCAL_MACHINE**, expand **SOFTWARE**, expand **Microsoft**, expand **Microsoft Operations Manager**, expand **3.0**, and then click **Setup**.
4. In the results pane, right-click **DatabaseServerName**, and then click **Modify**.
5. In the **Edit String** dialog box, in the Value data text box, append the database server name entry with a comma and a space, and then type the port number. For example, **<comuter_name>\<instance>, <port number>**.
6. Click **OK**.

How to Configure the Reporting Data Warehouse to Listen on a Specific TCP/IP Port

Perform the following procedures to configure a static port for the Reporting data warehouse:

- Use the SQL Server Configuration Manager to disable dynamic port addressing, specify a static port, disable and stop the SQL Server Browser service, and then restart the SQL Server <*Instance*> service.
- Edit the dbo.MT_ManagementGroup table with the static port number.
- Edit the dbo.MemberDatabase table with the static port number.
- Edit the registry to configure the static port number on the management server.

  Caution
  Incorrectly editing the registry can severely damage your system. Before making changes to the registry, you should back up any important data.
- Edit the SQL Server Reporting Services settings.

To configure the Operations Manager database port number

1. Log on the computer hosting the Reporting data warehouse.
2. On the Windows desktop, click **Start**, point to **Programs**, point to **Microsoft SQL Server 2008**, point to **Configuration Tools**, and then click **SQL Server Configuration Manager**.
3. In the **SQL Server Configuration Manager** dialog box, expand **SQL Server 2008 Network Configuration**, and then click **Protocols for <INSTANCE>**.
4. In the results pane, right-click **TCP/IP**, and then click **Properties**.
5. In the **TCP/IP Properties** dialog box, click the **IP Addresses** tab.
6. Several IP addresses appear in the format **IP1**, **IP2**, up to **IPAll**. One of these is for the IP address of the loopback adapter, 127.0.0.1. Additional IP addresses appear for each IP Address on the computer. Expand **IP1**, **IP2**, up to **IPAll**.
7. For the **IP***n* areas, if the **TCP Dynamic Ports** dialog box contains a **0**, indicating the Database Engine is listening on dynamic ports, delete the **0**.
8. In the **IPAll** area, if the **TCP Dynamic Ports** box contains a port number (which indicates the dynamic port number that was assigned) delete the port number.
9. In the **IPAll** area, in the **TCP Port** dialog box, enter the static port number you want to use, and then click **OK**.
10. In the **SQL Server Configuration Manager** dialog box, click **SQL Server 2008 Services**.
11. In the **SQL Server Configuration Manager** results pane, right-click **SQL Server Browser** and select **Properties**.
12. In the **SQL Server Browser Properties** dialog box, click the **Service** tab.
13. On the Service tab, click **Start Mode**. In the **Start Mode** list, click **Disabled**, and then click **OK**.
14. In the SQL Server Configuration Manager results pane, right-click **SQL Server Browser**,

and then click **Stop**.

15. In the results pane, right-click **SQL Server (<instance name>)** and then click **Restart**.
16. Close the **SQL Server Configuration Manager**.

To enter the SQL Server port number into the dbo.MT_ManagementGroup table

1. On the computer hosting the operational database, on the Windows desktop, click **Start**, point to **Programs**, point to **Microsoft SQL Server 2008**, and then click **SQL Server Management Studio**.
2. In the **Connect to Server** dialog box, in the **Server type** list, select **Database Engine**.
3. In the **Server name** list, type the server and instance for your operational database (for example, computer\INSTANCE1).
4. In the **Authentication** list, select **Windows Authentication**, and then click **Connect**.
5. In the Object Explorer pane, expand **Databases**, expand **OperationsManager** (or the name of the operational database if the default name was not used), expand **Tables**, right-click **dbo.MT_DataWarehouse**, and then click **Open Table**.
6. In the results pane, scroll to the right to the column titled **MainDatabaseServerName_<guid>**.
7. In the first row, enter computer\<instance> followed by a comma, a space, and then the SQL Server port number (for example, **computer\<instance>, <port>**).
8. Click **File**, and then click **Exit**.

To enter the SQL Server port number into the dbo.MemberDatabase table

1. On the computer hosting the Reporting data warehouse, on the Windows desktop, click **Start**, point to **Programs**, point to **Microsoft SQL Server 2008**, and then click **SQL Server Management Studio**.
2. In the **Connect to Server** dialog box, in the **Server type** list, select **Database Engine**.
3. In the **Server name** list, type the server and instance for your operational database (for example, **computer\<instance>**).
4. In the **Authentication** list, select **Windows Authentication**, and then click **Connect**.
5. In the Object Explorer pane, expand **Databases**, expand **OperationsManagerDW** (or the name of the data warehouse if you did not use the default name), expand **Tables**, right-click **dbo.MemberDatabase**, and then click **Open Table**.
6. In the results pane, scroll to the right to the column titled **ServerName**.
7. In the first row, enter computer\<instance> followed by a comma, a space, and then the SQL Server port number (for example, **computer\<instance>, <port>**).
8. Click **File**, and then click **Exit**.

To edit the registry on the Reporting Server

1. Log on to the computer hosting the management server.
2. On the Windows desktop, click **Start**, click **Run**, type **regedit**, and then click **OK**.

3. On the **Registry Editor** page, expand **HKEY_LOCAL_MACHINE**, expand **SOFTWARE**, expand **Microsoft**, expand **Microsoft Operations Manager**, expand **3.0**, and then click **Reporting**.
4. In the results pane, right-click **DWDBInstance**, and then click **Modify**.
5. In the **Edit String** dialog box, in the Value data text box, append the database server name entry with a comma and a space, and then type the port number. For example, **<comuter_name>\<instance>, <port number>**.
6. Click **OK**.

To edit SQL Server Reporting Services

1. Log on to the computer hosting the management server.
2. Start Internet Explorer and connect to http://<computer name>/reports$<instance name>.
3. Click the **Contents** tab.
4. On the right side of the toolbar, click **Show Details**.
5. Click **Data Warehouse Main**.
6. In the **Connection string** text box, locate the line that reads **source=<computer>\<instance>;initial**.
7. Append the instance name with a comma and a space, and then type the static port number. For example, **source=<computer>\<instance>, <port>;initial**.
8. Click **Apply**, and then close the browser.

Upgrading to System Center 2012 - Operations Manager

This section of the Deployment Guide provides information about how to upgrade to System Center 2012 – Operations Manager from System Center Operations Manager 2007 R2.

If you are upgrading from System Center 2012 – Operations Manager to System Center 2012 Service Pack 1 (SP1), Operations Manager, see the procedures for SP1 in Upgrading System Center 2012 – Operations Manager to System Center 2012 SP1

Important
This is the only supported upgrade path to System Center 2012 – Operations Manager. If you are using another, you must first upgrade to System Center Operations Manager 2007 R2.

See Also

Upgrading from System Center Operations Manager 2007 R2

Upgrading from System Center Operations Manager 2007 R2

This section of the Deployment Guide provides information about how to upgrade from System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager. This section of the guide is not intended to be read in order, from start to finish, because your upgrade path will depend on your current configurations. You should use the Upgrade Process Flow Diagrams or Upgrade Path Checklists for Operations Manager to help guide you through the upgrade process.

Upgrading to System Center 2012 – Operations Manager is supported from Operations Manager 2007 R2 CU4, or from the latest available CU. Before you begin the upgrade process, make sure that all the servers in the management group meet the minimum supported configurations for System Center 2012 – Operations Manager. For more information, see Supported Configurations for System Center 2012 – Operations Manager. If a server does not meet the minimum supported configurations, you might have to introduce new servers into your management group before you upgrade. For more information, see Upgrading Hardware and Software to Meet System Requirements.

When you run upgrade on an Operations Manager 2007 R2 management group, the Upgrade wizard automatically detects the Operations Manager 2007 R2 features that are installed, and it lists the features that will be upgraded. For example, on an Operations Manager 2007 R2 single-server management group with all the features installed, the Upgrade wizard lists the operational database, management server, data warehouse, operations console, web console, and reporting. The System Center 2012 – Operations Manager Upgrade wizard performs system prerequisite checks and provides resolution steps for any issues. Installation will not continue until you resolve all issues. If any of the mandatory Operations Manager features were not previously installed in the Operations Manager 2007 R2 management group, such as the data warehouse, the Upgrade wizard automatically detects the feature and adds it to the list of features to be added during the upgrade process.

In System Center 2012 – Operations Manager, all management servers are peers; there is no root management server (RMS). Therefore, the RMS is no longer a single point of failure as all management servers host the services previously hosted only by the RMS. Roles are distributed to all the management servers. If one management server becomes unavailable, its responsibilities are automatically redistributed.

If you are upgrading a distributed management group, you must upgrade certain features, such as the secondary management servers, gateways, and agents before you upgrade the management group. You run the management group upgrade from the server that hosts the RMS, unless it does not meet the minimum supported configurations for System Center 2012 – Operations Manager. For example, if the RMS is installed on a 32-bit operating system or if it is a clustered RMS, you cannot run upgrade from the RMS. Instead, you must upgrade the management group from a secondary management server. If you follow this upgrade path, this secondary management server is marked as the RMS emulator, and the unsupported RMS is removed from the management group. The RMS emulator enables legacy management packs that rely on the RMS to continue to function in System Center 2012 – Operations Manager. For

more information about the supported configurations for System Center 2012 – Operations Manager, see Supported Configurations for System Center 2012 – Operations Manager.

Note

If you upgrade from the secondary management server, you can build a new management server with the same Windows computer name as the old RMS, rather than change the configuration settings to point to the new management server.

There are four upgrade paths. The path you choose depends on your current topology and system configurations. The following table describes the upgrade paths in more detail.

Upgrade Paths	Description
Single-server Upgrade (Simple)	Use this upgrade path when you have an Operations Manager 2007 R2 management group where all features are installed on the same server, and the hardware and software meets the minimum supported configuration for System Center 2012 – Operations Manager.
Single-server Upgrade (Complex)	Use this upgrade path when you have an Operations Manager 2007 R2 management group where all features are installed on the same server, and the hardware and software do not meet the minimum supported configuration for System Center 2012 – Operations Manager. If the operating system on the server is 32-bit, a new, 64-bit server is required.
Distributed Upgrade (Simple)	Use this path when you have an Operations Manager 2007 R2 management group where various features are installed on separate servers, all of which meet the minimum supported configurations for System Center 2012 – Operations Manager.
Distributed Upgrade (Complex)	Use this path when you have an Operations Manager 2007 R2 management group where various features are installed on separate servers, and where one or more servers do not meet the minimum supported configuration for System Center 2012 – Operations Manager. For example, if the RMS is clustered, you must follow this path. If the operating system on any of the server is 32-bit, new 64-bit replacement

Upgrade Paths	Description
	servers are required.

This guide also contains the specific pre-upgrade and post-upgrade procedures and checklists to help you through the upgrade process. The following content will help you upgrade to System Center 2012 – Operations Manager.

- Upgrade Path Checklists for Operations Manager
- Upgrading Hardware and Software to Meet System Requirements
- Pre-Upgrade Tasks for Operations Manager
- Upgrade Tasks for Operations Manager
- Improving Upgrade Performance
- Upgrading a Single-Server Operations Manager 2007 R2 Environment
- Upgrading a Distributed Operations Manager 2007 R2 Environment
- Post-Upgrade Tasks when Upgrading from Operations Manager 2007 R2

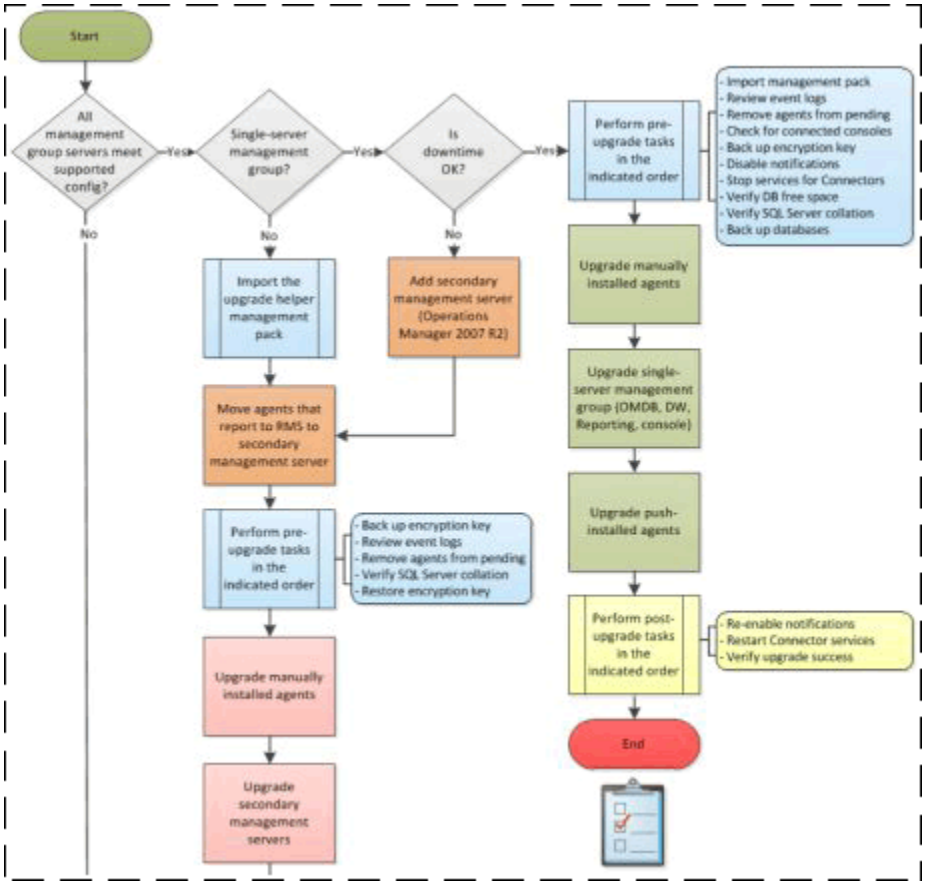
See Also

Upgrading to System Center 2012 - Operations Manager

Upgrade Process Flow Diagrams

Before you upgrade to System Center 2012 – Operations Manager, you must first determine whether all servers in your System Center Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. For more information, see Supported Configurations for System Center 2012 – Operations Manager. You can use a set of process flow diagrams to determine your upgrade path and visualize the process.

Upgrade process flow diagram



Note

You can click the appropriate process box to open and review the content for any step in the process.

The following table lists the process flow diagrams available, along with a description of when each upgrade path should be used.

Condition	Process flow diagram
When you have a single-server or distributed management group that already meets the minimum supported configuration requirements for System Center 2012 – Operations Manager.	Single-Server and Distributed Upgrade (Simple) Process Flow Diagram
When your single-server management group does not yet meet the minimum supported configuration requirements for System Center 2012 – Operations Manager, and requires new hardware.	Single-Server Upgrade (Complex) Process Flow Diagram

Condition	Process flow diagram
When your distributed management group has one or more servers that do not meet the minimum supported configuration requirements for System Center 2012 – Operations Manager, and might require new hardware.	Distributed Upgrade (Complex) Process Flow Diagram

See Also

Checklist: Single-Server Upgrade (Simple)

Checklist: Single-Server Upgrade (Complex)

Checklist: Distributed Upgrade (Simple)

Checklist: Distributed Upgrade (Complex)

Upgrade Path Checklists for Operations Manager

Use the following checklists to help guide you through an upgrade of System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager. In the table, use the list of conditions to identify the checklist that matches your upgrade path. Essentially, the “simple” path is used when your Operations Manager 2007 R2 management group already meets the supported configuration requirements for System Center 2012 – Operations Manager. The “complex” path is used when your Operations Manager 2007 R2 management group does not yet meet the supported configuration requirements for System Center 2012 – Operations Manager.

Important

Before you follow any of these procedures, make sure that you have verified that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you will need to add any new servers to your management group prior to upgrading. For more information, see Supported Configurations for System Center 2012 – Operations Manager.

Condition	Upgrade Path Checklist
Your Operations Manager 2007 R2 single-server management group already meets the minimum supported configuration requirements for System Center 2012 – Operations Manager.	Checklist: Single-Server Upgrade (Simple)
Your Operations Manager 2007 R2 single-server management group does not meet the minimum supported configuration requirements for System Center 2012 – Operations Manager	Checklist: Single-Server Upgrade (Complex)

Condition	Upgrade Path Checklist
and requires new hardware.	
Your Operations Manager 2007 R2 distributed management group already meets the minimum supported configuration requirements System Center 2012 – Operations Manager.	Checklist: Distributed Upgrade (Simple)
Your Operations Manager 2007 R2 distributed management group has one or more servers that do not meet the minimum supported configuration requirements for System Center 2012 – Operations Manager and might require new hardware.	Checklist: Distributed Upgrade (Complex)

See Also

Single-Server and Distributed Upgrade (Simple) Process Flow Diagram

Single-Server Upgrade (Complex) Process Flow Diagram

Distributed Upgrade (Complex) Process Flow Diagram

Checklist: Single-Server Upgrade (Simple)

This checklist walks you through an upgrade of a System Center Operations Manager 2007 R2 single-server management group that already meets the minimum supported configurations for Operations Manager. For more information, see Supported Configurations for System Center 2012 – Operations Manager.

If your single-server management group does not yet meet the minimum supported configurations for System Center 2012 – Operations Manager, or if you have a distributed management group, see the following checklists.

Upgrade Path Checklist	Condition
Checklist: Single-Server Upgrade (Complex)	Your Operations Manager 2007 R2 single-server management group does not meet the minimum supported configurations for System Center 2012 – Operations Manager and requires new hardware.
Checklist: Distributed Upgrade (Simple)	Your Operations Manager 2007 R2 distributed management group already meets the minimum supported configurations for System Center 2012 – Operations Manager.
Checklist: Distributed Upgrade (Complex)	Your Operations Manager 2007 R2 distributed management group has one or more servers

Upgrade Path Checklist	Condition
	that do not meet the minimum supported configurations for System Center 2012 – Operations Manager and might require new hardware.

If you prefer to avoid downtime on your single-server management group, you can add a secondary management server and then follow the distributed management group upgrade process. For more information, see:

- How to Add an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)
- Checklist: Distributed Upgrade (Simple)

Checklist

Use the following checklist to upgrade your single-server management group if it already meets the supported configuration requirements for System Center 2012 – Operations Manager

Tip
You can also view a process flow diagram that links to the relevant topics. For more information, see Single-Server and Distributed Upgrade (Simple) Process Flow Diagram

	Task	References
☐	Import the Upgrade Helper management pack.	Import the Upgrade Helper Management Pack
☐	Review the Operations Manager 2007 R2 event logs.	Review the Operations Manager 2007 R2 Event Logs
☐	Remove agents from Pending Management.	Remove Agents from Pending Management
☐	Check for any active connected consoles to the root management server.	Check the Operations Manager 2007 R2 RMS for Active Connected Consoles
☐	Back up the RMS encryption key (SecureStorageBackup.exe).	Back Up the RMS Encryption Key
☐	Disable all notification subscriptions.	Disable Notification Subscriptions
☐	Stop services or disable any connectors that are installed.	Stop Services for Connectors
☐	Verify that your operational database has enough free space.	Verify that the Operational Database Has More than 50

	Task	References
		Percent of Free Space
☐	Verify that you have a supported SQL Server collation on all databases and instances of databases.	Verify the SQL Server Collation
☐	Back up the databases.	Back up the Operations Manager Databases
☐	Upgrade the manually installed agents.	Upgrading Manually Installed Agents
☐	Run the management group upgrade on the root management server.	How to Upgrade an Operations Manager 2007 R2 Single-Server Management Group
☐	Upgrade the push-installed agents.	Upgrading Push-Installed Agents
☐	Re-enable the notification subscriptions.	Re-enable the Notification Subscriptions.
☐	Restart or re-enable the service for any connectors that are installed.	Restart the Connector Services
☐	Update overrides.	Update Overrides
☐	Verify the success of the upgrade.	Verify upgrade success

See Also

Upgrade Path Checklists for Operations Manager

Single-Server and Distributed Upgrade (Simple)

Checklist: Single-Server Upgrade (Complex)

This checklist walks you through an upgrade of a System Center Operations Manager 2007 R2 single-server management group that does not meet the supported configuration requirements for System Center 2012 – Operations Manager, and requires new hardware. For more information, see Supported Configurations for System Center 2012 – Operations Manager.

If your single-server management group already meets the minimum supported configurations for System Center 2012 – Operations Manager, or if you have a distributed management group, see the following checklists.

Upgrade Path Checklist	Condition
Checklist: Single-Server Upgrade (Simple)	Your Operations Manager 2007 R2 single-server management group already meets the minimum supported configurations for System Center 2012 – Operations Manager.
Checklist: Distributed Upgrade (Simple)	Your Operations Manager 2007 R2 distributed management group already meets the minimum supported configurations for System Center 2012 – Operations Manager.
Checklist: Distributed Upgrade (Complex)	Your Operations Manager 2007 R2 distributed management group has one or more servers that do not meet the minimum supported configurations for System Center 2012 – Operations Manager and might require new hardware.

Checklist

Use the following checklist to upgrade your single-server management group if it does not yet meet the supported configuration requirements for System Center 2012 – Operations Manager.

Tip

You can also view a process flow diagram that links to the relevant topics. For more information, see Single-Server Upgrade (Complex)

	Task	References
☐	Add a secondary management server and install System Center Operations Manager 2007 R2.	How to Add an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)
☐	Move agents that report to the root management (RMS) server to the secondary management server.	How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)
☐	If SQL Server does not meet the supported configuration requirements, upgrade SQL Server.	Upgrading SQL Server (Operations Manager Upgrade)
☐	Back up the encryption key.	Back Up the Encryption Key

	Task	References
☐	Review the Operations Manager 2007 R2 event logs.	Review the Operations Manager 2007 R2 Event Logs
☐	Remove agents from Pending Management.	Remove Agents from Pending Management
☐	Verify that you have a supported SQL Server collation on all databases and instances of databases.	Verify the SQL Collation
☐	Upgrade the manually installed agents.	Upgrading Manually Installed Agents
☐	Upgrade the secondary management server.	How to Upgrade a Secondary Management Server from Operations Manager 2007 R2
☐	Upgrade the push-installed agents.	Upgrading Push-Installed Agents
☐	Check for any active connected consoles to the root management server.	Check the Operations Manager 2007 R2 RMS for Active Connected Consoles
☐	Disable all notification subscriptions.	Disable the Notification Subscriptions
☐	Stop services or disable any connectors that are installed.	Stop the Services for Connectors
☐	Verify that your operational database has enough free space.	Verify that the Operational Database Has More than 50 Percent of Free Space
☐	Back up the databases.	Back Up the Operations Manager Databases
☐	Restore the encryption key on secondary management server.	Restore the Encryption Key on the Secondary Management Server
☐	Run management group upgrade on the secondary management server.	How to Upgrade a Management Group from an Operations Manager 2007 R2 Secondary Management Server
☐	Re-enable the notification	Re-enable the Notification

	Task	References
	subscriptions.	Subscriptions.
☐	Restart or re-enable the service for any connectors that are installed.	Restart the Connector Services
☐	Uninstall the old root management server.	Uninstall the Old RMS
☐	Update overrides.	Update Overrides
☐	Verify the success of the upgrade.	Verify the Upgrade Success

See Also

Upgrade Path Checklists for Operations Manager

Single-Server Upgrade (Complex)

Checklist: Distributed Upgrade (Simple)

This checklist walks you through an upgrade of a System Center Operations Manager 2007 R2 distributed management group that meets the supported configuration requirements for System Center 2012 – Operations Manager. For more information, see Supported Configurations for System Center 2012 – Operations Manager.

If your distributed management group does not yet meet the minimum supported configurations for System Center 2012 – Operations Manager, or if you have a single-server management group, see the following checklists.

Upgrade Path Checklist	Condition
Checklist: Single-Server Upgrade (Simple)	Your Operations Manager 2007 R2 single-server management group already meets the minimum supported configurations for System Center 2012 – Operations Manager.
Checklist: Single-Server Upgrade (Complex)	Your Operations Manager 2007 R2 single-server management group does not meet the minimum supported configurations for System Center 2012 – Operations Manager and requires new hardware.
Checklist: Distributed Upgrade (Complex)	Your Operations Manager 2007 R2 distributed management group has one or more servers that do not meet the minimum supported configurations for System Center 2012 –

Upgrade Path Checklist	Condition
	Operations Manager and might require new hardware.

Checklist

Use the following checklist to upgrade your distributed management group if it already meets the supported configuration requirements for System Center 2012 – Operations Manager.

Tip

You can also view a process flow diagram that links to the relevant topics. For more information, see Single-Server and Distributed Updated (Simple).

Note

In this checklist, we recommend that you move agents that report to the root management server (RMS) to a secondary management server before upgrading the agents. However, if you do not mind experiencing downtime, you can upgrade the agents after you upgrade the management group instead of moving them to a secondary management server.

	Task	References
☐	Import the Upgrade Helper management pack.	Import the Upgrade Helper Management Pack
☐	Move agents that report to the RMS to a secondary management server.	How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)
☐	Back up the encryption key.	Back Up the Encryption Key
☐	Review the Operations Manager 2007 R2 event logs.	Review the Operations Manager 2007 R2 Event Logs
☐	Remove agents from pending management.	Remove Agents from Pending Management
☐	Verify that you have a supported SQL Server collation on all databases and instances of databases.	Verify the SQL Collation
☐	Upgrade the manually installed agents.	Upgrading Manually Installed Agents
☐	Upgrade the secondary	How to Upgrade a Secondary

	Task	References
	management servers.	Management Server from Operations Manager 2007 R2
☐	Upgrade gateways, if present.	How to Upgrade a Gateway Server from Operations Manager 2007 R2
☐	Upgrade the push-installed agents.	Upgrading Push-Installed Agents
☐	Check for any active, connected consoles to the root management server.	Check the Operations Manager 2007 R2 RMS for Active, Connected Consoles
☐	Disable all notification subscriptions.	Disable the Notification Subscriptions
☐	Stop services or disable any connectors that are installed.	Stop the Services for Connectors
☐	Verify that your operational database has enough free space.	Verify that the Operational Database Has More than 50 Percent of Free Space
☐	Back up the databases.	Back Up the Operations Manager Databases
☐	Restore the encryption key on secondary management server.	Restore the Encryption Key on the Secondary Management Server
☐	Run management group upgrade on the root management server.	How to Upgrade a Management Group from an Operations Manager 2007 R2 RMS
☐	Upgrade or install the optional features, such as the web consoles and Reporting server.	Upgrading or Installing Optional Features
☐	Re-enable notification subscriptions.	Re-enable the Notification Subscriptions
☐	Restart or re-enable the service for any connectors that are installed.	Restart the Connector Services
☐	Update overrides.	Update Overrides

	Task	References
☐	Verify the success of the upgrade.	Verify the Upgrade Success

See Also

Upgrade Path Checklists for Operations Manager

Single-Server and Distributed Updated (Simple)

Checklist: Distributed Upgrade (Complex)

To upgrade a distributed System Center Operations Manager 2007 R2 management group to System Center 2012 – Operations Manager, you use a phased approach, starting with the management servers, then the gateway servers, and then the management group. The order in which you upgrade the agents depends on how they were deployed (manually installed or push-installed), and whether your root management server (RMS) meets the supported configuration requirements for System Center 2012 – Operations Manager. For example, a clustered RMS is not supported in System Center 2012 – Operations Manager. You also must perform a number of pre-upgrade and post-upgrade tasks, and might perform some optional upgrade tasks.

If any of the servers in your distributed management group do not meet the supported configuration requirements for System Center 2012 – Operations Manager, and require the installation of a new server, you should follow this checklist. For more information, see Supported Configurations for System Center 2012 – Operations Manager. Some of the servers might meet these requirements, and therefore, you might not have to perform the steps in every section. For example, if the server that hosts your RMS meets the supported configuration requirements, you can run the final upgrade from the RMS and skip the section on running the final upgrade from a secondary management server.

If your distributed management group already meets the minimum supported configurations for System Center 2012 – Operations Manager, or if you have a single-server management group, see the following topics.

Upgrade Path Checklist	Condition
Checklist: Single-Server Upgrade (Simple)	Your Operations Manager 2007 R2 single-server management group already meets the minimum supported configurations for System Center 2012 – Operations Manager.
Checklist: Single-Server Upgrade (Complex)	Your Operations Manager 2007 R2 single-server management group does not meet the minimum supported configurations for System Center 2012 – Operations Manager and requires new hardware.
Checklist: Distributed Upgrade (Simple)	Your Operations Manager 2007 R2 distributed

Upgrade Path Checklist	Condition
	management group already meets the minimum supported configurations for System Center 2012 – Operations Manager.

Checklist

Use the following checklist to upgrade your distributed management group if any of the servers do not yet meet the supported configuration requirements for System Center 2012 – Operations Manager.

Tip

You can also view a process flow diagram that links to the relevant topics. For more information, see Distributed Upgrade (Complex) .

This checklist contains multiple paths and you will not have to follow each step consecutively. For example, you will upgrade the management group from either the RMS or the secondary management server, depending on your current configuration. You should follow the steps in each as needed.

Section	Description
Import the Upgrade Helper Management Pack	Use these procedures to import and use the Upgrade Helper management pack.
Replacing Secondary Management Servers	Use these procedures if your secondary management servers do not meet the minimum system requirements for System Center 2012 – Operations Manager. If your secondary management servers have a 32-bit operating system, you must replace each server. For each 32-bit secondary management server, you must add a new 64-bit server and move the agents from the old management server to the new management server. You must ensure that all management servers meet all of the minimum system requirements for System Center 2012 – Operations Manager.
Replacing Gateways	Use these procedures if your gateway servers do not meet the minimum system requirements for System Center 2012 – Operations Manager. If your gateways have a 32-bit operating system, you must replace each gateway server with a new gateway server that meets the requirements. You must ensure that all

Section	Description
	gateway servers meet the minimum system requirements for System Center 2012 – Operations Manager.
Secondary Management Server Upgrade	Use these procedures to upgrade the secondary management servers, any gateway servers, and agents.
Management Group Upgrade from RMS	Use these procedures only if your RMS meets the minimum system requirements for System Center 2012 – Operations Manager.
Management Group Upgrade from Secondary Management Server	Use these procedures only if your RMS does not meet the minimum system requirements for System Center 2012 – Operations Manager.

Import the Upgrade Helper Management Pack

The Upgrade Helper management pack helps to guide you through the upgrade process. You should import this management pack before you start the upgrade process for a distributed management group that does not meet the supported configuration requirements for System Center 2012 – Operations Manager.

	Task	References
☐	Import the Upgrade Helper Management Pack	Upgrade Helper Management Pack

Replacing Secondary Management Servers

If your secondary management server already meets the minimum system requirements, go to the Replacing Gateways section of this checklist. Otherwise, use the following procedures for each secondary management server in your management group.

Note

You only have to add new secondary management servers if your current servers have a 32-bit operating system, which do not meet the supported configuration requirements for System Center 2012 – Operations Manager. Otherwise, just ensure that your secondary management servers meet the remaining supported configuration requirements.

	Task	References
☐	If operating system is 32-bit, add a secondary management server.	How to Add an Operations Manager 2007 R2 Secondary Management Server (Operations

	Task	References
		Manager Upgrade)
☐	Move the Operations Manager 2007 R2 agents to a secondary management server, and remove the old secondary management server.	How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)
☐	Ensure that the secondary management server meets the supported configuration requirements for System Center 2012 – Operations Manager.	Supported Configurations for System Center 2012 - Operations Manager

Replacing Gateways

If you do not have gateway servers, or you have gateways that meet the minimum system requirements, go to the Secondary Management Server Upgrade section of this checklist. Otherwise, use the following procedures for each gateway in your management group.

Note

You only have to add new gateway servers if your current servers are 32-bit, which do not meet the supported configuration requirements for System Center 2012 – Operations Manager. Otherwise, just ensure that your gateway servers meet the remaining supported configuration requirements.

	Task	References
☐	If gateway server does not have a 64-bit operating system, build a new gateway server.	How to Replace an Operations Manager 2007 R2 Gateway that Has an Unsupported Configuration (Operations Manager Upgrade)
☐	Remove the old gateway server.	How to Remove an Operations Manager 2007 R2 Gateway (Operations Manager Upgrade)
☐	Ensure that the gateway server meets the supported configuration requirements for System Center 2012 –	Supported Configurations for System Center 2012 - Operations Manager

	Task	References
	Operations Manager.	

Secondary Management Server Upgrade

Use the following procedures to upgrade your secondary management servers, gateway servers, and agents. Before you upgrade the secondary management server, you must ensure that your root management service (RMS) meets the supported configuration requirements for System Center 2012 – Operations Manager. For more information, see Supported Configurations for System Center 2012 - Operations Manager. If the RMS does not meet these configuration requirements, you must move agents that report to the RMS to the secondary management server before you upgrade the second management server. You should also ensure that SQL Server meets the supported configuration requirements.

	Task	References
☐	If RMS does not meet supported configuration requirements for System Center 2012 – Operations Manager, move agents that report to root management server to the secondary management server.	How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)
☐	If Microsoft SQL Server does not meet the supported configuration requirements, upgrade SQL Server.	Upgrading SQL Server (Operations Manager Upgrade)
☐	Back up the encryption key.	Back Up the Encryption Key
☐	Review the Operations Manager 2007 R2 event logs.	Review the Operations Manager 2007 R2 Event Logs
☐	Check if any gateway servers report to an unsupported RMS.	Check for Gateway Servers Reporting to the RMS
☐	Remove agents from Pending Management.	Remove Agents from Pending Management
☐	Verify that you have a supported SQL Server collation on all databases and instances of databases.	Verify the SQL Server Collation
☐	Upgrade the manually installed	Upgrading Manually Installed

	Task	References
	agents.	Agents
☐	Upgrade the secondary management servers.	How to Upgrade a Secondary Management Server from Operations Manager 2007 R2
☐	Upgrade gateway servers, if present.	How to Upgrade a Gateway Server from Operations Manager 2007 R2
☐	Upgrade the push-installed agents.	Upgrading Push-Installed Agents

Management Group Upgrade from RMS

If your RMS does not meet the minimum supported configurations for System Center 2012 – Operations Manager, go to the Management Group Upgrade from Secondary Management Server section of this checklist. Otherwise, use the following procedures to upgrade your management group from the root management server.

Note
A clustered RMS does not meet the supported configuration requirements for System Center 2012 – Operations Manager.

	Task	References
☐	Check for any active, connected consoles to the root management server.	Check the Operations Manager 2007 R2 RMS for Active Connected Consoles
☐	Disable all notification subscriptions.	Disable the Notification Subscriptions
☐	Stop services or disable any connectors that are installed.	Stop the Services for Connectors
☐	Verify that your operational database has sufficient free space.	Verify that the Operational Database has More than 50 Percent of Free Space
☐	Back up all databases.	Back Up the Operations Manager Databases
☐	Run management group upgrade on the root management server.	How to Upgrade a Management Group from an Operations Manager 2007 R2 RMS

	Task	References
☐	Upgrade optional features.	Upgrading or Installing Optional Features
☐	Re-enable the notification subscriptions.	Re-enable the Notification Subscriptions.
☐	Restart or re-enable the service for any connectors that are installed.	Restart the Connector Services
☐	Update overrides.	Update Overrides
☐	Verify the success of the upgrade.	Verify the Upgrade Success

Management Group Upgrade from Secondary Management Server

If your root management server meets the minimum supported configurations for System Center 2012 – Operations Manager, go to the Management Group Upgrade from RMS section of this checklist. Otherwise, use the following procedures to upgrade your management group from a secondary management server.

Note
A clustered RMS does not meet the supported configuration requirements for System Center 2012 – Operations Manager.

	Task	References
☐	Check for any active, connected consoles to the root management server.	Check the Operations Manager 2007 R2 RMS for Active, Connected Consoles
☐	Disable all notification subscriptions.	Disable the Notification Subscriptions
☐	Stop services or disable any connectors that are installed.	Stop the Services for Connectors
☐	Verify that your operational database has sufficient free space.	Verify that the Operational Database has More than 50 Percent of Free Space
☐	Back up all databases.	Back Up the Operations Manager Databases
☐	Restore the encryption key.	Restore the Encryption Key on the Secondary Management

	Task	References
		Server
☐	Run the management group upgrade on the secondary management server.	How to Upgrade a Management Group from an Operations Manager 2007 R2 Secondary Management Server
☐	If required, install the optional features, such as the consoles and Reporting.	Upgrading or Installing Optional Features
☐	Re-enable the notification subscriptions.	Re-enable the Notification Subscriptions.
☐	Restart or re-enable the service for any connectors that are installed.	Restart the Connector Services
☐	Uninstall the old root management server.	Uninstall the Old RMS
☐	Update overrides.	Update Overrides
☐	Verify the success of the upgrade.	Verify the Upgrade Success

See Also

Upgrade Path Checklists for Operations Manager

Distributed Upgrade (Complex)

Pre-Upgrade Tasks for Operations Manager

You have to perform a number of pre-upgrade tasks before you upgrade from System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager. The order in which you perform these tasks will vary depending on your upgrade path. For more information about which order you should follow, see Upgrade Path Checklists for Operations Manager.

Overview of the Pre-Upgrade Tasks

In a single-server management group upgrade, you must perform all the applicable pre-upgrade tasks before you start the upgrade process. Service will be interrupted until the upgrade process is completed. If your single-server management group does not meet the minimum system requirements, or you do not want to experience downtime, you can add a secondary management server, and then follow the distributed management group upgrade process.

In a distributed management group upgrade, you perform the upgrade in phases to minimize the interruption in service. For more information about these phases, see Upgrade Tasks for Operations Manager. You might have to perform pre-upgrade tasks before each upgrade phase.

Important
Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see Supported Configurations for System Center 2012 – Operations Manager.

The following table shows the tasks that you must complete before you upgrade from Operations Manager 2007 R2 to System Center 2012 – Operations Manager. This table provides the following information:

- Tasks to complete
- Links to the procedures related to those tasks
- Potential downtime that a task might create
- Description of the potential risk to the stability of your data and monitoring environment and how to mitigate that risk

Important
The order of the tasks depends on the upgrade path that you follow. Use the Upgrade Path Checklists for Operations Manager to follow the steps in order for your particular upgrade scenario.

Task	Downtime, risk, and mitigation
Upgrade Hardware and Software to Meet System Requirements	Possible downtime if hardware and software changes are needed. Risk dependent on required changes.
Import the Upgrade Helper Management Pack	No downtime or interference; low risk.
Back up the RMS Encryption Key	No downtime or interference; low risk.
Review the Operations Manager 2007 R2 Event Logs	No downtime or interference; low risk.
Check for Gateway Servers Reporting to the RMS	No downtime or interference; low risk if the management servers have the necessary certificates.
Remove Agents from Pending Management	No downtime or interference; low risk.
Check the Operations Manager 2007 R2 RMS for Active Connected Consoles	Consoles might lose connectivity to the RMS during upgrade.

Task	Downtime, risk, and mitigation
Disable the Notification Subscriptions	• Interference; no notifications are sent during the upgrade. • Mitigation; after the upgrade, check for any alerts that were missed.
Stop the Services or Disable any Connectors	Connectors do not function during upgrade.
Verify that the Operational Database Has More Than 50 Percent Free Space	No downtime or interference; low risk.
Verify the SQL Server Collation	The management group upgrade does not succeed if unsupported collation configurations exist.
Back up the Operations Manager Databases	Depending on the backup technology that you use, some backup methods might lock a database during backup.
Restore the RMS Encryption Key on the Secondary Management Server	No downtime or interference; low risk. Required only if the root management server (RMS) does not meet the supported configuration requirements for System Center 2012 – Operations Manager. This should be performed just prior to management group upgrade.
Upgrade SQL Server Reporting Services	The reports will be unavailable, but data will not be lost.

Upgrade Hardware and Software to Meet System Requirements

Before you perform the pre-upgrade and upgrade tasks, you might have to upgrade the hardware and software to meet system requirements. For more information, see Supported Configurations for System Center 2012 - Operations Manager and Upgrading Hardware and Software to Meet System Requirements.

Import the Upgrade Helper Management Pack

An Upgrade Helper management pack is available to help guide you through the upgrade process. For information about how to import and use the Upgrade Helper management pack, see Upgrade Helper Management Pack.

Review the Operations Manager 2007 R2 Event Logs

Review the event logs for Operations Manager 2007 R2 on the root management server (RMS) and on the management servers to look for recurring warning or critical events. Address them and save a copy of the event logs before you perform your upgrade.

Check for Gateway Servers Reporting to the RMS

If there are gateway servers that report to an Operations Manager 2007 R2 RMS with an unsupported configuration, you must ensure that the secondary management server from which you will perform the management group upgrade can communicate with the gateway. You can run a Windows PowerShell script to display the primary and failover management servers for all gateway servers. Run the following script.

```
#Display Primary and Failover Management Servers for all Gateway Servers

$GWs = Get-SCOMManagementServer | where {$_.IsGateway -eq $true}

$GWs | sort | foreach {

Write-Host "";

"Gateway MS :: " + $_.Name;

"--Primary MS :: " + ($_.GetPrimaryManagementServer()).ComputerName;

$failoverServers = $_.getFailoverManagementServers();

foreach ($managementServer in $failoverServers) {

"--Failover MS :: " + ($managementServer.ComputerName);

}

}

Write-Host "";
```

To ensure mutual authentication between the gateway and the secondary management server, you install certificates from a certification authority (CA) on the secondary management server and the gateway server. For more information, see the Deploying the Certificates section of How to Replace an Operations Manager 2007 R2 Gateway that Has an Unsupported Configuration (Operations Manager Upgrade).

After you have imported the certificates on the new secondary management server, and you verify that the gateway server has a healthy state, you must set the new management server as the primary management server for the gateway, and set the RMS as the secondary management server.

Remove Agents from Pending Management

Before you upgrade the secondary management server, remove any agents that are in Pending Management.

To remove agents that are in Pending Management

1. Log on to the Operations console by using an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 management group.
2. In the **Administration** pane, expand **Device Management**, and then click **Pending Management**.
3. Right-click each agent, and then click **Approve** or **Reject**.

Back up the RMS Encryption Key

The Operations Manager 2007 R2 root management server (RMS) encryption key is necessary to decrypt secure data in the operational database. When you have a backup of the RMS encryption key, you can import the key on a new management server when you upgrade the management group from an Operations Manager 2007 R2 secondary management server.

To back up the encryption key by using the Encryption Key Backup or Restore Wizard

1. Log on to the computer hosting the secondary management server with an account that is a member of the Administrators group.
2. Open a command prompt window by using the **Run as Administrator** option.
3. At the command prompt, type:

   cd <Operations Manager Installation Folder>

   SecureStorageBackup
4. In the **Encryption Key Backup or Restore Wizard**, on the **Backup or Restore** page, select the **Backup the Encryption Key** option, and then complete the wizard, providing a location and password for the key.

   Note
   Recovery of the password is not possible if the key is lost or forgotten.

   Note
   Store the encryption key in a location that can be easily accessed, such as a file share. You have to restore this encryption key on all management servers in your management group before you upgrade.

To back up the RMS encryption key by using the Command Prompt window

1. Log on to the computer that hosts the Operations Manager 2007 R2 root management server by using an account that is a member of the Administrators group.
2. Open a Command Prompt window as an administrator by using the **Run as administrator** option.
3. At the command prompt, type **cd <path to installation folder>**, and then press Enter.
4. To back up the encryption key, do the following:
   a. Type **SecureStorageBackup Backup <BackupFile>**, and then press Enter.
   b. At the **Please enter the password to use for storage/retrieval** prompt, type a password that is at least eight characters long, and then press Enter.
   c. At the **Please re-enter your password** prompt, type the same password, and then press Enter.

Check the Operations Manager 2007 R2 RMS for Active Connected Consoles

Consoles that are connected to the Operations Manager 2007 R2 RMS might lose connectivity during the upgrade of the management group. Before you perform the upgrade of the management group, you should notify anyone who has a connected console to close the connection.

Disable the Notification Subscriptions

You should disable notification subscription before you upgrade the management group to ensure that notifications are not sent during the upgrade process.

To disable subscriptions

1. Log on to the Operations console account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, select the **Administration** view.
3. In the navigation pane, expand **Administration**, expand the **Notifications** container, and then click **Subscriptions**.
4. Select each subscription, and then click **Disable** in the **Actions** pane.

   Note
   Multiselect does not work when you are disabling subscriptions.

Stop the Services or Disable any Connectors

Refer to the non-Microsoft connector documentation for any installed Connectors to determine the services used for each Connector, and whether it is supported for System Center 2012 – Operations Manager.

To stop a service for Connectors

1. On the **Start** menu, point to **Administrative Tools**, and then click **Services**.
2. In the **Name** column, right-click the Connector that you want to control, and then click **Stop**.

Verify that the Operational Database Has More Than 50 Percent Free Space

You must verify that the operational database has more than 50 percent of free space before you upgrade the management group because the upgrade might fail if there is not enough space. You should also ensure that the transactions logs are 50 percent of the total size of the operational database.

To check how much free space the Operational Database has

1. On the computer that hosts the operational database, open **SQL Server Management Studio**.
2. In the **Object Explorer**, expand **Databases**.
3. Right-click the operational database, point to **Reports**, **Standard Reports**, and then click **Disk Usage**.
4. View the **Disk Usage** report to determine the percentage of free space.

To increase the free space for the operational database and log files

1. On the computer that hosts the operational database, open **SQL Server Management Studio**.

2. In the **Connect to Server** dialog box, in the **Server Type** list, select **Database Engine**.
3. In the **Server Name** list, select the server and instance for your operational database (for example, computer\INSTANCE1).
4. In the **Authentication** list, select **Windows Authentication**, and then click **Connect**.
5. In the **Object Explorer** pane, expand **Databases**, right-click the operational database, and then click **Properties**.
6. In the **Database Properties** dialog box, under **Select a page**, click **Files**.
7. In the results pane, increase the **Initial Size** value for the **MOM_DATA** database by 50 percent.

   Note
   This step is not required if free space already exceeds 50 percent.
8. Set the **Initial Size** value for the **MOM_LOG** to be 50 percent of the total size of the database. For example, if the operational database size is 100 GB, the log file size should be 50 GB. Then click **OK**.

Verify the SQL Server Collation

SQL Server collation for all databases and database instances must be one of the following:

Language	Collation
English	SQL_Latin1_General_CP1_CI_AS
French	French_CI_AS
Russian	Cyrillic_General_CI_AS
Chinese CHS	Chinese_PRC_CI_AS
Japanese	Japanese_CI_AS
Spanish	Traditional_Spanish_CI_AS
Other Languages	Latin1_General_CI_AS

Important
You must ensure that all databases and database instances have the correct collation before you run upgrade on the management group.

To determine the SQL Server collation of a database, you can check the database properties. In SQL Server Management Studio, right-click the database you want to check, and then click **Properties**. The collation is listed under **Maintenance**.

For information about changing the SQL Server collation of a database, see Setting and Changing the Server Collation.

Restore the RMS Encryption Key on the Secondary Management Server

When you cannot upgrade the management group from the RMS because it does not meet the minimum supported configurations for System Center 2012 – Operations Manager, you must restore the encryption key on the Operations Manager 2007 R2 secondary manager server from which you will run the management group upgrade. For more information about whether the RMS meets the required supported configurations, see Supported Configurations for System Center 2012 - Operations Manager. You should restore the encryption key just prior to upgrading the management group. To restore the encryption key, you must use the SecureStorageBackup tool.

To restore up the RMS encryption key by using the Encryption Key Backup or Restore Wizard

1. Log on to the computer hosting the secondary management server with an account that is a member of the Administrators group.
2. Open a command prompt window by using the **Run as Administrator** option.
3. At the command prompt, type:

   cd <Operations Manager Installation Folder>

   SecureStorageBackup
4. In the **Encryption Key Backup or Restore Wizard**, on the **Backup or Restore?** page, select the **Restore the Encryption Key** option and then complete the wizard, providing location and password for the key.

To restore the RMS encryption key by using the command prompt

1. Log on to the computer hosting the secondary management server with an account that is a member of the Administrators group.
2. In a Command Prompt window using the **Run as Administrator** option, type:

   cd <Operations Manager Installation Folder>

   SecureStorageBackup Restore <BackupFile>
3. At the **Please enter the password to use for storage/retrieval** prompt, type the password, and then press Enter.
4. Use the same password that was used to back up the encryption keys.

To verify that the RMS encryption key has been restored

1. On the **Start** menu, click **Run**.
2. Type **regedit**, and then click **OK**. The Registry Editor starts.

   Caution
   Incorrectly editing the registry can severely damage your system. Before you make changes to the registry, back up any valued data that is on the computer.
3. Navigate to the **HKLM\Software\microsoft\Microsoft Operations Manager\3.0\MOMBins** key. If **value1** and **value2** exist, the encryption key has successfully been restored.

Back up the Operations Manager Databases

Obtain verified recent backups of the operational database and of the data warehouse database before you upgrade the secondary management server. You should also create backups of databases for optional features, such as the Reporting and the Audit Collection Services database before you upgrade them. For more information, see How to: Back up a Database and How to Schedule Backups of System Center 2012 - Operations Manager Databases.

Upgrade SQL Server Reporting Services

System Center 2012 – Operations Manager requires either SQL Server 2008 R2 or SQL Server 2008 R2 Sp1 on the SQL Server Reporting Services database (SSRS). For information about upgrading to SQL Server, see Upgrading to SQL Server 2008 R2.

See Also

Upgrade Path Checklists for Operations Manager

Upgrade Tasks for Operations Manager

Upgrading an installation of System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager is a multistep process. Before you can upgrade your monitoring environment, you have to understand exactly what you are upgrading, the pre-upgrade steps, and the implications for your day-to-day operations.

Upgrade Phases

When you upgrade a single-server management group, you run the upgrade on all features installed on a single server. In a distributed management group upgrade, upgrade tasks are performed in a number of phases.

Each type of upgrade requires some pre-upgrade and post-upgrade tasks. The phases of upgrade include the following:

Upgrade phase	Description
Pre-Upgrade Tasks	Pre-upgrade tasks might have to be performed before any of the upgrade phases. For more information, see Pre-Upgrade Tasks for Operations Manager. The starting point for an upgrade is having an Operations Manager 2007 R2 topology and ensuring that all hardware and software meets the supported configurations for System Center 2012 – Operations Manager.
Secondary Management Server Upgrade	In a distributed management group upgrade, you upgrade the secondary management servers (excluding the root management server), the gateways, and agents. The order of

Upgrade phase	Description
	agent upgrade depends on how the agents were deployed. If you installed the agents manually, you upgrade the agents before you upgrade the management servers and gateways. If you installed the agents by using the **Computer and Device Management Wizard** (the Discovery wizard), you upgrade the agents after you upgrade the management servers and gateways. These kinds of agents are known as push-installed agents.
Management Group Upgrade	In a distributed management group upgrade, the root management server (RMS), operational database, data warehouse database, and management group are upgraded. If the RMS does not meet system requirements, upgrade is run from a secondary management server. In a single-server management group upgrade, you upgrade manually installed agents first, and then run the management group upgrade. Push-installed agents can be upgraded after you upgrade the management group.
Optional Upgrade	Additional features can be upgraded, including operations consoles, web consoles, reporting server, and Audit Collection Services (ACS).
Post-Upgrade Tasks	Post-upgrade tasks, such as turning on notifications, must be performed after you have completed your upgrade. For more information, see Post-Upgrade Tasks when Upgrading from Operations Manager 2007 R2.

Upgrading with the Exchange 2010 Management Pack

The Exchange 2010 Management Pack includes the Correlation Engine, which is usually installed on the same system as the Operations Manager RMS. For a simple upgrade, where the system supports System Center 2012 – Operations Manager, you do not have to change the Exchange 2010 Management Pack.

For a complex upgrade, where Operations Manager must be moved to a different system, do one of the following:

- Unistall the Exchange 2010 MP from its current system using the Windows Installer package, upgrade Operations Manager to the new system, and run the Windows Installer package to install the Exchange 2010 MP on the new system. Do not remove the Exchange 2010 MP in the Operations console.
- Upgrade Operations Manager to the new system and configure the Exchange 2010 MP correlation engine to point to that system by editing Microsoft.Exchange.Monitoring.CorrelationEngine.exe.config. The default location for this file is: C:\Program Files\Microsoft\Exchange Server\v14\Bin. Change the **value** in the following line to equal the FQDN of the new Operations Manager system:

  <add key="OpsMgrRootManagementServer" value="localhost" />

  Note
  If your Exchange 2010 MP correlation engine is installed on a cluster, you need to edit the configuration file on each member of the cluster.

See Also

Upgrading to System Center 2012 - Operations Manager

Improving Upgrade Performance

The upgrade of a management server that hosts more than 800 agents might take more than one hour. You can significantly reduce the required time to perform an upgrade by running several SQL Server commands. Use the following procedure for each management server that hosts 800 or more agents. It can also be used if the upgrade of a particular management server is taking over an hour. You can implement this procedure either before you start the upgrade or while the upgrade is running.

To improve upgrade performance

1. On the computer that hosts the operational database, open **SQL Server Management Studio**.
2. In the **Connect to Server** dialog box, in the **Server Type** list, select **Database Engine**.
3. In the **Server Name** list, select the server and instance for your Operations Manager database (for example, computer\INSTANCE1).
4. In the **Authentication** list, select **Windows Authentication**, and then click **Connect**.
5. In the **Object Explorer** pane, right-click the computer and instance name at the top of the Object Explorer tree, and then click **New Query**.
6. In the **New Query** results pane, type the following three SQL commands:

   ```
   use OperationsManager
   exec sp_updatestats
   DBCC FREEPROCCACHE
   ```

   Note
   The `use` command assumes that the name of the operational database was not

changed and the default value of `OperationsManager` is used.

7. Click the **Query** menu, and then click **Execute**.
8. Click the **File** menu, and then click **Exit**.

Upgrade Helper Management Pack

The Upgrade Helper management pack guides you through the upgrade process from System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager for a distributed topology. If you have a single-server management group, you can run an upgrade without the management pack. For more information, see Upgrading a Single-Server Operations Manager 2007 R2 Environment.

Note
Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see Supported Configurations for System Center 2012 – Operations Manager.

The Upgrade Helper management pack discovers the root management server, secondary management servers, gateway servers, and any agent-managed computers in your distributed Operations Manager 2007 R2 management group. The Upgrade Helper management pack monitors the progress of each phase of your upgrade.

Note
You might have to perform a number of pre-upgrade tasks before each phase of upgrade. For more information, see Upgrade Path Checklists for Operations Manager.

Importing and Using the Upgrade Helper Management Pack

The Upgrade Helper management pack is available on the System Center 2012 – Operations Manager installation media.

Note
It may take up to 15 minutes for discovery to run after you first import the management pack.

To import the Upgrade Helper Management pack

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 R2 management group.
2. In the Operations console, click **Administration**.

   Note
   When you run the Operations console on a computer that is not a management

server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the management server from which you want to connect to the Operations console.

3. Right-click the **Management Packs** node, and then click **Import Management Packs**.
4. In the Import Management Packs wizard, click **Add**, and then click **Add from disk**.
5. The **Select Management Packs to import** dialog box opens. Browse to the /ManagementPacks directory of the Operations Manager installation media. Select **OperationsManager.Upgrade.mp**, and then click **Open**.
6. The **Select Management Packs** page lists the management pack that you selected for import. A green check mark next to the management pack in the list indicates that the management pack can be imported. Click **Install**.

   The **Import Management Packs** page appears and shows the progress for the management pack. The management pack is downloaded to a temporary directory, imported to Operations Manager 2007 R2, and then deleted from the temporary directory. If there is a problem at any stage of the import process, select the management pack in the list to view the status details.
7. Click **Close**.

After you have imported the Upgrade Helper management pack, you can view steps for each upgrade phase in the **Monitoring** workspace of the Operations console.

Important

Typically, you follow each of the steps in the Upgrade Helper management pack in order. However, if you have manually installed agents, you should upgrade them before you upgrade the secondary management servers. You upgrade push-installed agents after you upgrade the secondary management servers.

To review the status of the secondary management servers in your management group

1. In the Operations Manager 2007 R2 console, in the navigation pane, click the **Monitoring** button.
2. Expand **Operations Manager 2007 R2 -> 2012 Upgrade MP**, and then click **Step 1: Upgrade Secondary Management Servers**. This displays all secondary management servers in your management group.
3. Review the state of each management server. If the secondary management server is upgraded, the state is **Healthy**. If it is not upgraded, a **Warning** appears.
4. You must upgrade each secondary management server and ensure that the status is healthy before you move to the next step in the process. For more information, see How to Upgrade a Secondary Management Server from Operations Manager 2007 R2.

   Note

   You can open the discovered instances with the Operations Manager Health Explorer to see the upgrade status, with additional information about how to upgrade the management servers.

To review the status of the gateway servers in your management group

1. In the Operations Manager 2007 R2 console, in the navigation pane, click the **Monitoring** button.
2. Expand **Operations Manager 2007 R2 -> 2012 Upgrade MP**, and then click **Step 2: Upgrade Gateway Servers**. This displays all gateway servers in your management group.
3. Review the state of each gateway server. If the gateway server is upgraded, the state is **Healthy**. If it is not upgraded, a **Warning** appears.
4. You must upgrade each gateway server and ensure that the status is healthy before you move to the next step in the process. For more information, see How to Upgrade a Gateway Server from Operations Manager 2007 R2.

Note

You can open the discovered instances with the Health Explorer to see the upgrade status, with additional information about how to upgrade the gateways.

To review the status of the agents in your management group

1. In the Operations Manager 2007 R2 console, in the navigation pane, click the **Monitoring** button.
2. Expand**Operations Manager 2007 R2 -> 2012 Upgrade MP**, and then click **Step 3: Upgrade Agents**. This displays all agent-managed computers in your management group. It also displays additional properties about the agents, such as **IsManuallyInstalled** and **DeployedViaActiveDirectory** to help you determine which upgrade process to follow.

Important

You must upgrade the agents that have a value of **True** in the **IsManuallyInstalled** property before you upgrade your secondary management servers.

3. Review the state of each agent. If the agent is upgraded, the state is **Healthy**. If it is not upgraded, a **Warning** appears.
4. You must upgrade the agents and ensure that the status of each is healthy before you move to the next step in the process. For more information, see How to Upgrade Agents from Operations Manager 2007 R2.

Note

You can open the discovered instances with the Health Explorer to see the upgrade status, with additional information about how to upgrade the agents.

To review the status of the RMS in the management group

1. In the Operations Manager 2007 R2 console, in the navigation pane, click the **Monitoring** button.

2. Expand **Operations Manager 2007 R2 -> 2012 Upgrade MP**, and then click **Step 4: Upgrade Management Group (RMS, DB, DW)**. This displays the root management server (RMS) in your management group.

   After the secondary management servers, gateways, and agents have been upgraded, you can upgrade the management group from the RMS. This upgrade process upgrades the operational database and the data warehouse. If the data warehouse does not already exist, it is installed.
3. If the management group has been upgraded, the state is **Healthy**. If it is not upgraded, a **Warning** appears.
4. If the root management server meets the minimum supported configurations for System Center 2012 – Operations Manager, you can upgrade from the RMS. For more information, see How to Upgrade a Management Group from an Operations Manager 2007 R2 RMS. If the root management server does not meet the minimum supported configurations, you must upgrade the management group from a secondary management server. For more information, see How to Upgrade a Management Group from an Operations Manager 2007 R2 Secondary Management Server. For more information about the supported configuration requirements for System Center 2012 – Operations Manager, see Supported Configurations for System Center 2012 - Operations Manager.

   Note
   You can open the discovered instances with the Health Explorer to see the upgrade status, with additional information about how to upgrade the management group.

See Also

Checklist: Distributed Upgrade (Simple)

Checklist: Distributed Upgrade (Complex)

Upgrading Hardware and Software to Meet System Requirements

Upgrading to System Center 2012 – Operations Manager requires that you start with an System Center Operations Manager 2007 R2 management groupIf you are using an earlier version of Operations Manager, you must first upgrade to Operations Manager 2007 R2. For more information, see Operations Manager 2007 Upgrade Guide.

Before you begin the upgrade process to System Center 2012 – Operations Manager, you should ensure that all servers in the management group meet the minimum supported configurations for System Center 2012 – Operations Manager. For more information, see Supported Configurations for System Center 2012 - Operations Manager.

If your servers do not meet the supported configuration requirements because they cannot support a 64-bit operating system, you have to add new servers that meet these requirements in addition to ensuring that all other required configuration requirements are met. The following topics describe how to perform the tasks necessary introduce new hardware to the Operations Manager 2007 R2 management group:

- How to Add an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)
- How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)
- How to Replace an Operations Manager 2007 R2 Gateway that Has an Unsupported Configuration (Operations Manager Upgrade)
- How to Remove an Operations Manager 2007 R2 Gateway (Operations Manager Upgrade)
- Upgrading SQL Server (Operations Manager Upgrade)

How to Add an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)

When you want to upgrade to System Center 2012 – Operations Manager but have a management server in your System Center Operations Manager 2007 R2 environment that does not meet the minimum supported configurations for System Center 2012 – Operations Manager, you must add a new server to replace the old one. You should install an Operations Manager 2007 R2 secondary management server, and then join it to your existing management group. Afterwards, you can move the agents from the old server to the new server. For more information, see How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade).

To ensure that your new server hardware and software meet the minimum supported configurations for System Center 2012 – Operations Manager, see Supported Configurations for System Center 2012 - Operations Manager.

To install a secondary management server

1. On a server that meets the supported configuration requirements for System Center 2012 – Operations Manager, install Operations Manager 2007 R2 by using the instructions in Deploying Stand-Alone Management Servers on Windows Server 2008.

   Note
   It can take up to five minutes for the System Center Management Service on the new management server to establish secure communications with the root management (RMS) server, and during that time it appears as not monitored. When communications are established, its Health state changes to Healthy.

   The next step is to move the agents that reported to the old management server or RMS to the new secondary management server. For more information, see How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade).

See Also

Upgrading Hardware and Software to Meet System Requirements

How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)

After you have added a secondary management server to your System Center Operations Manager 2007 R2 management group, you must move the agents that are reporting to the root management server (RMS) or management server that you are replacing to the new secondary management server.

You also move the agents to a secondary management server to avoid downtime when you upgrade a distributed management group that meets the minimum supported configurations for System Center 2012 – Operations Manager. For more information, see Supported Configurations for System Center 2012 - Operations Manager.

Important

If you have a distributed management group that meets the minimum supported configurations, you can alternatively upgrade the agents after you upgrade the management group instead of moving the agents to a secondary management server. However, you will experience monitoring downtime until the agents are upgraded.

You can move the agents by using the Operations console, by using Active Directory Integration, or by running a Windows PowerShell script. However, if the agents were deployed manually, you cannot move them by using the Operations console.

Moving Agents to a Secondary Management Server

To move Windows, UNIX, and Linux push-installed agents to a secondary management server by using the Operations console

1. Log on to a computer that hosts an Operations console with an Operations Manager Administrators role account for the Operations Manager 2007 R2 management group.
2. In the Operations console, click the **Administration** button.

   Note

   When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the Operations Manager 2007 R2 management server that you want the Operations console to connect to.
3. In the **Administration** pane, under **Device Management**, click **Agent-Managed**.
4. For Windows agents, right-click the computers in the **Agent-Managed** pane that have agents that you want to move to the secondary management server, and then click **Change Primary Management Server**.

   For UNIX and Linux agents, right-click the computers in the **UNIX/Linux Servers** pane that have agents that you want to move to the secondary management server, and then click **Change Primary Management Server**.
5. In the **Change Management Server** dialog box, select the secondary management server from the list, and then click **OK**. The change takes effect on the agent after its next update interval.

To move Windows agents to a secondary management server by using a Windows PowerShell script

1. Log on to a computer that hosts an Operations console with an Operations Manager Administrators role account for the Operations Manager 2007 R2 management group.
2. Run the following script.

```
$newMS = Get-ManagementServer | where {$_.Name –eq
'<SecondaryMgmtServer.DomainName.COM>'}

$agent = Get-Agent | where {$_.PrincipalName –eq
'<AgentComputer.Domain.COM>'}

Set-ManagementServer -AgentManagedComputer: $agent -
PrimaryManagementServer: $newMS
```

The Operations console should now list the secondary management server as the primary management server for the agent that was moved.

Moving Agents to a Secondary Management Server by using Active Directory Integration

Using Active Directory Integration to move Windows agents to a secondary management server is a multistep process. First, you delete the configuration rule for the management server that you will replace. Then, you create a new rule that sets the replacement management server as the failover management server. This step is an intermediary step that is required for the agent to recognize the replacement management server. After the agent assignment propagates in Active Directory Domain Services, which can take up to one hour, you delete the configuration rule that you just created. Finally, you create a new configuration rule on the replacement management server.

In the following procedures, it is assumed that you have an existing primary management server and a failover management server that do not meet the minimum configuration requirements for System Center 2012 – Operations Manager, and you have already created two new secondary management servers that do meet these requirements to replace the old ones. By creating the configuration rules for Active Directory Integration, you move the agents from the old servers to the new servers in a multistep process.

To create a configuration rule for the management server that you are replacing (step 1)

1. Log on to a computer that hosts an Operations console with an Operations Manager Administrators role account for the Operations Manager 2007 R2 management group.
2. In the Operations console, click the **Administration** button.

> **Note**
> When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the Operations Manager 2007 R2 management server that you want the Operations console to connect to.

3. In the **Administration** pane, under **Device Management**, click **Management Servers**.
4. In the **Management Servers** pane, right-click the management server that you are replacing, and then click **Properties**. This sets the management server that you are replacing as the **Primary Management Server** for the computers that are returned by the rules you will create in the following procedure.
5. In the **Management Server Properties** dialog box, click the **Auto Agent Assignment** tab.
6. Select the agent assignment, and then click **Delete**.

   Click **Add** to start the **Agent Assignment and Failover Wizard**, and then click **Next**.

   Note
   The **Introduction** page does not appear if the wizard has been run and **Do not show this page again** was selected.
7. On the **Domain** page, do the following:
   - Select the domain of the computers from the **Domain name** list. The management server must be able to resolve the domain name.

     Important
     The management server and the computers that you want to manage must be in 2-way trusted domains.
   - Select the **Use a different account to perform agent assigned in the specified domain** check box.
   - Set **Select Run As Profile** to the Run As profile associated with the Run As account that was provided when MOMADAdmin.exe was run for the domain. The default account that is used to perform agent assignment is the computer account for the root management server, also referred to as the **Active Directory-Based Agent Assignment Account**. If this was not the account that was used to run MOMADAdmin.exe, select **Use a different account to perform agent assignment in the specified domain**, and then select or create the account from the **Select Run As Profile** list.
8. On the **Inclusion Criteria** page, either type the LDAP query for assigning computers to this management server, and then click **Next**, or click **Configure**. If you click **Configure**, do the following:
   a. In the **Find Computers** dialog box, type the criteria that you want to use for assigning computers to this management server.
   b. Click **OK**, and then click **Next**.

   Note
   The following LDAP query returns computers with a name starting with MsgOps,
   (&(sAMAccountType=805306369)(objectCategory=computer)(cn=MsgOps*))
   For more information about LDAP queries, see Creating a Query Filter.
9. On the **Exclusion Rule** page, type the fully qualified domain name (FQDN) of computers that you explicitly want to prevent from being managed by this management server, and then click **Next**.

Important

You must separate the computer FQDNs that you type with a semicolon, colon, or a new line (CTRL+ENTER).

10. On the **Agent Failover** page, select **Manually configure failover**, and then do the following:
    a. Select the check box of the replacement secondary management server. This sets the replacement server as the failover server.
    b. Click **Create**.
11. In the **Management Server Properties** dialog box, click **OK**.

Note

It can take up to one hour for the agent assignment setting to propagate in Active Directory Domain Services.

12. After you have confirmed that the agent assignment was successful, delete the agent assignment that you created earlier.

To create a configuration rule for the replacement management server (step 2)

1. In the Operations console, click the **Administration** button.
2. In the **Administration** pane, under **Device Management**, click **Management Servers**.
3. In the **Management Servers** pane, right-click the replacement secondary management server, and then click **Properties**. This sets the replacement management server as the **Primary Management Server** for the computers that are returned by the rules that you will create in the following procedure.
4. In the **Management Server Properties** dialog box, click the **Auto Agent Assignment** tab.
5. Click **Add** to start the **Agent Assignment and Failover Wizard**, and then click **Next**.

Note

The **Introduction** page does not appear if the wizard has been run and **Do not show this page again** was selected.

6. On the **Domain** page, do the following:
    - Select the domain of the computers from the **Domain name** list. The management server must be able to resolve the domain name.

Important

The management server and the computers that you want to manage must be in 2-way trusted domains.

    - Select the **Use a different account to perform agent assigned in the specified domain** check box.
    - Set **Select Run As Profile** to the Run As profile associated with the Run As account that was provided when MOMADAdmin.exe was run for the domain. The default account that is used to perform agent assignment is the computer account for the

root management server, also referred to as the **Active Directory-Based Agent Assignment Account**. If this was not the account that was used to run MOMADAdmin.exe, select **Use a different account to perform agent assignment in the specified domain**, and then select or create the account from the **Select Run As Profile** list.

7. On the **Inclusion Criteria** page, either type the LDAP query for assigning computers to this management server, and then click **Next**, or click **Configure**. If you click **Configure**, do the following:
   a. In the **Find Computers** dialog box, type the criteria that you want to use for assigning computers to this management server.
   b. Click **OK**, and then click **Next**.

   Note
   The following LDAP query returns computers with a name starting with MsgOps, **(&(sAMAccountType=805306369)(objectCategory=computer)(cn=MsgOps*))**
   For more information about LDAP queries, see Creating a Query Filter.
8. On the **Exclusion Rule** page, type the fully qualified domain name (FQDN) of computers that you explicitly want to prevent from being managed by this management server, and then click **Next**.

   Important
   You must separate the computer FQDNs that you type with a semicolon, colon, or a new line (CTRL+ENTER).
9. On the **Agent Failover** page, select **Manually configure failover**, and then do the following:
   a. Select the check box of the second replacement management server that you added to the management group. This sets it as the failover server.
   b. Click **Create**.
10. In the **Management Server Properties** dialog box, click **OK**.

    Note
    It can take up to one hour for the agent assignment setting to propagate in Active Directory Domain Services.

See Also

Upgrading Hardware and Software to Meet System Requirements

How to Replace an Operations Manager 2007 R2 Gateway that Has an Unsupported Configuration (Operations Manager Upgrade)

If you have an System Center Operations Manager 2007 R2 gateway server that does not meet the minimum supported configuration requirements for System Center 2012 – Operations Manager, you must replace the gateway server before you upgrade to System Center 2012 – Operations Manager. For more information, see Supported Configurations for

System Center 2012 - Operations Manager. This procedure shows you how to add a new Operations Manager 2007 R2 gateway and to prepare it for upgrade.

Replacing an Operations Manager 2007 R2 Gateway Server

The steps you take to replace the gateway server include the following:

1. Register the computer that will host the gateway with the management group. See Registering the Gateway with the Management Group.
2. Install the Operations Manager 2007 R2 gateway server. See Installing a Gateway Server.
3. Deploy and import certificates on the gateway and management servers. See Deploying the Certificates.
4. Remove the old gateway server. See How to Remove an Operations Manager 2007 R2 Gateway (Operations Manager Upgrade).

Registering the Gateway with the Management Group

Before you install a new Operations Manager 2007 R2 gateway server, you must register the computer that will host the gateway with the management group. This procedure registers the gateway server with the management group, and when registration is completed, the gateway server appears in the **Discovered Inventory** view of the management group.

You must first copy the gateway approval tool (Microsoft.EnterpriseManagement.GatewayApprovalTool.exe) to the management server. This tool is required only on the management server, and it only has to be run one time.

To copy Microsoft.EnterpriseManagement.GatewayApprovalTool.exe to management servers

1. From a targeted management server, open the Operations Manager 2007 R2 installation media \SupportTools directory.
2. Copy the Microsoft.EnterpriseManagement.GatewayApprovalTool.exe from the installation media to the targeted management server. You should copy it to the installation directory of the management server.

To run the gateway approval tool

1. Log on to the management server that the gateway server will target by using the Operations Manager Administrators credentials.
2. Open a Command Prompt window, and browse to the directory where you copied Microsoft.EnterpriseManagement.gatewayApprovalTool.exe.
3. At the command prompt, run **Microsoft.EnterpriseManagement.gatewayApprovalTool.exe /ManagementServerName=<managementserverFQDN> /GatewayName=<GatewayFQDN> /Action=Create**
4. If the approval is successful, the following message appears **The approval of server <GatewayFQDN> completed successfully.**
5. Open the Operations console to the Monitoring view. Select the Discovered Inventory view to verify that the gateway server is present.

Installing a Gateway Server

You must install an Operations Manager 2007 R2 gateway on a server that meets the minimum supported configuration requirements for System Center 2012 – Operations Manager.

To install an Operations Manager 2007 R2 gateway server

1. Log on to the gateway server with local administrator rights.
2. From the Operations Manager 2007 R2 installation media, run **SetupOM.exe**.
3. In the **Install** area, click the **Install Operations Manager 2007 R2 Gateway** link.
4. On the **Welcome** page, click **Next**.
5. On the **Destination Folder** page, accept the default, or click **Change** to select a different installation directory, and then click **Next**.
6. On the **Management Group Configuration** page, type the targeted management group name in the **Management Group Name** box, type the targeted management server name in the **Management Server** box, check that the **Management Server Port** box is **5723**, and then click **Next**. This port can be changed if you have enabled a different port for management server communication in the Operations console.
7. On the **Gateway Action Account** page, select the **Local System** account option, unless you have specifically created a domain-based or local computer-based gateway action account. Click **Next**.
8. On the **Microsoft Update** page, optionally indicate if you want to use Microsoft Update, and then click **Next**.
9. On the **Ready to Install** page, click **Install**.
10. On the **Completing Installation** page, click **Finish**.

Deploying the Certificates

Because the gateway server is not trusted by the domain that the management group is in, certificates must be used to establish the identity of each gateway server and management server. This arrangement satisfies the requirement of Operations Manager for mutual authentication. You must request and download the certificates, and then import them by using the Operations Manager 2007 R2 MOMCertImport.exe tool.

Reliable name resolution must exist between the agent-managed computers and the gateway server and between the gateway server and the management servers. Typically, Domain Name System (DNS) is used to resolve host names, such as www.contoso.com, to their corresponding IP addresses. However, if it is not possible to get proper name resolution through DNS, you might have to manually create entries in the Hosts file of each computer to resolve host names to IP addresses.

Note

The Hosts file is located in a subdirectory of the C:\Windows\System32\Drivers, and it contains directions for configuration.

After you have downloaded the certificates to each gateway server and management server, you import them by using the MOMCertImport tool.

To request and download certificates

1. Request and download a Trusted Root (CA) certificate on each gateway and management server.

To import computer certificates by using MOMCertImport.exe

1. Copy the MOMCertImport.exe tool from the installation media \SupportTools directory to the root of the gateway server or to the Operations Manager 2007 R2 installation directory of the management server.
2. Open a Command Prompt window by using the **Run as Administrator** option, change to the directory to the location of MOMCertImport.exe, and then run **momcertimport.exe /SubjectName <certificate subject name>**. This makes the certificate usable by Operations Manager.

   Tip
   If you double-click MOMCertImport.exe or run it at the Command Prompt window without any parameters, a dialog box appears where you can select the installed certificate, and then click **OK**.

The next step is to remove the old gateway server from the management group. For more information, see How to Remove an Operations Manager 2007 R2 Gateway (Operations Manager Upgrade).

See Also

Upgrading Hardware and Software to Meet System Requirements

How to Remove an Operations Manager 2007 R2 Gateway (Operations Manager Upgrade)

How to Remove an Operations Manager 2007 R2 Gateway (Operations Manager Upgrade)

After you have replaced a System Center Operations Manager 2007 R2 gateway server that does not meet the minimum supported configurations for System Center 2012 – Operations Manager, you can remove the old gateways from the management group and uninstall the old gateway from the server. For more information, see Supported Configurations for System Center 2012 – Operations Manager.

You must first copy the gateway approval tool (Microsoft.EnterpriseManagement.GatewayApprovalTool.exe) from the \SupportTools directory of the Operations Manager 2007 R2 installation media to the management server, if it does not already exist.

To uninstall the gateway server

1. Log on to the gateway server to be removed with the Operations Manager 2007 R2 Administrators credentials.
2. In Control Panel, in **Programs and Features**, right-click **System Center Operations Manager 2007 R2 Gateway**, and then click **Uninstall**.

To remove a gateway from the management group

1. On the management server that was targeted during the gateway server installation, log on with Operations Manager Administrators credentials.
2. Open a Command Prompt window, and browse to the directory to where you copied Microsoft.EnterpriseManagement.gatewayApprovalTool.exe.
3. At the command prompt, run the following command, where GatewayName is the name of the gateway that you want to remove.
   Microsoft.EnterpriseManagement.gatewayApprovalTool.exe /ManagementServerName=<managementserverFQDN> /GatewayName=<GatewayFQDN> /Action=Delete
4. Open the Operations console to the Monitoring view. Select the **Discovered Inventory** view to see that the gateway server is no longer present.

See Also

Upgrading Hardware and Software to Meet System Requirements

Upgrading SQL Server (Operations Manager Upgrade)

Upgrading to System Center 2012 – Operations Manager requires Microsoft SQL Server 2008 SP1, SQL Server 2008 R2, or SQL Server 2008 R2 SP1 for the operational database, data warehouse database, and Audit Collection Services (ACS) database. If your servers do not support this upgrade, you have to add new servers and move your SQL Server databases from the old servers to the new servers. For more information, see Supported Configurations for System Center 2012 - Operations Manager.

For more information about how to move your System Center Operations Manager 2007 R2 databases, see:

- How to Move the Operational Database
- How to Move the Data Warehouse Database
- How to Move the OperationsManagerAC Database in Operations Manager 2007

For more information about how to upgrade a database, see:

- How to: Upgrade to SQL Server 2008 R2 (Setup)
- Upgrading to SQL Server 2008 R2

Upgrading a Single-Server Operations Manager 2007 R2 Environment

When you upgrade a single-server System Center Operations Manager 2007 R2 environment to System Center 2012 – Operations Manager, you run the upgrade on all features on a single server. If a data warehouse does not already exist, it is created during the upgrade process because having a data warehouse is a requirement for System Center 2012 – Operations Manager. You upgrade any manually installed agents before you run upgrade on the management group. If you installed agents by using the **Computer and Device Management Wizard** (the Discovery wizard), you can upgrade these agents after you upgrade the management group by using the Operations Manager Operations console.

The following topics describe how to perform the necessary steps to upgrade a single-server management group that has a supported configuration for System Center 2012 – Operations Manager. For more information, see Supported Configurations for System Center 2012 - Operations Manager.

- How to Upgrade an Operations Manager 2007 R2 Single-Server Management Group
- Upgrading Agents in an Operations Manager 2007 R2 Single-Server Management Group

See Also

Checklist: Single-Server Upgrade (Simple)

Checklist: Single-Server Upgrade (Complex)

Single-Server and Distributed Upgrade Process Flow Diagram

How to Upgrade an Operations Manager 2007 R2 Single-Server Management Group

When you upgrade a System Center Operations Manager 2007 R2 single-server management group to System Center 2012 – Operations Manager, all features that are installed on the server are upgraded. This includes the Operations Manager 2007 R2 operational database, management server, operations console, web console, and Reporting server, if installed. The Operations Manager 2007 R2 data warehouse is also upgraded, if it exists. Otherwise, the **System Center Operations Manager 2012 Setup Wizard** installs it.

Important
Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see Supported Configurations for System Center 2012 – Operations Manager.

If your single-server management group meets the supported configuration requirements, but you do not want to experience any downtime during the upgrade process, you can add a secondary management server, and then follow the upgrade process for a distributed upgrade. For more information, see Supported Configurations for System Center 2012 - Operations Manager. If your server cannot meet the supported configurations because it requires new hardware, you can add a secondary management server, and then follow the upgrade process for a distributed upgrade. For more information, see Upgrade Path Checklists for Operations Manager.

To upgrade a single-server management group

1. Log on to the computer that is hosting a root management server (RMS) with an account that is a member of the Operations Manager Administrators role for your Operations Manager 2007 R2 management group and a local administrator on the computer.
2. On the System Center 2012 – Operations Manager media, run **Setup.exe**, and then click **Install**.

Note

The **Getting Started** page displays information about what will be upgraded. The Operations Manager data warehouse will be installed if it does not already exist. Click **Next** to proceed with the upgrade.

3. On the **Getting Started**, **Please read the license terms** page, read the Microsoft Software License Terms, click **I have read, understood, and agree with the license terms**, and then click **Next.**
4. On the **Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager**, or type in a new location or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.

   Note

   Microsoft SQL Server Full Text Search must be enabled.

   Note

   The **Agent Upgrade Check** warning can be ignored if you plan to upgrade the agents after the single-server management group has been upgraded.
6. If the Prerequisites checker does not return any other errors or warnings that have to be addressed, click **Next**.
7. If the single-server management group does not already have a data warehouse installed, a data warehouse is created, and you must configure it as follows:
   a. On the **Configure the data warehouse database** page, in the **Server name and instance name** box, type the server name of the SQL Server database and instance for the database server that will host the data warehouse database.
   b. After you have typed in the correct values for the server name of the SQL Server database, Setup attempts to validate the values that you have typed as the SQL Server name and the port number. In the **Database name**, **Database size (MB)**, **Data file folder**, and **Log file folder** boxes, we recommend that you accept the default values. Click **Next**.

      Warning

      These paths do not change if you connect to a different instance of SQL Server.

   c. On the **Configuration**, **Specify a web site for use with the Web console** page, select the **Default Web Site**, or the name of an existing website. Select **Enable SSL** only if the website has been configured to use Secure Sockets Layer (SSL), and then click **Next**.
   d. On the **Configuration**, **Select an authentication mode for use with the Web console** page, select your options, and then click **Next**.
8. On the **Configuration**, **Configure Operations Manager accounts** page, we recommend that you use the **Domain Account** option for the **System Center**

Configuration service and System Center Data Access service accounts. Enter the credentials for a domain account in each box, and then click **Next**.

Important
If you receive a message about using the wrong version of SQL Server, or experience a problem with the SQL Server Windows Management Instrumentation (WMI) provider, you can resolve this. Open a Command Prompt window by using the **Run as administrator** option. Then run the following command, where <path> is the location of Microsoft SQL Server:

mofcomp.exe "<path>\Microsoft SQL Server\100\Shared\sqlmgmproviderxpsp2up.mof".

9. When the **Ready to Upgrade** page appears, review the upgrade summary, and then click **Upgrade**.

To upgrade a single-server management group by using the Command Prompt window

1. Log on to the computer that is hosting a RMS with an account that is a member of the Operations Manager Administrators role for your Operations Manager 2007 R2 management group and a local administrator on the computer.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the System Center 2012 – Operations Manager Setup.exe file is located.

Important
Use the `/WebConsoleUseSSL` parameter only if your website has Secure Sockets Layer (SSL) activated. For a default web installation, specify **Default Web Site** for the `/WebSiteName` parameter.

Note
If the web console reports to an unsupported or inaccessible root management server, you must also pass the following parameter:

`/ManagementServer:<servername>.`

Important
The following commands assume that you specified the Local System for the Data Access service (`/UseLocalSystemDASAccount`). To specify a domain\user name for these accounts, you must provide the following parameters instead:

`/DASAccountUser: <domain\username> /DASAccountPassword: <password>`

If you installed a data warehouse in your Operations Manager 2007 R2 management group, use the following command.

```
setup.exe /silent /upgrade /UseLocalSystemDASAccount
/WebsiteName: "<WebSiteName>" [/WebConsoleUseSSL]
/WebConsoleAuthorizationMode: [Mixed|Network]
```

If you did not install a data warehouse in your Operations Manager 2007 R2 management group, use the following command.

```
Setup.exe /silent /upgrade /UseLocalSystemDASAccount
/AcceptEndUserLicenseAgreement
/WebsiteName: "<WebSiteName>" [/WebConsoleUseSSL]
/WebConsoleAuthorizationMode: [Mixed|Network]
/DWSqlServerInstance: <server\instance>
/DWDatabaseName: <DW name>
/DataReaderUser: <domain\username>
/DataReaderPassword: <password>
/DataWriterUser: <domain\username>
/DataWriterPassword: <password>
```

See Also

Upgrading Agents in an Operations Manager 2007 R2 Single-Server Management Group

Checklist: Single-Server Upgrade (Simple)

Checklist: Single-Server Upgrade (Complex)

Upgrading Agents in an Operations Manager 2007 R2 Single-Server Management Group

You can upgrade System Center Operations Manager 2007 R2 agents in a single-server management group by using the Operations console, manually by using the Setup Wizard, or manually, by using a command prompt. Determining which option to use depends on how the agents were deployed. For example, agents that were installed by using the **Computer and Device Management Wizard** (“push-installed agents”) can be upgraded through the Operations console. However, agents that were installed manually (“manually installed agents”) cannot be upgraded this way. You can verify how agents were installed by using the Upgrade Helper management pack. For more information, see Upgrade Helper Management Pack.

Important

For information about how upgrade works with AVIcode 5.7 agents and .NET Application Performance Monitoring Agents, see Notes for AVIcode 5.7 Customers.

You should upgrade manually installed agents before you run upgrade on the management group. Push-installed agents can be upgraded after you run upgrade on the management group. You use the System Center 2012 – Operations Manager Operations console to upgrade push-installed agents in a single-server management group.

For information about how to upgrade Windows agents and UNIX and Linux agents, see How to Upgrade Agents from Operations Manager 2007 R2.

See Also

Upgrading Operations Manager 2007 R2 Agents in a Distributed Management Group

Upgrading a Distributed Operations Manager 2007 R2 Environment

When you upgrade a distributed System Center Operations Manager 2007 R2 environment to System Center 2012 – Operations Manager, you start by upgrading any manually installed agents, followed by the secondary management servers, gateways, and any push-installed agents. You then run upgrade of the management server either on the root management server (RMS), if it meets the minimum supported configurations for Operations Manager, or from the secondary management server if it does not meet these requirements. You can then upgrade additional, optional features, such as consoles, the Reporting server, and the Audit Collection Services (ACS) Collector.

Important

Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see Supported Configurations for System Center 2012 – Operations Manager.

The following topics describe how to perform the necessary steps in a distributed management group upgrade. The specific upgrade path you take depends on your current environment. For information on choosing an upgrade path, see Upgrade Path Checklists for Operations Manager.

- How to Upgrade a Secondary Management Server from Operations Manager 2007 R2
- How to Upgrade a Gateway Server from Operations Manager 2007 R2
- Upgrading Operations Manager 2007 R2 Agents in a Distributed Management Group
- How to Upgrade Agents from Operations Manager 2007 R2
- How to Upgrade a Management Group from an Operations Manager 2007 R2 RMS
- How to Upgrade a Management Group from an Operations Manager 2007 R2 Secondary Management Server
- How to Upgrade a Stand-Alone Operations Console from Operations Manager 2007 R2
- How to Upgrade a Web Console from Operations Manager 2007 R2
- How to Upgrade Reporting from Operations Manager 2007 R2
- How to Upgrade an ACS Collector from Operations Manager 2007 R2

See Also

Checklist: Distributed Upgrade (Simple)

Checklist: Distributed Upgrade (Complex)

Distributed Upgrade (Complex) Process Flow Diagram

Single-Server and Distributed Upgrade (Simple) Process Flow Diagram

Upgrading a Single-Server Operations Manager 2007 R2 Environment

How to Upgrade a Secondary Management Server from Operations Manager 2007 R2

This procedure demonstrates how to upgrade a System Center Operations Manager 2007 R2 secondary management server to System Center 2012 – Operations Manager in a distributed environment. To learn more about each upgrade path and the order in which to perform each upgrade task, see the Upgrade Path Checklists for Operations Manager.

Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see Supported Configurations for System Center 2012 – Operations Manager.

To upgrade a secondary management server

1. Log on to the secondary management server with an account that is a member of the Operations Manager Administrators role for your Operations Manager 2007 R2 management group and a local administrator on the computer.
2. From the System Center 2012 – Operations Manager media, run **Setup.exe**, and then click **Install**. The **Getting Started** page displays information about which features will be upgraded.

   Note
   If a web console exists on the secondary management server, it will be removed instead of upgraded. You have to re-install the web console after you upgrade the management group. For more information, see How to Install the Operations Manager Web Console. To minimize downtime, you can install the Operations Manager 2007 R2 web console on a stand-alone server.
3. On the **Getting Started**, **System Center 2012 - Operations Manager Upgrade** page, click **Next** to proceed with the upgrade.
4. On the **Getting Started**, **Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager**, or type in a new location, or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration**, **Configure Operations Manager accounts** page, we recommend that you use the **Domain Account** option for the **System Center Configuration service and System Center Data Access service** accounts.

   Enter the credentials for a domain account, and then click **Next**.
8. Review the options on the **Configuration**, **Ready To Upgrade** page, and then click **Upgrade**. The upgrade proceeds and displays the upgrade progress.
9. When the upgrade is finished, the **Upgrade complete** page appears. Click **Close**.

Upgrading a secondary management server is just one phase of the distributed upgrade process. Upgrade is not completed until you have upgraded all of the other features in your management group, and have run upgrade on the management group itself. The next step is to upgrade any gateways.

To upgrade a secondary management server by using the Command Prompt window

1. Log on to the secondary management server with an account that is a member of the Operations Manager Administrators role for your Operations Manager 2007 R2 management group and a local administrator on the computer.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the System Center 2012 – Operations Manager setup.exe file is located, and run the following command.

   Important
   The following commands assume that you specified the Local System account for the Data Access service (`/UseLocalSystemDASAccount`). To specify a domain\user name for these accounts, you must provide the following parameters instead.

   ```
   /DASAccountUser: <domain\username> /DASAccountPassword: <password>
   ```

   ```
   setup.exe /silent /upgrade
   /UseLocalSystemDASAccount
   /DataReaderUser:<domain\user>
   /DataReaderPassword:<domain\user>
   ```

See Also

[How to Upgrade a Gateway Server from Operations Manager 2007 R2]

[How to Upgrade Agents from Operations Manager 2007 R2]

[Upgrading a Distributed Operations Manager 2007 R2 Environment]

[Upgrade Path Checklists for Operations Manager]

How to Upgrade a Gateway Server from Operations Manager 2007 R2

After you upgrade the secondary management server, you upgrade any gateway servers. The procedure to upgrade a gateway server from System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager is performed locally on the gateway server. You can then verify whether the upgrade is successful.

For more information about each upgrade path and the order in which to perform each upgrade task, see the Upgrade Path Checklists for Operations Manager.

Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to

add any new servers to your management group before you upgrade. For more information, see Supported Configurations for System Center 2012 – Operations Manager.

To upgrade a gateway server

1. Log on to a computer that hosts the gateway server with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.
2. On the System Center 2012 – Operations Manager media, run **Setup.exe**.
3. In the **Optional Installations** area, click **Gateway management server**.
4. On the **Welcome to the System Center 2012 - Operations Manager Gateway Upgrade Wizard** page, click **Next**.
5. On the **The wizard is ready to begin gateway upgrade** page, click **Upgrade**.
6. On the **Completing the System Center 2012 - Operations Manager Gateway Setup wizard** page, click **Finish**.

To upgrade a gateway server by using the Command Prompt window

1. Log on to a computer that is hosting the gateway server with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the directory to the System Center 2012 – Operations Manager installation media and change directory again to gateway\AMD64, where the MOMGateway.msi file is located.
4. Run the following command where D:\ is the location for the upgrade log file.

```
msiexec /i MOMgateway.msi /qn /l*v D:\logs\GatewayUpgrade.log
```

To verify the gateway server upgrade

1. In the Operations console, in the navigation pane, click the **Administration** button.
2. Under **Device Management**, click **Management Servers**.
3. In the **Management Servers** pane, verify that the value listed in the **Version** column is 7.0.85xx.x, where x is any positive integer.

See Also

Upgrading a Distributed Operations Manager 2007 R2 Environment

Upgrade Path Checklists for Operations Manager

Upgrading Operations Manager 2007 R2 Agents in a Distributed Management Group

You can upgrade System Center Operations Manager 2007 R2 agents in a distributed management group by using the Operations console, or manually, by using the Setup Wizard or by using a command prompt. Determining which option to use depends on how the agents were deployed. For example, you can upgrade agents that were installed by using the Computer and Device Management Wizard (“push-installed agents”) through the Operations console. However, agents that were installed manually (“manually installed agents”) cannot be upgraded this way.

You can use the Upgrade Helper management pack to verify how agents were installed. For more information, see Upgrade Helper Management Pack.

Important
For information about how upgrade works with AVIcode 5.7 agents and .NET Application Performance Monitoring Agents, see Notes for AVIcode 5.7 Customers.

You should upgrade manually installed agents before you run upgrade on the secondary management server. Push-installed agents can be upgraded after you run upgrade on the secondary management server, before you upgrade the management group. You use the Operations Manager 2007 R2 Operations console to upgrade push-installed agents in a distributed topology.

When you move the push-installed agents to a secondary management server by using the Operations console, they are placed in Pending Management, and you must approve the update to upgrade the agents to System Center 2012 – Operations Manager.

For information about how to upgrade agents, see How to Upgrade Agents from Operations Manager 2007 R2

See Also

Upgrading Agents in an Operations Manager 2007 R2 Single-Server Management Group

Upgrading a Distributed Operations Manager 2007 R2 Environment

Upgrade Path Checklists for Operations Manager

How to Upgrade Agents from Operations Manager 2007 R2

The order in which you upgrade agents depends on how they were installed and whether you are upgrading a single-server management group or a distributed management group. For more information, see Upgrading Agents in an Operations Manager 2007 R2 Single-Server Management Group and Upgrading Operations Manager 2007 R2 Agents in a Distributed Management Group.

When you upgrade an agent, the System Center 2012 – Operations Manager installer service runs and is not removed until after the completion of the upgrade. If the agent upgrade fails, you might have to re-install the agent, because the installer service was not properly removed. If you attempt to upgrade the agent again and it fails, you should re-install the agent after you have completed upgrading all features of Operations Manager.

Use the following procedures to upgrade System Center Operations Manager 2007 R2 agents to System Center 2012 – Operations Manager agents.If you are upgrading agents that are deployed to a computer that has other Operations Manager 2007 R2 features installed, you must take the following steps:

- If the agent is installed on a computer that has the Operations Manager 2007 R2 Operations console or web console installed, you must first uninstall the consoles before you upgrade the agents. You can do this by uninstalling **System Center Operations Manager 2007** in **Programs and Features**. You can reinstall these consoles after upgrade is completed.
- If the agent is installed on computer that has an Operations Manager 2007 R2 operational database and at least one Reporting feature (such as the data warehouse server or

Reporting server), uninstall **System Center Operations Manager 2007** in **Programs and Features**. Do not uninstall **System Center Operations Manager 2007 Reporting**.

- If the agent is installed on a computer that is an Operations Manager 2007 R2 secondary management server, you should remove the agents from the management server. After management group upgrade is completed, you should run repair on that management server.

If you have ACS installed, after the agent upgrade is complete, you must manually start the ACS forwarding service and change the startup setting to automatic.

After you upgrade the server hosting ACS and any agents that act as ACS forwarders, you may need to re-enable ACS forwarding on the agents. In Operations console, go to the **Monitoring** workspace and in the navigation pane, select **Microsoft Audit Collection Services**, then expand **Forwarder**, then expand **State View**. If any of your forwarders do not appear, re-enable them. For more information, see How to Enable Audit Collection Services (ACS) Forwarders.

To learn more about each upgrade path and the order in which to perform each upgrade task, see the Upgrade Path Checklists for Operations Manager.

Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see Supported Configurations for System Center 2012 – Operations Manager.

You should also verify that the agents meet the supported configurations for System Center 2012 – Operations Manager. For more information, see Supported Configurations for System Center 2012 - Operations Manager.

Note
If you attempt to upgrade a 32-bit agent that was installed on a 64-bit machine, the upgrade of the agent will fail.

Note
If UAC is enabled, you must run the agent upgrade from an elevated command prompt.

Note
Information about upgraded agents might not appear in the Operations console for up to 60 minutes after performing the upgrade.

Upgrading Push-Installed Agents

To upgrade push-installed Windows agents by using the Operations console

1. If you are upgrading agents in a distributed management group or if you have added a secondary management server, log on to the computer hosting the Operations Manager 2007 R2 Operations console. Use an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 R2 management group.

   If you are upgrading agents in a single-server management group, log on to the computer hosting the Operations Manager Operations console by using an account that is a

member of the Operations Manager Administrators role.

2. In the Operations console, click **Administration**.

   Note
   When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the management server to which you want to connect.

3. In the **Administration** workspace, in the navigation pane under **Device Management**, click **Pending Management**.
4. In the **Pending Management** pane, under **Type: Agent Requires Update**, right-click each agent-managed computer listed, and then click **Approve**.

   Warning
   You should not approve more than 200 agents at one time.

5. In the **Update Agents** dialog box, enter the administrator account credentials, and then click **Update**. The upgrade status is displayed in the **Agent Management Task Status** dialog box.
6. When the upgrade is completed, click **Close**.

Upgrading Manually Installed Agents

To upgrade a manually installed Windows agent by using the Setup Wizard

1. Log on to the computer that hosts the agent with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.
2. Run **Setup.exe** from the System Center 2012 – Operations Manager installation media.
3. On the first page of the Setup Wizard, click **Local agent**. When the **Welcome to the System Center 2012 - Operations Manager Agent Upgrade Wizard** page opens, click **Next**.
4. In the **System Center 2012 - Operations Manager Agent Setup** dialog box, click **Upgrade**. The status page displays the progress of the upgrade.
5. When the **Completing the System Center 2012 - Operations Manager Agent Setup wizard** page appears, click **Finish**.

To upgrade a manually installed Windows agent by using the Command Prompt window

1. Log on to the computer hosting the agent with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change directory to **agent**, and then change directory again to **AMD64**, **i386**, or **ia64**, as appropriate for the current system.
4. Run the following command, where D:\ is the location for the upgrade log file.

   Note
   If you upgrade manually installed agents that also run the AVIcode 5.7 agent (or

earlier versions of the AVICode agent), you must include the option: **NOAPM=1** in the command. For more information, see Install Agent Using the Command Line.

```
msiexec /i MOMAgent.msi /qn /l*v D:\logs\AgentUpgrade.log
```

Verifying Windows Agent Upgrade

To verify the Windows agent upgrade

1. In the Operations console, in the navigation pane, click the **Administration** button.
2. Under **Device Management**, click **Agent Managed**.
3. In the **Agent Managed** pane, verify that the value listed in the **Version** column is 7.0.85xx.x, where x is any positive integer.

   Note
   It can take up to one hour for the console to show the updated version of the agent.

Upgrading UNIX and Linux Agents

To upgrade UNIX and Linux agents in a distributed management group

1. Log on to the root management server hosting the Operations Manager 2007 R2 Operations console with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 R2 management group.
2. In the Operations console, click **Administration**.
3. At the bottom of the navigation pane, select the **Discovery Wizard** link.

   You must initiate the upgrade by running the Discovery Wizard in Operations Manager 2007 R2 on agents that have been moved to a secondary management server that has been upgraded to Operations Manager. There is no **Pending Management** feature for UNIX and Linux agents in either version.
4. In the **Computer and Device Management Wizard**, select **Discovery Type**, select **Unix/Linux Discovery Wizard**, and then click **Next**.
5. On the **Discovery Method** page, click **Add**.
6. On the **Define discovery criteria** page, type the credentials and necessary information to locate the secondary management server, and then click **OK.**
7. On the **Discovery Method** page, click **Add** to add the secondary management server to the **Discovery Scope** list.
8. In the **Management Server** list, select the secondary management server that will monitor the agents.
9. Click **Discover** to initiate system discovery.
10. On the **Discovery results** page, the wizard detects that the agents are already managed and that an upgrade is available. Continue with the upgrade.
11. Click **Done** to close the wizard.

Any existing Run As profiles and Run As accounts continue to have valid configurations. For information about changes to Run As profiles and accounts for UNIX and Linux monitoring in System Center 2012 – Operations Manager, see Accessing UNIX and Linux Computers in System Center 2012 - Operations Manager.

You can specify the resource pool that manages a particular UNIX or Linux computer and allows you to create a resource pool dedicated to managing only UNIX and Linux computers. For more information see Managing Resource Pools for UNIX and Linux Computers.

To upgrade UNIX and Linux agents in a single-server management group by using the Operations console

1. On the management server that was upgraded to System Center 2012 – Operations Manager, configure at least an Agent Maintenance account (for a Run As account) for the predefined UNIX and Linux profiles. Optionally configure other accounts.

   Note

   If any UNIX or Linux agents are not upgraded to the System Center 2012 – Operations Manager version, and a Run As account is configured for a normal user account on the UNIX or Linux computer that uses sudo elevation, the elevation fails under that circumstance. A normal user account does not have root-level access or special permissions, but allows monitoring of system processes and of performance data. For more information about credentials and elevation, see Accessing UNIX and Linux Computers in Operations Manager 2012.

2. Run the **UNIX/Linux Upgrade Wizard**. For more information, see Upgrading and Uninstalling Agents on UNIX and Linux Computers.

To manually upgrade UNIX and Linux agents in a single-server management group

1. Copy the System Center 2012 – Operations Manager agent package to the managed UNIX or Linux computer. The default location of the agent package is C:\Program Files\System Center 2012\Operations Manager\Server\AgentManagement\UnixAgents.
2. Run the appropriate package upgrade command. For example, the following command upgrades the agents on a Linux computer.

   ```
   rpm –Uvh <filename>.rpm
   ```

To verify the UNIX or Linux agent upgrade

1. In the Operations console, in the navigation pane, click the **Administration** button.
2. Under **Device Management**, click **UNIX/Linux Computers**.
3. In the **Agent Managed** pane, verify that the value listed in the **Version** column is 1.2.0-xxx, where x is any positive integer.

   Note

   It can take up to one hour for the console to show the updated version of the

agent.

See Also

Upgrading Agents in an Operations Manager 2007 R2 Single-Server Management Group

Upgrading Operations Manager 2007 R2 Agents in a Distributed Management Group

Upgrading a Distributed Operations Manager 2007 R2 Environment

Upgrade Path Checklists for Operations Manager

How to Upgrade a Management Group from an Operations Manager 2007 R2 RMS

You upgrade your System Center Operations Manager 2007 R2 management group to System Center 2012 – Operations Manager from the root management server (RMS) when the computer hosting the Operations Manager 2007 R2 RMS meets the minimum supported configurations for System Center 2012 – Operations Manager.

You should first upgrade other features, such as secondary management servers, agents, and gateways before running the final upgrade on the management group. For more information about each upgrade path and the order in which to perform each upgrade task, see Upgrade Path Checklists for Operations Manager.

Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see Supported Configurations for System Center 2012 – Operations Manager.

If the computer hosting the RMS does not meet the minimum supported configurations, you must run upgrade from a secondary management server. For more information, see How to Upgrade a Management Group from an Operations Manager 2007 R2 Secondary Management Server.

To upgrade a management group from an RMS

1. Log on to the computer that hosts the root management server with an account that is a member of the Operations Manager Administrators role for your Operations Manager 2007 R2 management group and a local administrator on the computer. You also require SQL Server Administrator rights on both the operational database server and the data warehouse server.
2. On the System Center 2012 – Operations Manager media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started**, **System Center 2012 - Operations Manager Upgrade** page, review the features that will be upgraded and added, and click **Next**.

   Important
   The Operations Manager data warehouse will be added if it does not already exist.
4. On the **Getting Started**, **Please read the license terms** page, review the license terms and select the option **I have read, understood, and agree with the license terms**, and

then click **Next**.

5. On the **Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager**, or type in a new location or browse to one. Then click **Next**.
6. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.

   Note
   SQL Server Full Text Search must be enabled. For more information, see Full-text Search Overview.
7. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
8. If a data warehouse was not already installed, it is created, and you must configure it as follows:
   a. In the **Configuration**, **Configure the data warehouse database** page, type the name and instance of the SQL Server database server for the database server that will host the System Center 2012 – Operations Manager data warehouse database in the **Server name and instance name** box.
   b. Accept the default value of **Create a new data warehouse database** or select an existing data warehouse.
   c. In the **Database name**, **Database size (MB) Data file folder**, and **Log file folder** boxes, we recommend that you accept the default values. Click **Next**.

      Note
      These paths do not change if you connect to a different instance of SQL Server.
9. On the **Configuration**, **Configure Operations Manager accounts** page, we recommend that you use the **Domain Account** option for the **System Center Configuration service and System Center Data Access service** accounts. Before the account is validated, an error icon appears to the left of the **Domain\Username** box.
10. Enter the credentials for a domain account in each box. The error icons disappear after account validation. Click **Next**.
11. On the **Configuration**, **Ready To Upgrade** page, click **Upgrade**.
12. When the upgrade is finished, the **Upgrade complete** page appears. Click **Close**.

To upgrade a management group from an RMS by using the Command Prompt window

1. Log on to the computer that hosts the root management server with an account that is a member of the Operations Manager Administrators role for your Operations Manager 2007 R2 management group and a local administrator on the computer. You also need SQL Server Administrator rights on both the operational database server and the data warehouse server.
2. Open a Command Prompt window by using the **Run as administrator** option.

3. Change the path to where the System Center 2012 – Operations Manager Setup.exe file is located.

   Important
   The following commands assume that you specified the Local System account for the Data Access service (`/UseLocalSystemDASAccount`). To specify a domain\user name for these accounts, you must provide the following parameters instead.

   ```
   /DASAccountUser: <domain\username> /DASAccountPassword: <password>
   ```

   If you installed a data warehouse in your Operations Manager 2007 R2 management group, use the following command.

   ```
   setup.exe /silent /upgrade
   /AcceptEndUserLicenseAgreement
   /UseLocalSystemDASAccount
   /DataReaderUser:<domain\user>
   /DataReaderPassword:<domain\user>
   ```

   If you did not install a data warehouse in your Operations Manager 2007 R2 management group, use the following command.

   ```
   Setup.exe /silent /upgrade
   /AcceptEndUserLicenseAgreement
   /UseLocalSystemDASAccount
   /DWSqlServerInstance:<server\instance>
   /DWDatabaseName:<DW name>
   /DataReaderUser:<domain\username>
   /DataReaderPassword:<password>
   /DataWriterUser:<domain\username>
   /DataWriterPassword:<password>
   ```

See Also

Upgrading a Distributed Operations Manager 2007 R2 Environment

Upgrade Path Checklists for Operations Manager

How to Upgrade a Management Group from an Operations Manager 2007 R2 Secondary Management Server

You upgrade your System Center Operations Manager 2007 R2 management group to System Center 2012 – Operations Manager from a secondary management server when the computer hosting the Operations Manager 2007 R2 root management server (RMS) does not meet the minimum supported configurations for System Center 2012 – Operations Manager. For more

information, see Supported Configurations for System Center 2012 - Operations Manager. You must first move the agents over to the secondary management server and gateway servers. For more information, see How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade).

Important

If you have a clustered Operations Manager 2007 R2 RMS, you might receive an error during the prerequisite check that indicates that the root management server still has devices reporting to it, even if you have moved the agents to a secondary management server. To resolve this, open the Operations console, and select the **Administration** workspace. In **Device Management**, select **Agentless Managed**. Right-click the agentless nodes, and then click **Delete**.

Note

Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see Supported Configurations for System Center 2012 – Operations Manager.

You should first upgrade other features, such as secondary management servers, agents, and gateways before running the final upgrade on the management group. If you have more than one secondary management server in your management group, we recommend that you upgrade from the secondary management server that has the simplest configuration. For example, if you have a management server that does not have any gateways, agents, or network devices, run upgrade from that management server. For more information about each upgrade path and the order in which to perform each upgrade task, see Upgrade Path Checklists for Operations Manager.

If the computer hosting the RMS meets the minimum supported configurations, you can run upgrade on that server. For more information, see How to Upgrade a Management Group from an Operations Manager 2007 R2 RMS.

When you run upgrade from the secondary management server, the management server is marked as the RMS emulator, and the unsupported RMS is removed from the management group. The RMS emulator enables legacy management packs that rely on the RMS to continue to function in System Center 2012 – Operations Manager.

Important

You must restore the encryption key on the secondary management server before you attempt to upgrade the management group. For more information, see Restore the Encryption Key on the Secondary Management Server

To upgrade a management group from a secondary management server

1. Log on to the computer that hosts the secondary management server with an account

that is a member of the Operations Manager Administrators role for your Operations Manager 2007 R2 management group and a local administrator on the computer. You also need SQL Server Administrator rights on both the operational database server and the data warehouse server.

2. Open a Command Prompt window as an administrator by using the **Run as administrator** feature.
3. Change to the path of the System Center 2012 – Operations Manager Setup.exe file, and run the following command.

```
setup.exe /upgrademanagementgroup
```

4. When the **System Center 2012 - Operations Manager** wizard opens, click **Install**.
5. On the **Getting Started**, **System Center 2012 - Operations Manager Upgrade** page, review the features that will be upgraded and added, and click **Next**.

   Important
   The Operations Manager data warehouse is added if it does not already exist.
   The Operations Manager 2007 R2 root management server is removed from the management group.

6. On the **Getting Started**, **Please read the license terms** page, review the license terms and select the option **I have read, understood, and agree with the license terms**, and then click **Next**.
7. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.

   Important
   If there are any issues with the upgrade, such as having agents still reporting to the RMS, the **Prerequisites** page appears with information about the issue and how to resolve it.

8. If the Prerequisites checker does not return any warnings or errors the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
9. If a data warehouse was not already installed, it is created, and you must configure it as follows:
   a. In the **Configuration**, **Configure the data warehouse database** page, type the name and instance of the SQL Server database server that will host the Operations Manager data warehouse database in the **Server name and instance name** box.
   b. Accept the default value of **Create a new data warehouse database**.
   c. In the **Database name**, **Database size (MB) Data file folder**, and **Log file folder** boxes, we recommend that you accept the default values. Click **Next**.

      Note
      These paths do not change if you connect to a different instance of SQL Server.

10. On the **Configuration**, **Configure Operations Manager accounts** page, we

recommend that you use the **Domain Account** option for the **System Center Configuration service and System Center Data Access service** accounts, the **Data Reader account** and **Data Writer account**. Before the account is validated, an error icon appears to the left of the **Domain\Username** box.

11. Enter the credentials for a domain account in each box. The error icons disappear after account validation. Click **Next**.
12. If Windows Update is not enabled on the computer, the **Configuration**, **Microsoft Update** page appears. Select your options, and then click **Next**.
13. Review the options on the **Configuration**, **Ready to Upgrade** page, and then click **Upgrade**.
14. When the upgrade is finished, the **Upgrade complete** page appears. Click **Close**.

To upgrade a management group from a secondary management server by using the Command Prompt window

1. Log on to the computer that hosts the secondary management server with an account that is a member of the Operations Manager Administrators role for your Operations Manager 2007 R2 management group and a local administrator on the computer.
2. Open a Command Prompt window as an administrator by using the **Run as administrator** option.
3. Change the path to where the System Center 2012 – Operations Manager Setup.exe file is located.

   Important
   The following commands assume that you specified the Local System account for the Data Access service (`/UseLocalSystemDASAccount`). To specify a domain\user name for these accounts, you must provide the following parameters instead:

   ```
   /DASAccountUser: <domain\username> /DASAccountPassword: <password>
   ```

   If you installed a data warehouse in your Operations Manager 2007 R2 management group, use the following command.

   ```
   setup.exe /silent /upgrademanagementgroup
   /AcceptEndUserLicenseAgreement
   /UseLocalSystemDASAccount
   ```

   If you did not install a data warehouse in your Operations Manager 2007 R2 management group, use the following command.

   ```
   setup.exe /silent /upgrademanagementgroup
   /AcceptEndUserLicenseAgreement
   /UseLocalSystemDASAccount
   /DWSqlServerInstance:<server\instance>
   /DataReaderUser:<domain\username>
   ```

```
/DataReaderPassword:<password>
/DataWriterUser:<domain\username>
/DataWriterPassword:<password>
```

See Also

Upgrading a Distributed Operations Manager 2007 R2 Environment

Upgrade Path Checklists for Operations Manager

Upgrading or Installing Optional Features

When you upgrade to System Center 2012 – Operations Manager, there are optional features, such as a stand-alone operations console, web console, Reporting server, and ACS collector that you might want to upgrade. If they were not already installed in the System Center Operations Manager 2007 R2 management group, you might want to install the System Center 2012 – Operations Manager versions after you have completed upgrade.

Important

If you have a Reporting server installed on a root management server (RMS) that does not meet the supported configuration for System Center 2012 – Operations Manager, you will not be able to upgrade it. Instead, you can install a System Center 2012 – Operations Manager Reporting server after you have upgraded your management group.

The following list provides links to optional features you can upgrade.

- How to Upgrade a Stand-Alone Operations Console from Operations Manager 2007 R2
- How to Upgrade a Web Console from Operations Manager 2007 R2
- How to Upgrade Reporting from Operations Manager 2007 R2
- How to Upgrade an ACS Collector from Operations Manager 2007 R2

The following list provides links to optional features you can install.

- How to Install the Operations Console
- How to Install the Operations Manager Web Console
- How to Install the Operations Manager Reporting Server
- How to Deploy ACS on a Secondary Management Server

How to Upgrade a Stand-Alone Operations Console from Operations Manager 2007 R2

This procedure upgrades a stand-alone Operations console from System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager. Perform this procedure locally on the computer that has a stand-alone Operations console installed. You should only upgrade stand-alone Operations consoles after you have upgraded your management group. You do not have to perform this procedure to upgrade Operations consoles that are installed locally on a management server. For more information about each upgrade path and the order in which to perform each upgrade task, see Upgrade Path Checklists for Operations Manager.

Before you proceed, ensure that your server meets the minimum supported configurations for System Center 2012 – Operations Manager. For more information, see Supported Configurations for System Center 2012 - Operations Manager.

To upgrade a stand-alone Operations console

1. Log on to the computer that hosts the Operations console with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.
2. On the Operations Manager source media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started**, **System Center 2012 - Operations Manager Upgrade** page, click **Next**.
4. On the **Getting Started**, **Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager**, or type in a new location or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that are returned by the Prerequisites checker, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration**, **Ready To Upgrade** page, click **Upgrade**.
8. When the upgrade is finished, the **Upgrade complete** page appears. Click **Close**.

To upgrade a stand-alone Operations console by using the Command Prompt window

1. Log on to the computer that hosts the Operations console with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change to the path to the System Center 2012 – Operations Manager source media, and run the following command.

```
Setup.exe /silent /upgrade
```

To verify the Operations console upgrade

1. On the Windows desktop, click **Start**, and then click **Run**.
2. Type **regedit**, and then click **OK**. The Registry Editor starts.

   Caution
   Incorrectly editing the registry can severely damage your system. Before you make changes to the registry, you should back up any valued data that is on the computer.
3. Browse to the **HKey_Local_Machine\Software\Microsoft\Microsoft Operations Manager\3.0\Setup** key. If the value of the **UIVersion** entry is **7.0.85##.#**, where # is any positive integer, the Operations console was upgraded successfully.

See Also

Upgrading a Distributed Operations Manager 2007 R2 Environment

Upgrade Path Checklists for Operations Manager

How to Upgrade a Web Console from Operations Manager 2007 R2

If you have a stand-alone System Center Operations Manager 2007 R2 web console server, you can upgrade it to System Center 2012 – Operations Manager. If your web console server was on the same computer as a secondary management server that was upgraded, you must re-install the web console. For more information, see How to Install the Operations Manager Web Console.

Note

When you upgrade the web console, any customizations that were made to the web.config file after the web console was installed will be reset.

For more information about each upgrade path and the order in which to perform each upgrade task, see Upgrade Path Checklists for Operations Manager.

Before you proceed, ensure that your server meets the minimum supported configurations for System Center 2012 – Operations Manager. For more information, see Supported Configurations for System Center 2012 - Operations Manager.

To upgrade the web console server

1. Log on to the computer that hosts the web console server with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.
2. On the System Center 2012 – Operations Manager source media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started**, **System Center 2012 - Operations Manager Upgrade** page, review the features that will be upgraded, and then click **Next**.
4. On the **Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager**, or type in a new location or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
7. If the root management server has not been upgraded or is unavailable, the **Configuration**, **Specify a management server** page appears. Enter the name of a System Center 2012 – Operations Manager management server that is to be used by the web console, and then click **Next**.
8. On the **Configuration**, **Specify a web site for use with the Web console** page, select the **Default Web Site**, or the name of an existing website. Select **Enable SSL** only if the website has been configured to use Secure Sockets Layer (SSL), and then click **Next**.
9. On the **Configuration**, **Select an authentication mode for use with the Web console** page, select your options, and then click **Next**.

10. When the **Ready to Upgrade** page appears, review the upgrade summary, and then click **Upgrade**.

To upgrade the web console server by using the Command Prompt window

1. Log on to the computer that hosts the web console server with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the System Center 2012 – Operations Manager Setup.exe file is located, and run the following command.

   Important
   Use the `/WebConsoleUseSSL` parameter only if your website has Secure Sockets Layer (SSL) activated. For a default web installation, specify **Default Web Site** for the `/WebSiteName` parameter.

   Note
   If the web console reports to an unsupported or inaccessible root management server, you must also pass the following parameter: /ManagementServer:<servername>.

```
setup.exe /silent /upgrade
/WebsiteName: "<WebSiteName>" [/WebConsoleUseSSL]
/WebConsoleAuthorizationMode: [Mixed|Network]
```

See Also

Upgrading a Distributed Operations Manager 2007 R2 Environment

Upgrade Path Checklists for Operations Manager

How to Upgrade Reporting from Operations Manager 2007 R2

Use this procedure to upgrade a stand-alone Reporting server from System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager. You run upgrade on the Reporting server after you have upgraded the management group. For more information about each upgrade path and the order in which to perform each upgrade task, see Upgrade Path Checklists for Operations Manager.

Before you proceed, ensure that your server meets the minimum supported configurations for System Center 2012 – Operations Manager. For more information, see Supported Configurations for System Center 2012 - Operations Manager.

If you upgraded your management group from the secondary management server, the System Center Operations Manager 2007 R2 root management server (RMS) was removed during the upgrade process. As a result, you will have to manually edit the configuration file for the Reporting server (rsreportserver.config). If you attempt to upgrade Operations Manager Reporting

without making this change, the Upgrade Wizard will report a critical prerequisite issue, because Operations Manager is unable to connect to the reporting server.

Important
If you upgraded your management group from the RMS, then you do not have to manually update the configuration file for the Reporting server.

To Modify the Reporting Server Configuration File

1. On computer that hosts the Reporting server you plan to upgrade, open the **rsreportserver.config** file using Notepad. The path is typically **C:\Program Files\Microsoft SQL Server\MSRS10.MSSQLServer\Reporting Services\ReportServer**, where MSSQLServer is the name of the SQL Server instance.
2. From the **Edit** menu, click **Find**. Search for **<ServerName>**.

   Note
   The <ServerName> element appears in two places in the configuration file, in the Security Extension and in the Authentication Extension.
3. Replace the name of the management server from the old RMS name, with the name of an upgraded management server.
4. Search for **<ServerName>** again, and update the server name.
5. Save and close the configuration file.
6. If the Setup wizard is open, you should close it and restart the upgrade process.

To upgrade the Reporting server

1. Log on to the computer that hosts the Reporting server with an account that is a member of the Operations Manager 2007 R2 Administrators role for your Operations Manager 2007 R2 management group.
2. On the System Center 2012 – Operations Manager source media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started**, **System Center 2012 - Operations Manager Upgrade** page, review the features that will be upgraded. In this case, it is Operations Manager 2007 R2 Reporting. Click **Next**.
4. On the **Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager**, or type in a new location or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites**, **Proceed with Setup** page appears. Click **Next**.
7. If the root management server has not been upgraded or is unavailable, the **Configuration**, **Specify a management server** page appears. Enter the name of a System Center 2012 – Operations Manager management server that is to be used by the

Reporting server, and then click **Next**.

8. On the **Ready to Upgrade** page, review the options, and then click **Upgrade**.
9. When upgrade is finished, the **Upgrade complete** page appears. Click **Close**.

To upgrade the Reporting server by using the command prompt

1. Log on to the computer that hosts the Reporting server with an account that is a member of the Operations Manager 2007 R2 Administrators role for your Operations Manager 2007 R2 management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the System Center 2012 – Operations Manager Setup.exe file is located, and run the following command:

   Note
   If the Reporting server reports to an unsupported or inaccessible root management server, you must also pass the following parameter:
   `/ManagementServer: <ManagementServerName>.`

   ```
   setup.exe /silent /upgrade
   ```

See Also

Upgrading a Distributed Operations Manager 2007 R2 Environment

Upgrade Path Checklists for Operations Manager

How to Upgrade an ACS Collector from Operations Manager 2007 R2

Perform this procedure to upgrade the Audit Collection Services (ACS) Collector from System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager locally on the ACS Collector. During this procedure, the ACS database is also upgraded without any additional steps.

Note
A computer that hosts an ACS Collector must also be an Operations Manager management server or gateway server. You must upgrade the management servers before you upgrade the ACS Collector. For more information about each upgrade path and the order in which to perform each upgrade task, see Upgrade Path Checklists for Operations Manager.

Before you proceed, ensure that your server meets the minimum supported configurations for System Center 2012 – Operations Manager. For more information, see Supported Configurations for System Center 2012 - Operations Manager.

To upgrade an ACS Collector

1. Log on to the computer that hosts the ACS Collector with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.

2. On the System Center 2012 – Operations Manager media, run **Setup.exe**.
3. In the **Install** section, click **Audit collection services**. The Audit Collection Services Collector Setup wizard starts.
4. On the **Welcome to the Audit Collection Services Collector Setup Wizard** page, click **Next**.
5. In the **ACS Collector Maintenance** page, select Update the ACS collector configuration, and then click **Next**.
6. On the **Database Installation Options** page, select **Use an existing database**, and then click **Next**.
7. On the **Data Source** page, type the name that you used as the Open Database Connectivity data source name for your ACS database in the **Data source name** box. By default, this name is **OpsMgrAC**. Click **Next**.
8. On the **Database** page, if the database is on a separate server than the ACS Collector, click **Remote Database Server**, and then type the computer name of the database server that will host the database for this installation of ACS. Otherwise, click **Database server running locally**, and then click **Next**.
9. On the **Database Authentication** page, select one authentication method. If the ACS Collector and the ACS database are members of the same domain, you can select **Windows authentication**; otherwise, select **SQL authentication**, and then click **Next**.

   Note
   If you select **SQL Server Authentication** and click **Next**, the **Database Credentials** page appears. Enter the name of the user account that has access to the SQL Server in the **SQL login name** box and the password for that account in the **SQL password** password box, and then click **Next**.
10. The **Summary** page displays a list of actions that the installation program will perform to upgrade ACS. Review the list, and then click **Next** to begin the installation.

    Note
    If a **SQL Server Login** dialog box appears and the database authentication is set to **Windows Authentication**, select the correct database, and then verify that the **Use Trusted Connection** check box is selected. Otherwise, clear it, enter the SQL Server login name and password, and then click **OK**.
11. When the upgrade is finished, click **Finish**.

See Also

Upgrading a Distributed Operations Manager 2007 R2 Environment

Upgrade Path Checklists for Operations Manager

Post-Upgrade Tasks when Upgrading from Operations Manager 2007 R2

After you have completed the upgrade process for System Center 2012 – Operations Manager, you must perform a number of post-upgrade tasks.

Post-Upgrade Tasks

The following table shows the tasks that you need to complete after you have upgraded to System Center 2012 – Operations Manager. It also indicates when to perform the task.

Task	When to the Perform Task
Re-enable the Notification Subscriptions.	After you complete the upgrade tasks in any upgrade path.
Restart or Re-enable the Connector Services	After you complete the upgrade tasks in any upgrade path, and only if the connector services are installed.
Uninstall the Old RMS	Only if you upgrade the management group on the secondary management server.
Update Overrides	After you upgrade the management group
Verify That the Upgrade Was Successful	After you complete the upgrade tasks in any upgrade path.
Run SQL Query on each Management Group	Run SQL query on each management group to clean up the Localizedtext table and the Publishmessage table.
Assign UNIX/Linux Agents to a Resource Pool	After you complete the upgrade tasks in any upgrade path.

Re-enable the Notification Subscriptions.

After the upgrade has finished, use the following procedure to re-enable subscriptions.

To re-enable the subscriptions

1. Open the Operations console by using an account that is a member of the Operations Manager Administrators role for the System Center 2012 – Operations Manager management group.
2. In the Operations console, in the navigation pane, click the **Administration** button.

   Note
   When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** text box, type the name of the System Center 2012 – Operations Manager management server to which you want to connect.
3. In the **Administration** pane, under **Notifications**, click **Subscriptions**.
4. In the **Actions** pane, click **Enable** for each subscription listed.

Restart or Re-enable the Connector Services

Refer to the third-party documentation for any installed connectors to determine if the connectors are supported for System Center 2012 – Operations Manager.

To restart a connector service

1. On the taskbar, click **Start**, click **Administrative Tools**, and then click **Services**.
2. In the **Name** column, right-click the connector that you want to restart, and then click **Start**.

Uninstall the Old RMS

If you have upgraded to System Center 2012 – Operations Manager from the secondary management server because the RMS did not meet the supported configurations for System Center 2012 – Operations Manager, the RMS is removed from the management group during upgrade. You can then uninstall the old root management server (RMS).

Note
If you upgraded from the secondary management server, you can build a new management server with the same Windows computer name as the old RMS, rather than change the configuration settings to point to the new management server.

To uninstall the old RMS

1. Log on to the computer hosting the RMS with an account that has local administrator permissions.
2. On the taskbar, click **Start**, and then click **Control Panel**, and then run **Programs and Features**.
3. Right-click Operations Manager 2007 R2, and then click **Uninstall**.
4. In the **Program and Features** dialog box, click **Yes** to confirm that you want to uninstall.

Update Overrides

If you created any overrides for the Active Directory Integration rules, you must recreate them after the management group upgrade is complete. Delete the old override, and then create a new, matching override that targets the Active Directory Assignment Resource Pools.

Verify That the Upgrade Was Successful

Perform the following tasks to verify that the upgrade was successful.

- Check the health state of the management servers and agents in the Health Service Watcher state view. In the **Administration** workspace of the Operations console, ensure that the management servers and agents are healthy. In the **Monitoring** workspace, check if there are any alerts related to the management group health.
- Review the event logs of all the management servers for new errors.
- Sort alerts by the last-modified column to review the new alerts.
- Check the CPU utilization and disk I/O on your database servers to ensure that they are functioning normally.

- If the Reporting feature is installed, click Reporting, and then run a generic performance report to ensure that Reporting is functioning correctly.
- Re-deploy any agents that you uninstalled during the upgrade process.

Run SQL Query on each Management Group

Run the following SQL query on the Operational database in each management group to clean up the Localizedtext table and the Publishmessage table.

```
-- Create a temporary table to quickly find a PublisherId when you know the MessageId.
BEGIN TRY
CREATE TABLE #PublisherMessageReverseIndex(MessageStringId UNIQUEIDENTIFIER,
   MessageId INT)
CREATE CLUSTERED INDEX #PublisherMessageReverseIndex_CI ON
#PublisherMessageReverseIndex(MessageStringId)
INSERT INTO #PublisherMessageReverseIndex (MessageStringId, MessageId)
SELECT MessageStringId, MessageId
FROM dbo.PublisherMessages

-- Create a temporary table of message lengths, message IDs, and message hashes with the
-- MessageStringId to quickly determine whether a message is duplicated. Index the table.

CREATE TABLE #LTHashStrings (MessageStringId UNIQUEIDENTIFIER,
 LTValueLen INT,
 LTValueHash VARBINARY(32),
 MessageId INT NULL)
CREATE CLUSTERED INDEX #LTHashStrings_CI ON #LTHashStrings(MessageStringId)
CREATE NONCLUSTERED INDEX #LTHashStrings_NCI1 ON #LTHashStrings(LTValueLen, MessageId,
LTValueHash)

-- Create a temporary table for the orphaned PublisherStrings that you find. Orphaned
PublisherStrings
-- are rows in PublisherMessages whose corresponding events have already been groomed.
They still
-- have corresponding rows in LocalizedText.  Do not add rows for PublisherMessages; they
are not
-- for duplicated messages.
```

```
CREATE TABLE #OrphanedPublisherStrings (PublisherId UNIQUEIDENTIFIER,
MessageStringId UNIQUEIDENTIFIER)
CREATE CLUSTERED INDEX #OrphanedPublisherStrings_CI ON
#OrphanedPublisherStrings(MessageStringId)

-- Create a temporary table so that you can determine whether a PublisherMessages row
still
-- has a corresponding event. These events do not have an index on the PublisherId, so do
-- not query the EventAllView. If a PublisherId occurs multiple times in the event
tables,
-- it is only needed one time in the temp table; therefore, the unique clustered index
-- must contain IGNORE_DUP_KEY. This keeps the temporary table relatively small and saves
-- time when you want to see the orphaned PublisherMessages.

CREATE TABLE #EventAllPublishers (PublisherId UNIQUEIDENTIFIER)
CREATE UNIQUE CLUSTERED INDEX #EventAllPublishers_CI ON #EventAllPublishers (PublisherId)
WITH (IGNORE_DUP_KEY = ON)

-- Populate the temporary table by scanning EventAllView one time.
INSERT INTO #EventAllPublishers(PublisherId)
SELECT PublisherId
FROM EventAllView

-- Populate the first temporary table to determine which messages are duplicated.
INSERT INTO #LTHashStrings (MessageStringId, LTValueLen, LTValueHash, MessageId)
SELECT LTStringId, len(LTValue), HashBytes('SHA1', LTValue), MessageId
FROM dbo.LocalizedText LT
JOIN #PublisherMessageReverseIndex PM ON PM.MessageStringId = LTStringId

-- Create the second table to determine which messages are duplicated.
CREATE TABLE #LTCountByMessage( LTValueLen INT,
MessageId INT,
LTValueHash VARBINARY(32),
```

```
MsgCount INT)
CREATE CLUSTERED INDEX #LTCountByMessage_CI ON #LTCountByMessage(LTValueLen, MessageId,
LTValueHash)

-- Populate second message for duplicate message detection by scanning the INDEX of
-- the first one and by doing a grouped count.
INSERT INTO #LTCountByMessage (LTValueLen, MessageId, LTValueHash, MsgCount)
SELECT LTValueLen, MessageId, LTValueHash, COUNT(1)
FROM #LTHashStrings
GROUP BY LTValueLen, MessageId, LTValueHash

-- You are now set up to detect both orphaned PublisherStrings and duplicated messages
-- by joining to our relatively small (and correctly indexed) temporary tables.
-- Determine the OrphanedPublisherStrings that have duplicate messages.
INSERT INTO #OrphanedPublisherStrings (PublisherId, MessageStringId)
SELECT PM.PublisherId, PM.MessageStringId
FROM dbo.PublisherMessages PM
JOIN #LTHashStrings LTS ON (LTS.MessageStringId = PM.MessageStringId AND LTS.MessageId =
PM.MessageId)
JOIN #LTCountByMessage LTC ON (LTC.LTValueLen = LTS.LTValueLen AND
LTC.MessageId = LTS.MessageId AND LTC.LTValueHash = LTS.LTValueHash)
WHERE PM.PublisherId NOT IN (SELECT PublisherId FROM #EventAllPublishers) AND
LTC.MsgCount > 1

-- Deleting all the OrphanedPublisherStrings and all the corresponding LocalizedText rows
-- at one time may be too large for the transaction log to handle.  Create a numbered
-- or ordered table so that you can delete them in relatively small batches and not
-- overtax the transaction log.
CREATE TABLE #NumberOrphanPublisherStrings(OrphanNum INT IDENTITY,
   PublisherId UNIQUEIDENTIFIER,
   MessageStringId UNIQUEIDENTIFIER)
CREATE CLUSTERED INDEX #NumberOrphanPublisherStrings_CI on
#NumberOrphanPublisherStrings(OrphanNum)
```

```
-- Populate the numbered table.
INSERT INTO #NumberOrphanPublisherStrings (PublisherId, MessageStringId)
SELECT PublisherId, MessageStringId FROM #OrphanedPublisherStrings
END TRY
BEGIN CATCH
GOTO Error
END CATCH

-- Set up variables so that you can delete the orphaned rows.
-- If the transaction log fills up, try to reduce the @OrphanIncrement value,
-- which controls the number of rows that are delete at the same time.
DECLARE @OrphanNum INT
DECLARE @OrphanIncrement INT
DECLARE @OrphanLimit INT
SET @OrphanNum = 0
SET @OrphanIncrement = 10000
SELECT @OrphanLimit = MAX(OrphanNum) FROM #NumberOrphanPublisherStrings
BEGIN TRY
WHILE @OrphanNum < @OrphanLimit
BEGIN
DELETE dbo.LocalizedText FROM
#NumberOrphanPublisherStrings OPS JOIN dbo.LocalizedText LT
ON LT.LTStringId = OPS.MessageStringId
WHERE OPS.OrphanNum >= @OrphanNum AND OPS.OrphanNum < @OrphanNum + @OrphanIncrement
DELETE dbo.PublisherMessages FROM
#NumberOrphanPublisherStrings OPS JOIN dbo.PublisherMessages PM
ON PM.PublisherId = OPS.PublisherId
WHERE OPS.OrphanNum >= @OrphanNum AND OPS.OrphanNum < @OrphanNum + @OrphanIncrement
SET @OrphanNum = @OrphanNum + @OrphanIncrement
END
END TRY
BEGIN CATCH
GOTO Error
END CATCH
```

```
Error:
IF @@ERROR <> 0
   SELECT
        ERROR_NUMBER() AS ErrorNumber,
        ERROR_MESSAGE() AS ErrorMessage;

-- Try to drop all the temporary tables
BEGIN TRY
IF EXISTS (SELECT 1 FROM tempdb.INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME LIKE
'#PublisherMessage%')
DROP TABLE #PublisherMessageReverseIndex
IF EXISTS (SELECT 1 FROM tempdb.INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME LIKE
'#OrphanedPublisherStrings%')
DROP TABLE #OrphanedPublisherStrings
IF EXISTS (SELECT 1 FROM tempdb.INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME LIKE
'#LTHashStrings%')
DROP TABLE #LTHashStrings
IF EXISTS (SELECT 1 FROM tempdb.INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME LIKE
'#EventAllPublishers%')
DROP TABLE #EventAllPublishers
IF EXISTS (SELECT 1 FROM tempdb.INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME LIKE
'#LTCountByMessage%')
DROP TABLE #LTCountByMessage
IF EXISTS (SELECT 1 FROM tempdb.INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME LIKE
'#NumberOrphanPublisherStrings%')
DROP TABLE #NumberOrphanPublisherStrings
END TRY
BEGIN CATCH
   SELECT
        ERROR_NUMBER() AS ErrorNumber,
        ERROR_MESSAGE() AS ErrorMessage;
END CATCH
```

Assign UNIX/Linux Agents to a Resource Pool

After completing the upgrade, UNIX/Linux agents must be assigned to a resource pool to enable highly-available monitoring and agent administration. For more information on creating resource pools, see How to Create a Resource Pool.

1. Open the Operations console by using an account that is a member of the Operations Manager Administrators role for the **om12short** management group.
2. In the Operations console, in the navigation pane, click the **Administration** button.
3. In the **Administration** pane, under **Device Management**, click **UNIX/Linux Computers**.
4. Select the UNIX/Linux computers to assign to a resource pool, and in the **Actions** pane, click **Change Resource Pool**.
5. Complete the **Change Resource Pool** wizard to assign the computers to the selected resource pool.

Upgrading to System Center 2012 - Operations Manager by Using the Command Prompt Window

You can upgrade to System Center 2012 – Operations Manager by using the **setup.exe** command in the Command Prompt window. Gateway and agent upgrades require the use of MOMGateway.msi and MOMAgent.msi. For information about supported configuration requirements of System Center 2012 – Operations Manager, see Supported Configurations for System Center 2012 – Operations Manager.

Command-line Parameters for setup.exe

The following table lists the command-line parameters for installing features of System Center 2012 – Operations Manager.

Note

If the parameter contains a colon, a value is required. Otherwise, it is simply a switch.

Parameter	Value
/silent	Does not display the installation wizard during upgrade.
/upgrade	Used to upgrade all features of Operations Manager, if they meet the minimum supported configuration requirements.
/upgrademanagementgroup	Used to upgrade the management group from the secondary management server if the Root

Parameter	Value
	Management Server does not meet the supported configuration requirements. Used after you have upgraded other features, such as secondary management servers, agents, and gateways.
/UseLocalSystemDASAccount	Used to specify the Local System for the Data Access service account.
/DASAccountUser:	The domain and user name of the Data Access service account. Used if you did not specify the Local System.
/DASAccountPassword:	The password for the Data Access service account. Used if you did not specify the Local System.
/AcceptEndUserLicenseAgreement	Used to specify that you accept the End User License Agreement (EULA). This is only required when you are upgrading the System Center Operations Manager 2007 R2 management group from the Root Management Server (RMS) or the secondary management server.
/ManagementServer:	Used to specify the name of the management server to associate with a web console and/or Reporting server that you are upgrading. Only required if the web console and/or Reporting server is associated with an RMS that cannot be upgraded.
/DWSqlServerInstance:	The data warehouse server and instance (<server\instance>).
/DWDatabaseName:	The name of the data warehouse database.
/DataReaderUser:	The domain and user name of the data reader account.
/DataReaderPassword:	The password for the data reader account.
/DataWriterUser:	The domain and user name of the data writer account.
/DataWriterPassword:	The password for the data writer account.

Parameter	Value
/WebSiteName:	The name of the website. If default web installation, specify "**Default Web Site**". Used for web console upgrades.
/WebConsoleUseSSL	Specify only if your website has Secure Sockets Layer (SSL) activated. Used for web console upgrades.
/WebConsoleAuthorizationMode:	Mixed: Used for intranet scenarios. Network: Used for extranet scenarios. Used for web console upgrades.

For examples of command lines for upgrading the various features of Operations Manager 2007 R2 to System Center 2012 – Operations Manager, see the following:

- How to Upgrade an Operations Manager 2007 R2 Single-Server Management Group
- Upgrading Agents in an Operations Manager 2007 R2 Single-Server Management Group
- How to Upgrade a Secondary Management Server from Operations Manager 2007 R2
- How to Upgrade a Gateway Server from Operations Manager 2007 R2
- How to Upgrade Agents from Operations Manager 2007 R2
- How to Upgrade a Management Group from an Operations Manager 2007 R2 RMS
- How to Upgrade a Management Group from an Operations Manager 2007 R2 Secondary Management Server
- How to Upgrade a Stand-Alone Operations Console from Operations Manager 2007 R2
- How to Upgrade a Web Console from Operations Manager 2007 R2
- How to Upgrade Reporting from Operations Manager 2007 R2

Maintaining the System Center 2012 - Operations Manager Infrastructure

After you have deployed or upgraded to System Center 2012 – Operations Manager, you might want to make changes to your Operations Manager infrastructure, such as backing up or moving a database. This section of the Deploying System Center 2012 - Operations Manager provides information about maintaining your installation of Operations Manager.

- Backup and Disaster Recovery in Operations Manager
- Making Changes to an Operations Manager Environment
- Sending Data to Microsoft

Backup and Disaster Recovery in Operations Manager

As part of your maintenance plan, it is important to include a backup plan. This plan should be thoroughly tested and documented in a simulated environment by using production backups. Ensure that the System Center 2012 – Operations Manager backup plan is integrated in any existing backup procedures in the organization.

Note

Before reading this section, be sure to review Planning the System Center 2012 - Operations Manager Deployment to understand the components of Operations Manager and to learn how to prepare for failure recovery.

Decide on the following issues:

- What to back up
- How often to back up
- Whether to perform complete or incremental backups
- How and when to practice restore procedures

After you decide what the best backup strategies for your System Center 2012 – Operations Manager environment, develop and document a backup plan to become part of the overall disaster recovery plan.

We strongly recommend that you test your backup and restore procedures thoroughly. Testing helps ensure that you have the required backups to recover from various failures and that staff can run the procedures smoothly and quickly if a failure occurs.

You can use a test environment including all the Operations Manager features to test your backup and restore processes.

Note

The overall backup practices in your organization might include backing up the disk drives that the Operations Manager is installed on. When backing up those disk drives, including the management servers, ensure to exclude the <Installed Partition>\Program Files\System Center 2012\Operations Manager\Server\Health Service State folder.

In This Section

Complete and Incremental Backups in Operations Manager

Backup File Naming Conventions in System Center 2012 - Operations Manager

Back Up System Center 2012 - Operations Manager

Complete and Incremental Backups in Operations Manager

You must ensure that database backups are as recent and complete as possible. This topic provides information to help you decide how to incorporate both complete and incremental database backups into an overall backup plan.

Note

By default, the report server database uses a full recovery model. Other Operations Manager databases use a simple recovery model. For more information about backup options, see Backup Overview (SQL Server).

Complete Database Backups

A complete database backup captures the entire database, including all entries in the transaction log, and excluding any unallocated extents in the files. Pages are read directly from disk to increase the speed of the operation.

You can re-create a database from its backup in one step by restoring a backup of the database. The restore process overwrites the existing database or creates the database if it does not exist. The restored database matches the state of the database at the time the backup finished, without any uncommitted transactions. Uncommitted transactions are rolled back when the database is restored.

A complete database backup uses more storage space per backup than transaction log and incremental database backups. Consequently, complete database backups take longer and therefore are typically created less frequently than incremental database or transaction log backups.

Incremental Database Backups

An incremental (differential) database backup records only the data that has changed after the last database backup. You can frequently make incremental backups of a database because incremental database backups are smaller and faster than complete database backups. Making frequent incremental backups decreases your risk of losing data.

In case of database failure, you can use incremental database backups to restore the database to the point at which the incremental database backup was finished.

Transaction Log Backups

The transaction log is a serial record of all the transactions that have been performed against the database after the transaction log was last backed up. With transaction log backups, you can restore the database to a specific point in time (for example, before entering unwanted data) or to the point of failure.

When restoring a transaction log backup, Microsoft SQL Server rolls forward all changes recorded in the transaction log. When SQL Server reaches the end of the transaction log, the state of the database is exactly as it was at the time the backup operation started. If the database is recovered, SQL Server then rolls back all transactions that were incomplete when the backup operation started.

Note

The data warehouse database uses a simple recovery model that truncates all transactions after completion. This means that backing up the log file is insufficient. Perform a complete database file backup.

For more information about recovery models, see Recovery Model Overview.

Backup File Naming Conventions in System Center 2012 - Operations Manager

Correct use of naming conventions for backup files helps you distinguish between them. Backup files are unique based on the management group that they back up and the time that the backup was created. Consistent use of a standard naming convention can help you avoid the unintentional restoration of a backup to the wrong management group or restoring a backup from the wrong time.

Database File Naming Conventions

There might be multiple management groups in your Operations Manager environment; therefore, ensure to include the management group name or some distinguishing name in the database backup file names.

You can also include other information in the file name, such as the database name, date, and type of backup. For example, a file name might be formatted as follows: **OpsMgrDB_DIFFERENTIAL_<management group name>_7_15_2011** or **REPORTING_FULL_<management group name>_7_15_2011**.

Custom Management Pack Naming Conventions

If your monitoring infrastructure consists of multiple management groups, it is very likely that the configuration of management packs and their overrides vary across those management groups. Therefore, implementing a standard naming convention for custom management packs helps prevent the same problems as using a standard naming convention for databases.

Include the management group name or some distinguishing name in the .xml file name for these backups. Also include the version of the sealed management pack for which the custom management pack contains overrides and other information in the file name, such as the date. For example, a file name might be in the following format: **<management group name>_<Management pack name>_<Management pack version>_7_15_2011.xml**.

Back Up System Center 2012 - Operations Manager

To preserve data in case of a failure, you must have a recent backup of System Center 2012 – Operations Manager databases and other important data as listed in this topic.

Data to Back Up

To ensure your ability to correctly preserve and restore your Operations Manager environment, you should back up the following key items:

- Operational database, data warehouse database, and the Audit Collection Services (ACS) database
- Custom management packs
- Custom report definition files and computer certificates
- Recommended Backup Schedule for System Center 2012 - Operations Manager
- How to Back Up Custom Management Packs
- How to Schedule Backups of System Center 2012 - Operations Manager Databases

- Backup and Recovery Using VSS Writer

Recommended Backup Schedule for System Center 2012 - Operations Manager

You should determine how often and when to run backups. In general, you should perform database backups according to your company's backup policy.

Backup Schedule

The following table suggests a schedule for regular backups of your Operations Manager features. These suggestions are specific to your Operations Manager environment and are meant to complement other regularly scheduled backups in your environment.

You should schedule those backup jobs at a time that does not conflict with the schedule of the Operations Manager grooming tasks. The Operations Manager grooming jobs run on the Operations Manager database server and both read from and write to the database. Backing up the database during the same time might cause failures in the backup job, the grooming job, or both.

At a minimum, an incremental backup of the operational database should be performed on a daily basis. A complete backup should be performed on the operational database weekly. The master and msdb databases should be backed up any time a change occurs that affects either database, but you should back them up at least monthly.

Feature to back up	Full backup	Incremental backup
Operational database	Weekly	Daily
Data warehouse database	Monthly	Weekly
Reporting server	On a recurring basis, with the frequency depending on how often reports change in your organization, and every time after significant changes are made to report definitions (including additions, changes, and deletions).	Same as full backup
Audit Collection Services (ACS) database	Monthly	Weekly
Master database (Master)	Every time, after installing and configuring the Operations Manager database features and after making significant changes to logons or other security changes.	Per IT policies
Msdb database (Msdbdata)	After the initial installation and	After changing the scheduled

Feature to back up	Full backup	Incremental backup
	configuration of the Operations Manager database features.	Microsoft SQL Server Agent jobs that Operations Manager uses.
Custom Management Packs (.xml files)	Monthly or after making significant changes to management packs.	Not applicable

How to Back Up Custom Management Packs

Management packs contain monitoring rules for applications and services. Both sealed and unsealed management packs can be customized by superseding their default values using overrides, or by defining custom rules or monitors. Custom management packs are unsealed and are saved to a separate .xml management pack file. Only custom management packs can be exported. By default, the file is saved to the My Default management pack folder.

You should back up custom management packs regularly even though backing up the operational database captures management pack information. When you run management pack backups as an independent operation from database backups, you can re-import them separately from the database, which can be useful in cases when you must roll back the customized changes in one or more custom management packs.

Use the Export feature from the Operations console to back up management packs.

To export a custom management pack

1. Log on to a management server with an account that is a member of the System Center 2012 – Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click **Administration**.
3. In the **Administration** pane, click **Management Packs**.
4. Right-click the custom management pack that you want to export, and then click **Export Management Pack**.
5. In the **Save As** dialog box, type the path and file name for the management pack file, or click **Browse** to save the file to a different directory, and then click **Save**.

How to Schedule Backups of System Center 2012 - Operations Manager Databases

Schedule a Database Backup

Use this procedure to schedule a database backup by using Microsoft SQL Server Management Studio to back up the operational database, the Audit Collection Services (ACS) database, and the data warehouse database.

To schedule a database backup to a file

1. Start SQL Server Management Studio.
2. In the **Connect to Server** dialog box, select the appropriate values in the **Server type** list, in the **Server name** box, and in the **Authentication** box.
3. Click **Connect**.
4. In **Object Explorer**, expand **Databases**.
5. Right-click the database that you want to back up, click **Tasks**, and then click **Back Up**.
6. In the **Back Up Database** dialog box, type the name of the backup set in the **Name** box, and then under **Destination**, click **Add**.
7. In the **Select Backup Destination** dialog box, type a path and a file name in the **Destination on disk** box, and then click **OK**.

   Important
   The destination location must have enough available free disk space to store the backup files based on the frequency of your backup schedule.
8. In the **Script** list, click **Script Action to Job**.
9. If you want to change job parameters, in the **New Job** dialog box, under **Select a page**, click **Steps**, and then click **Edit**.
10. Under **Select a page**, click **Schedules**, and then click **New**.
11. In the **New Job Schedule** dialog box, type the job name in the **Name** box, specify the job schedule, and then click **OK**.

    Note
    If you want to configure alerts or notifications, you can click **Alerts** or **Notifications** under **Select a page**.
12. Click **OK** and **OK**.

Operational Database

The operational database contains almost all of the System Center 2012 – Operations Manager environment configuration settings, agent information, management packs with customizations, operations data, and other data required for Operations Manager to operate correctly.

Important
It is critical that you back up the operational database regularly to preserve the latest information about your Operations Manager environment. A database failure without a recent backup results in the loss of almost all Operations Manager-specific data, and you would have to rebuild the entire Operations Manager environment.

Note
If your backup procedure sets the operational database to be offline during backup, Operations Manager caches incoming data, and then, after backup is completed, Operations Manager stores that data in the database.

Reporting Databases

Operations Manager Reporting uses the following databases:

- Operations Manager data warehouse (data warehouse database)
- SQL Server Reporting Services databases (ReportServer and ReportServerTempDB)

The data warehouse database contains all of the performance and other operational data from your Operations Manager environment. SQL Server Reporting Services then uses this data to generate reports such as trend analysis and performance tracking.

To be able to restore reporting functionality in case of failure, it is critical that you back up the data warehouse database. When determining how often and when to back up this database, you should consider the following:

- This database can grow to a very large size (more than one terabyte) over time.
- Management servers frequently write data to this database.
- IT SLA requirements are based on the requirement for reporting availability in the organization.

Note

The data warehouse database uses a simple recovery model, which truncates all transactions after completion. Therefore, backing up only the log file is insufficient; you must back up the entire database.

The SQL Server Reporting Services databases store report definitions, report metadata, cached reports, and snapshots. In case of failure, you can re-create report definitions by re-importing the reports. However, cached reports, which are reports that have already been created, will be lost.

To be able to restore reporting functionality in case of failure, we recommend that you back up the SQL Server Reporting Services databases.

ACS Database

The Audit Collection Services (ACS) database, OperationsManagerAC, is the central repository for events and security logs that are collected by ACS forwarders on monitored computers.

The Audit Collection Services database can grow significantly depending on how many ACS forwarders send events to the ACS database and the filters configured to control what events are written to the database.

Master Database

The master database is a system database, which records all of the system-level information for a Microsoft SQL Server system, including the location of the database files. It also records all logon accounts and system configuration settings. The appropriate functionality of the master database is key to the operation of all of the databases in an instance of SQL Server.

MSDB Database

The MSDB database, Msdbdata, is a SQL Server system database, which is used by the SQL Server agent to schedule jobs and alerts and for recording operators. The appropriate functionality of the MSDB database is key to the operation of all the databases in an instance of SQL Server.

Note

This database contains task schedules that are vital to the health of the Operations Manager database, and it should be included in your backup plan. You have to back up this database only after you configure Operations Manager or if you change the scheduled agent jobs.

Backup and Recovery Using VSS Writer

With System Center 2012 Service Pack 1 (SP1), Operations Manager, VSS writers offer a shortcut for backing up the Operations Manager and Audit Collection Services databases using the SQL VSS writer, providing an alternative mechanism of selecting what to be backed up, versus using the user interface in Data Protection Manager (DPM) or some other application to select the SQL databases. Backup and restoration can be accomplished with DPM or any other backup application because we employ a generic VSS Writer.

The writer IDs are:

- Audit Collection Service: 2488ec56-996a-4716-8165-7436a683
- Operations Manager: 5ACDEAFF-4A8C-4FCE-BB24-BFCB4CD8A572

The VSS writers make it easy to discover what databases to backup, showing all the SQL data being used by Operations Manager and Audit Collection Service under the respective nodes.

Note

For Disaster recovery you need to follow the instructions at Disaster Recovery in System Center 2012 - Operations Manager with VSS writer based recovery.

Note

You must have local administrative credentials to back up and restore Operations Manager and ACS data stores.

Disaster Recovery in System Center 2012 - Operations Manager

Various System Center 2012 – Operations Manager servers and features can potentially fail, impacting Operations Manager functionality. The amount of data and functionality lost during a failure is different in each failure scenario. It depends on the role of the failing feature, the length of time it takes to restore the failing feature, and on the availability of backups.

You should always keep a backup of your operational database and data warehouse database. For information about scheduling regular backups of the Operations Manager databases, see How to Schedule Backups of System Center 2012 - Operations Manager Databases.

The amount of data and functionality lost during a failure is different in each failure scenario. The impact of failure is minimized if the Operations Manager deployment includes multiple management servers. The impact is greater if only one management server is implemented. This is because you do not have a second management server which can take on the load if one fails, and you will lose all monitoring capabilities. The impact of failure of a management server in a distributed environment is minimized, but it increases the workload on additional management servers in the management group until the failed management server is restored.

Recovering Operations Manager Features

If your Operations Manager databases have failed, you can restore them from back up. For more information, see How to Restore Operations Manager Databases.

If your Operations console, web console, or Reporting server have failed, you must reinstall them. For information on installing these features, see

- How to Install the Operations Manager Web Console
- How to Install the Operations Console
- How to Install the Operations Manager Reporting Server

If one or more management servers have failed, you can recover them by using the **setup.exe** command with a **/recover** switch in Command Prompt window. There are two scenarios for recovery. The first scenario is when you have to recover a management server when all management servers in the management group have failed. In this case, you must recover all of the failed management servers, and then reconfigure the RunAs accounts. The second scenario is when you have a failed management server, but one or more management servers are still online. In this case, you just recover all of the failed management servers. You should not reconfigure the RunAs accounts.

To Recover a Management Server

1. Build a new server, ensuring that it meets the minimum supported configurations for System Center 2012 – Operations Manager, and use the same name that was given to the failed management server.
2. Restore the operational database and data warehouse database, if required. For more information, see How to Restore Operations Manager Databases.
3. On the new server, open a Command Prompt window by using the Run as Administrator option, and run the following command:

   Note
   This process only recovers the management server. If consoles or Reporting were also installed on the failed management server, you must reinstall them after recovery is complete.

   Important
   You must use the same parameter values for account credentials, management group, and database names as the failed server you are trying to recover.

   Important
   The following command assumes that you specified the Local System for the Management server action account (`/UseLocalSystemActionAccount`) and Data Access service (`/UseLocalSystemDASAccount`). To specify a domain\user name for these accounts, you must provide the following parameters instead.

   ```
   /ActionAccountUser: <domain\username> /ActionAccountPassword: <password>

   /DASAccountUser: <domain\username> /DASAccountPassword: <password>
   ```

```
Setup.exe /silent /AcceptEndUserLicenseAgreement
/recover
/EnableErrorReporting:[Never|Queued|Always]
/SendCEIPReports:[0|1]
/UseMicrosoftUpdate:[0|1]
/DatabaseName:<OperationalDatabaseName>
/SqlServerInstance:<server\instance>
/DWDatabaseName:<DWDatabaseName>
/DWSqlServerInstance:<server\instance>
/UseLocalSystemDASAccount
/DatareaderUser:<domain\username>
/DatareaderPassword:<password>
/DataWriterUser:<domain\username>
/DataWriterPassword:<password>
/ActionAccountUser:<domain\username>
/ActionAccountPassword:<password>
```

Setup detects that the server was a prior management server in the management group, and recovers the management server. You must follow these procedures for each failed management server in your management group.

For information about the command-line parameters, see Disaster Recovery Command-line Parameters.

If you have to recover a management server when all management servers in the management group have failed, then you must also reconfigure the RunAs Accounts.

Important

If you have management servers that have not failed, you should not reconfigure the RunAs Accounts.

To Reconfigure the RunAs Accounts

1. In the Operations console, click the **Administration** button.
2. In the **Administration** pane, under **Run As Configuration**, click **Accounts**.
3. In the **Accounts** pane, right-click a Run As account, and then click **Properties**.
4. In the **Run As Account Properties** dialog box, click the **Credentials** tab.
5. Re-enter your credentials for the Run As account and click OK.
6. Repeat these steps for all Run As accounts.

Note

If you are not using SQL Server authentication, you can remove any associations to the **Data Warehouse SQL Server Authentication Account** and **Reporting SDK SQL Server Authentication Account** and then delete these accounts.

If you are not using SQL Server authentication, you can remove the SQL Server Authentication accounts.

To Remove the SQL Server Authentication Accounts

1. In the Operations console, click the **Administration** button.
2. In the **Administration** pane, under **Run As Configuration**, click **Profiles**.
3. In the **Profiles** pane, right-click **Data Warehouse SQL Server Authentication Account**, and then click **Properties**.
4. Click **Run As Accounts** in the right pane, click **Data Warehouse SQL Server Authentication Account**, and then click **Remove**.
5. Click **Save**, and then click **Close**.
6. In the **Profiles** pane, right-click **Reporting SDK SQL Server Authentication Account**, and then click Properties.
7. Click **Run As Accounts** in the right pane, click **Reporting SDK SQL Server Authentication Account**, and then click **Remove**.
8. Click **Save**, and then click **Close**.
9. In the **Administration** pane, under **Run As Configuration**, click **Accounts**.
10. In the **Profiles** pane, right-click **Data Warehouse SQL Server Authentication Account**, and then click **Delete**.
11. In the **Profiles** pane, right-click **Reporting SDK SQL Server Authentication Account**, and then click **Delete**.

See Also

Backup and Disaster Recovery in Operations Manager

Disaster Recovery Command-line Parameters

Disaster Recovery Command-line Parameters

You can recover one or more management servers by using the **setup.exe** command in the Command Prompt window.

Command-line Parameters

The following table lists the command-line parameters for recovering an System Center 2012 – Operations Manager management server.

Note

If the parameter contains a colon, a value is required. Otherwise, it is simply a switch.

Parameter	Value
/silent	Required parameter. Runs the installation wizard without displaying the user interface
/recover	Recovers a management server.
/ManagementGroupName:	Optional. The name of the management group
/SqlServerInstance:	The SQL server and instance (<server\instance>).
/DatabaseName:	The name of the Operational database.
/DWSqlServerInstance:	The data warehouse server and instance (<server\instance>).
/DWDatabaseName:	The name of the data warehouse database.
/UseLocalSystemActionAccount	Used to specify the Local System for the Management server action account.
/ActionAccountUser:	The domain and user name of the Management server action account. Used if you do not want to specify the Local System
/ActionAccountPassword:	The password for the Management server action account. Used if you do not want to specify the Local System.
/UseLocalSystemDASAccount	Used to specify the Local System for the Data Access service account.
/DASAccountUser:	The domain and user name of the Data Access service account. Used if you do not want to specify the Local System.
/DASAccountPassword:	The password for the Data Access service account. Used if you do not want to specify the Local System.
/DataReaderUser:	The domain and user name of the data reader account.
/DataReaderPassword:	The password for the data reader account.

Parameter	Value
/DataWriterUser:	The domain and user name of the data writer account.
/DataWriterPassword:	The password for the data writer account.
/EnableErrorReporting:	Never: Do not opt in to sending automatic error reports. Queued: Opt in to sending error reports, but queue the reports for review before sending. Always: Opt in to automatically send error reports.
/SendCEIPReports:	0 : Do not opt in to the Customer Experience Improvement Program (CEIP). 1 : Opt in to CEIP.
/UseMicrosoftUpdate:	0 : Do not opt in to Microsoft Update. 1 : Opt in to Microsoft Update.
/AcceptEndUserLicenseAgreement	Used to specify that you accept the End User License Agreement (EULA).

See Also

Disaster Recovery in System Center 2012 - Operations Manager

How to Restore Operations Manager Databases

Use the following procedure to restore a System Center 2012 – Operations Manager database using Microsoft SQL Server Management Studio. This procedure applies to databases on SQL Server 2008 R2 and SQL Server 2008 R2 SP1.

Note

If you want to resize the operational database, you must resize it by using SQL Server. For more information, see Microsoft SQL Server in the TechNet Library.

To restore a database backup

1. Start SQL Server Management Studio.
2. In the **Connect to Server** dialog box, select the appropriate values in the **Server type** drop-down combo box, in the **Server name** box, and in the **Authentication** box.
3. Click **Connect**.
4. In **Object Explorer**, expand **Databases**, and then select the **OperationsManager**, **OperationsManagerAC**, or **OperationsManagerDW** database.

5. Right-click the database, point to **Tasks**, and then click **Restore**.
6. Click **Database** to open the **Restore Database** dialog box.
7. On the **General** page, the name of the restoring database appears in the **To database** list.
8. In the **To a point in time** text box, either retain the default (**the most recent possible**) or select a specific date and time by clicking the browse button, which opens the **Point in Time Restore** dialog box.
9. To specify the source and location of the backup sets to restore, click the **From Device** option.
10. Click **Browse** to open the **Specify Backup** dialog box.
11. In the **Backup media** list box, select one of the listed device types. To select one or more devices for the Backup location list box, click **Add**.
12. In the **Select the backup sets to restore** grid, select the backups to restore. This grid displays the backups available for the specified location.
13. In the **Restore options** panel, select the **Overwrite the existing database** option.
14. In the **Restore the database files as** options panel, verify the original database file name and path are correct.
15. For the **Recovery state** options, specify the state option **Leave the databases ready to use by rolling back the uncommitted transactions**. Additional transaction logs cannot be restored.
16. Click **OK** to restore the database.

Making Changes to an Operations Manager Environment

After the initial deployment of System Center 2012 – Operations Manager, you might need to make changes or upgrades to the original deployment for reasons such as the following:

- You need to replace hardware that is experiencing problems and that is no longer considered reliable.
- You need to replace hardware as part of the upgrade process from System Center Operations Manager 2007 R2.
- You need to add additional hardware to improve scalability and performance.
- You need to move a database and log file to a different volume because of space or performance reasons.
- You need to change hardware that is leased and is due to expire soon.
- You need to change or upgrade hardware to comply with new hardware standards.
- You initially installed multiple Operations Manager features on a single server and you need to distribute some components to other servers.
- You need to restore functionality in a failure scenario.

Operations Manager supports changes to your Operations Manager infrastructure as listed below. Be cautious when performing these operations because they can result in data loss if not performed correctly.

- Account Information for Operations Manager
- How to Uninstall Operations Manager
- How to Manage the Report Server Unattended Execution Account
- How to Configure the Internet Proxy Settings for a Management Server
- How to Move the Operational Database
- How to Move the Data Warehouse Database
- How to Move the Audit Collection Database
- How to Move the Reporting Server Role
- How to Remove the Management Server Role
- Removing a Gateway Server from a Management Group
- How to Remove Certificates Imported with MOMCertImport

See Also

Maintaining the System Center 2012 - Operations Manager Infrastructure

Account Information for Operations Manager

During the setup and operation of System Center 2012 – Operations Manager, you are asked to provide credentials for several accounts. This section provides information about the various accounts and how to change the credentials or passwords for the accounts after a deployment.

- Action Accounts
- Service Accounts
- Agent Installation Account
- Data Warehouse Write Account
- Data Reader Account

Action Accounts

The Operations Manager management server, gateway server, and agent, all contain a process called MonitoringHost.exe. MonitoringHost.exe is used to accomplish monitoring activities, such as running a monitor or a task. For example, when an agent subscribes to the event log to read events, it is the MonitoringHost.exe process that runs those activities. The account that a MonitoringHost.exe process runs as is called the action account. The action account for the MonitoringHost.exe process that is running on an agent is called the agent action account. The action account used by the MonitoringHost.exe process on a management server is called the management server action account. The action account used by the MonitoringHost.exe process on a gateway server is called the gateway server action account.

When you validate or change the default action account, you must ensure that the account you are using for your default Action Account is configured to be a **Role** member of the **ConfigServiceMonitoringUsers** database role.

To validate the Action Account

1. On the server that hosts the operational database, open SQL Server Management Studio and connect to the local server.
2. Expand **Databases**, and then expand the operational database, which by default is **OperationsManager**.
3. Expand **Security**, then **Roles**, and then **Database Roles**.
4. Verify that the **ConfigServiceMonitoringUsers** role is listed.
5. If this role is not listed, you can right-click **Database Roles** to add it.

Agent Action Account

Unless an action has been associated with a Run As profile, the credentials used to perform the action are those defined for the action account. For more information about the Run As profile, see Managing Run As Accounts and Profiles. Some examples of actions include the following:

- Monitoring and collecting Windows event log data
- Monitoring and collecting Windows performance counter data
- Monitoring and collecting Windows Management Instrumentation (WMI) data
- Running actions such as scripts or batch files

MonitoringHost.exe is the process that runs these actions by using the credentials specified in the action account. A new instance of MonitoringHost.exe is created for each account.

Using a Low-Privileged Account

When you install Operations Manager, you can choose one of two options while assigning the action account:

- Local System
- Domain or Local Account

A common approach is to specify a domain account, which allows you to select a user with the least amount of privileges necessary for your environment.

The default action account must have the following minimum privileges:

- Member of the local Users group
- Member of the local Performance Monitor Users group
- Allow log-on-locally permission (SetInteractiveLogonRight)

The minimum described above are the lowest privileges that Operations Manager supports for the action account. Other Run As accounts can have lower privileges. The actual privileges required for the Run As accounts depend on which management packs are running on the computer and how they are configured. For more information about which specific credentials are required, see the appropriate management pack guide.

Keep the following points in mind when choosing credentials for the agent action account:

- A low-privileged account is all that is necessary for agents that are used to monitor domain controllers.
- Using a domain account requires you to update your password consistent with your password expiration policies.
- You must stop and then start System Center Management service if the action account has been configured to use a low-privilege account and this account was added to the required groups while the System Center Management service was running.

Notification Action Account

The notification action account is a Run As account that is created by the user to configure notifications. This is the action account that is used for creating and sending notifications. Ensure that the credentials you use for this account have sufficient rights for the SMTP server, instant messaging server, or SIP server that you will use for notifications.

If you change the password for the credentials that you entered for the notification action account, you have to make the same password changes for the Run As account.

Managing Action Account Credentials

For the account you choose, Operations Manager determines what the password expiration date is and generates an alert 14 days before the account expires. When you change the password in Active Directory, you can change the password for the action account in Operations Manager on the **Account** tab on the **Run As Account Properties** page. For more information about managing the action account credentials, see How to Change the Credentials for the Action Account.

Service Accounts

The set of credentials of the System Center Configuration service and System Center Data Access service account is used by the System Center Data Access service and System Center Management Configuration service to update and read information in the operational database. Operations Manager ensures that the credentials used for the Data Access Services (DAS) service account are assigned to the Sdk_user role in the operational database. The System Center Configuration service and System Center Data Access service account can be configured as either a Local System account or as a domain account. A local User account is not supported.

If the management server and the operational database are on different computers, the System Center Configuration service and System Center Data Access account have to be changed to a domain account. For better security, we recommend that you use an account different from the one used for the management server action account. To change these accounts, see How to Change Credentials for the System Center Management Configuration service and System Center Data Access service.

Agent Installation Account

When implementing discovery-based agent deployment, you are prompted for an account with administrator rights. This account is used to install the agent on the computer, and therefore it must be a local administrator on all the computers you are deploying agents to. The management server action account is the default account for agent installation. If the management server

action account does not have administrator rights, select **Other user account** and type an account that has administrator rights. This account is encrypted before it is used and then discarded.

Data Warehouse Write Account

The Data Warehouse Write account writes data from the management server to the Reporting data warehouse and reads data from the operational database. The credentials that you supply for this account are made a member of the roles according to the application, as described in the following table.

Note
For information about supported configurations for System Center 2012 – Operations Manager, see Supported Configurations for Operations Manager for System Center 2012.

Application	Database/Role	Role/Account
Supported versions of Microsoft SQL Server	Operational database	db_datareader
Supported versions of Microsoft SQL Server	Operational database	dwsync_user
Supported versions of Microsoft SQL Server	Data warehouse database	OpsMgrWriter
Supported versions of Microsoft SQL Server	Data warehouse database	db_owner
Operations Manager	User role	Operations Manager Report Security Administrators account
Operations Manager	Run As account	Data Warehouse Action account
Operations Manager	Run As account	Data Warehouse Configuration Synchronization Reader account

If you change the password for the credentials that you entered for the Data Warehouse Write account, you have to make the same password changes for the following accounts:

- Run As account called Data Warehouse Action account
- Run As account called Data Warehouse Configuration Synchronization Reader account

Data Reader Account

This account is used to deploy reports, define what user the SQL Server Reporting Services uses to run queries against the Reporting data warehouse, and for the SQL Server Reporting Services

IIS Application Pool account to connect to the management server. This account is added to the Report Administrator User profile.

The credentials that you supply for this account are made a member of the roles according to the application, as described in the following table.

Note
For information about supported configurations for System Center 2012 – Operations Manager, see Supported Configurations for Operations Manager for System Center 2012.

Application	Database/Role	Role/Account
Supported versions of Microsoft SQL Server	Reporting server installation instance	Report Server Execution Account
Supported versions of Microsoft SQL Server	Data warehouse database	OpsMgrReader
System Center 2012 – Operations Manager	User role	Operations Manager Report Security Administrators
System Center 2012 – Operations Manager	User role	Operation Manager Report Operators
System Center 2012 – Operations Manager	Run As account	Data Warehouse Report Deployment account
Internet Information Services (IIS)	Application pool	ReportServer$<INSTANCE>
Windows Service	SQL Server Reporting Services	Log on account

If you change the password for the credentials that you entered for the Data Reader account, you have to make the same password changes for the following accounts:

- Report Server Execution Account
- The SQL Server Reporting Services service account on the computer that is hosting SQL Server Reporting Services (SSRS)
- The IIS ReportServer$<INSTANCE> Application Pool account
- Run As account called Data Warehouse Report Deployment account

Account Information

- How to Change the Credentials for the Action Account
- How to Change Credentials for the System Center Management Configuration service and System Center Data Access service
- How to Change IIS ReportServer Application Pool Account Password

- How to Change the Reporting Server Execution Account Password
- How to Change the Windows Service Account Password for the SQL Server Reporting Service
- How to Change the Run As Account Associated with a Run As Profile

How to Change the Credentials for the Action Account

During the installation of System Center 2012 – Operations Manager, you are prompted for credentials for the management server action account. If you want to change the password for the credentials that you provided or use a different set of credentials, use the following procedure.

To change the credentials for the action account

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click the **Administration** button.
3. In the **Administration** pane, under the **Run As Configuration**, click **Accounts**.
4. In the **Accounts** pane, under **Type: Action Account**, right-click the account (domain\user name) that you want to change, and then click **Properties**.
5. In the **Run As Account Properties** dialog box, click the **Credentials** tab.
6. Enter the new credentials for the action account, and then click **OK**.

See Also

Making Changes to an Operations Manager Environment

How to Change Credentials for the System Center Management Configuration service and System Center Data Access service

How to Change Credentials for the System Center Management Configuration service and System Center Data Access service

During the installation of System Center 2012 – Operations Manager, you are prompted for credentials for the System Center Configuration service and System Center Data Access service. If you want to change the password for the credentials that you provided or use a different set of credentials, use the following procedure.

Note

The same credentials must be used for both services.

To change credentials or password for the System Center Configuration service and System Center Data Access service

1. On the computer hosting the management server, on the Windows desktop, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **services.msc**, and then click **OK**.
3. In the list of services, right-click **System Center Data Access Service**, and then click

Properties.

4. In the **System Center Data Access Properties** dialog box, click the **Log On** tab.
5. Enter new credentials or change the password of the existing credentials, and then click **OK**.
6. In the list of services, right-click **System Center Management Configuration**, and then click **Properties**.
7. In the **System Center Management Configuration Properties** dialog box, click the **Log On** tab.
8. Enter new credentials or change the password of the existing credentials, and then click **OK**.
9. Stop and restart both the **System Center Data Access** service and **System Center Management Configuration** service.

See Also

Making Changes to an Operations Manager Environment

How to Change the Credentials for the Action Account

How to Change IIS ReportServer Application Pool Account Password

If you change the password for the account that you specified as the Data Reader account during the setup of the System Center 2012 – Operations Manager Reporting server, you must change the IIS Report Server Application Pool account password. You can accomplish this by using the following procedure on the computer that is running SQL Server Reporting Services.

To change the IIS ReportServer Application Pool account

1. On the computer running SQL Server Reporting Services, on the Windows desktop, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In **Internet Information Services (IIS) Manager**, expand **<Computer Name> (local computer)**, expand **Application Pools**, right-click **ReportServer<INSTANCE>**, and then click **Properties**.
3. In the **ReportServer<INSTANCE> Properties** dialog box, click **Identity**.
4. In the **Password** box, type the new password, and then click **OK**.
5. Close Internet Information Services (IIS) Manager.

See Also

Account Information for Operations Manager

How to Change the Reporting Server Execution Account Password

How to Change the Windows Service Account Password for the SQL Server Reporting Service

How to Change the Reporting Server Execution Account Password

If the password changes for the account that you specified as the Data Reader Account during the setup of the Reporting server, use the following procedure to change the Execution account password on the Reporting server.

To change the Reporting Server Execution account password

1. On the computer hosting the Reporting server, on the Windows desktop, click **Start**, point to **Programs**, point to **Microsoft SQL Server 2008 R2**, point to **Configuration Tools**, and then click **Reporting Services Configuration**.
2. In the **Reporting Server Installation Instance Selection** dialog box, click **Connect**.
3. In the **Reporting Services Configuration Manager** pane, in the left pane, click **Execution Account**.
4. In the **Execution Account** pane, type the new password for the execution account.
5. Click **Apply**, and then click **Exit** to close Reporting Services Configuration Manager.

See Also

Account Information for Operations Manager

How to Change IIS ReportServer Application Pool Account Password

How to Change the Windows Service Account Password for the SQL Server Reporting Service

How to Change the Windows Service Account Password for the SQL Server Reporting Service

If the password changes for the account that you specified as the Data Reader account during the setup of the Reporting server, use the following procedure to change the Windows service account for the SQL Server Reporting Services password on the computer running SQL Server Reporting Services (SSRS).

To change the Windows service account for the SQL Server Reporting Services

1. On the computer running SQL Server Reporting Services, on the Windows desktop, click **Start**, point to **Settings**, and then click **Run**.
2. In the **Run** dialog box, type **services.msc**, and then click **OK**.
3. In **Services**, scroll down the list, right-click **SQL Server Reporting Services (<INSTANCE>)**, and then click **Properties**.
4. In the **SQL Server Reporting Services (<INSTANCE>) Properties** dialog box, click **Log On**.
5. In the **Password** and **Confirm Password** boxes, type the new password, and then click **OK**.
6. Close **Services**, and then close **Administrative Tools**.

See Also

Account Information for Operations Manager

How to Change IIS ReportServer Application Pool Account Password

How to Change the Reporting Server Execution Account Password

How to Change the Run As Account Associated with a Run As Profile

By default, the following Run As profiles have a Run As account associated with them.

- Data Warehouse account
- Data Warehouse Configuration Synchronization Reader account
- Data Warehouse Report Deployment account
- Data Warehouse SQL Server Authentication account
- Reporting SDK SQL Server Authentication account

For example, the Run As profile named Data Warehouse SQL Server Authentication account has the Run As account named Data Warehouse SQL Server Authentication account associated with it. As an example, you can use the following procedure to change the Run As account associated with the Run As profile called Data Warehouse SQL Server Authentication account. It is assumed that the new Run As account that you want to associate with this Run As profile has already been created. For more information about Run As accounts and Run As profiles, see Managing Run As Accounts and Profiles

To change the Run As account associated with a Run As profile

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the System Center 2012 – Operations Manager management group.
2. In the Operations console, click the **Administration** button.

   Note
   When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the Operations Manager management server that you want the Operations console to connect to.
3. In the **Administration** pane, expand **Administration**, expand **Security**, and then click **Run As Profiles**.
4. In the Run As profiles pane, right-click **Data Warehouse SQL Server Authentication Account**, and then click **Properties**.
5. In the **Run As Profile - Data Warehouse SQL Server Authentication Account** dialog box, and then click the **Run As Accounts** tab.
6. Under **Run As Accounts**, click the targeted computer, and then click **Edit**.
7. In the **Edit Alternate Run As Account** dialog box, click the **Run As Account** list, select the new Run As account that you want to associate with this Run As profile, and then click **OK**.
8. In the **Run As Profile - Data Warehouse SQL Server Authentication Account** dialog box, click **OK**.

See Also

Account Information for Operations Manager

How to Uninstall Operations Manager

Use the following procedure to uninstall any feature of System Center 2012 – Operations Manager, including the management server, gateway server, Reporting server, operations console, web console, and agent.

To uninstall System Center 2012 - Operations Manager

1. Log on to the server with an account that has local administrator rights.
2. In Control Panel, click **Programs and Features**.
3. On the **Uninstall or change a program** page, right-click **System Center 2012 - Operations Manager**, and then select **Uninstall/Change**.

   Note
   When you uninstall a stand-alone feature, the name that appears in **Program and Features** reflects the name of the feature.
4. On the **Getting Started**, **What do you want to do?** page, click **Remove a feature**. The Setup Wizard then identifies and lists all the features and roles that are installed on the local computer.
5. Select the features that you want to remove, and then click **Uninstall**.
6. On the **Complete**, **Component removal is complete** page, click **Close**.

See Also

Making Changes to an Operations Manager Environment

How to Manage the Report Server Unattended Execution Account

The System Center 2012 – Operations Manager Report Server unattended execution account is used to query data from the Reporting Data Warehouse. Users that manage this account require only the Read user right. This account is not managed from within the Operations Manager user interface. Use this procedure to change the user name or password for this account.

To manage the Report Server unattended execution account

1. On the Windows desktop, click **Start**, point to **Programs**, point to **Microsoft SQL Server 2008 R2 SP1**, point to **Configuration Tools**, and then click **Reporting Services Configuration**.
2. In Reporting Services Configuration Manager, in the **Report Server Installation Instance Selection dialog** box, click **Connect**.
3. In the navigation pane, click **Execution Account**.
4. In the Execution Account pane, type a new user name or password as required.
5. Click **Apply**, and then click **Exit**.

See Also

Account Information for Operations Manager

How to Configure the Internet Proxy Settings for a Management Server

Use the following procedure to configure the Internet proxy settings for a System Center 2012 – Operations Manager management server. You must configure these settings if features of Operations Manager are enabled that require the management server to communicate over the Internet. For example, you must configure these settings if the Client Monitoring feature of Operations Manager is configured to transmit or receive data from Microsoft.

To Configure Internet Proxy Settings for a Management Server

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click the Administration button.
3. In the Administration pane, expand **Administration**, expand **Device Management**, and then click **Management Servers**.
4. In the results pane, right-click the management server for which you want to view the properties, and then click **Properties**.
5. In the **Management Server Properties** dialog box, click the **Proxy Settings** tab.
6. On the **Proxy Settings** tab, select **Use a proxy server for communication with Microsoft** and then do the following:
7. Select **http://** or **https://** from the drop-down list, and type the name of the Internet proxy server in the **Address** text box.
8. Type the **Port** number, and then click **OK**.

See Also

Making Changes to an Operations Manager Environment

How to Move the Operational Database

After the initial deployment of System Center 2012 – Operations Manager, you might need to move the operational database from one Microsoft SQL Server-based computer to another.

This procedure requires Microsoft SQL Server configuration. You need to back up a database, restore a database, update a database table, add new Logins, and modify User Mapping settings for Logins. For more information, see SQL Server documentation.

Operational Database Relocation

Use the procedure below to move the operational database to a different server.

To move the operational database

1. Stop the Operations Manager services (System Center Data Access, System Center Management, and System Center Management Configuration) on all the management

servers in the management group.

2. Use Microsoft SQL Server Management Studio to create a full backup of the operational database. The default name is OperationsManager.

   For more information, see How to: Back Up a Database (SQL Server Management Studio).

3. On the new SQL server, copy the backup file to a local drive or map a local drive to the folder that contains the backup file.
4. Optionally, on the original server that hosts the operational database, delete the operational database.
5. On the new server, use Microsoft SQL Server Management Studio to restore the operational database that you previously backed up.

   For more information, see How to: Restore a Database Backup (SQL Server Management Studio).

6. Update the registry on each management server in the management group to refer to the new SQL Server-based computer.

   Note
   Before editing the registry, follow your organization's backup policies with regard to the registry.

   a. Log on to the management server with Administrator permissions.
   b. Click **Start**, select **Run**, type **regedit** in the **Open** box, and then click **OK** to start Registry Editor.
   c. Under **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\System Center\2010\Common\Database**, double-click the name **DatabaseServerName**, and then change the value to the hostname of the SQL Server-based computer now hosting the operational database, and then click **OK** to save your change.

      Note
      If you are using a named instance of SQL Server, be sure to use the `ServerName\Instance` name format.

   d. Close the Registry Editor.

7. On each management server, edit the following file:

   `%ProgramFiles%\System Center 2012\Operations Manager\Server\ConfigService.config`

   In the `<Category>` tag named "Cmdb", change the value for `ServerName` to the name of the new SQL server.

8. Update the operational database with the new database server name.

   a. Open SQL Server Management Studio.
   b. Expand **Databases**, **OperationsManager,** and **Tables**.
   c. Right-click **dbo. MT_Microsoft$SystemCenter$ManagementGroup** , and then click **Edit Top 200 Rows**.
   d. Change the value in the **SQLServerName_6B1D1BE8_EBB4_B425_08DC_2385C5930B04** column to

reflect the name of the new SQL Server-based computer.

e. Save the change.

9. Update the operational database with the new database server name to specify the location of the Application Performance Monitoring tables.
   a. Open SQL Server Management Studio.
   b. Expand **Databases**, **OperationsManager,** and **Tables**.
   c. Right-click **dbo. MT_Microsoft$SystemCenter$OpsMgrDB$AppMonitoring**, and then click **Edit Top 200 Rows**.
   d. Change the value in the **MainDatabaseServerName_5C00C79B_6B71_6EEE_4ADE_80C11F84527A** column to reflect the name of the new SQL Server-based computer.
   e. Save the change.
10. On the new server hosting the operational database, expand **Security**, then expand **Logins**, and then add the data writer account.

    For more information, see How to: Create a SQL Server Login.
11. Also in **Logins**, add the action account.
12. Also in **Logins**, add the Data Access Service (DAS) computer account, using the form "domain\computername$".
13. For the DAS computer account, add the following user mappings:
    - ConfigService
    - db_accessadmin
    - db_datareader
    - db_datawriter
    - db_ddladmin
    - db_securityadmin
    - sdk_users
    - sql_dependency_subscriber

    Note

    If an account has not existed before in the SQL instance in which you are adding it, the mapping will be picked up by SID automatically from the restored operations database. If the account has existed in that SQL instance before, you receive an error indicating failure for that login, although the account appears in **Logins**. If you are creating a new login, ensure the User Mapping for that login and database are set to the same values as the previous login:

    DW Data Writer: apm_datareader, apm_datawriter, db_datareader, dwsynch_users

    Action account: db_datareader, db_datawriter, db_ddladmin, dbmodule_users

    DAS/Configuration account: ConfigService, db_accessadmin, db_datareader, db_datawriter, db_ddladmin, db_securityadmin, sdk_users,

sql_dependency_subscriber

If DAS/Configuration uses the LocalSystem account, specify computer account in form `<domain>\<computername>$`.

14. Execute the following SQL commands on new Operations database instance:

    sp_configure 'show advanced options',1

    reconfigure

    sp_configure 'clr enabled',1

    reconfigure

15. Run the following SQL query:

    SELECT is_broker_enabled FROM sys.databases WHERE name='OperationsManager'

16. If the result of the preceding query was an **is_broker_enabled** value of 1, skip this step. Otherwise, run the following SQL queries:

    ALTER DATABASE OperationsManager SET SINGLE_USER WITH ROLLBACK IMMEDIATE

    ALTER DATABASE OperationsManager SET ENABLE_BROKER

    ALTER DATABASE OperationsManager SET MULTI_USER

17. Start the Operations Manager services (System Center Data Access, System Center Management, and System Center Management Configuration) on all the management servers in the management group.

See Also

Making Changes to an Operations Manager Environment

How to Move the Data Warehouse Database

How to Move the Data Warehouse Database

After the initial deployment of System Center 2012 – Operations Manager, you might need to move the data warehouse database from one Microsoft SQL Server-based computer to another.

Caution

This procedure can result in data loss if it is not performed correctly and within a reasonable length of time of the failure. Ensure that you follow all steps precisely, without unnecessary delays between the steps.

This procedure requires Microsoft SQL Server configuration. You need to back up a database, restore a database, update a database table, add new Logins, and modify User Mapping settings for Logins. For more information, see SQL Server documentation.

Data Warehouse Database Relocation Procedure

Use the procedure below to move the data warehouse database to a different system.

To move the data warehouse database

1. Stop the Operations Manager services (System Center Data Access Service, System Center Management Service, System Center Management Configuration Service) on all management servers in the management group.
2. On the current Data Warehouse server, use SQL Server Management Studio to create a full backup of the data warehouse database. The default name is OperationsManagerDW. We recommend that you also back up the associated master database.

   For more information, see How to: Back Up a Database (SQL Server Management Studio).
3. On the new SQL server, copy the backup file to a local drive or map a local drive to the folder that contains the backup file.
4. Optionally, on the current Data Warehouse server, delete the data warehouse database.
5. On the new Data Warehouse server, use SQL Management Studio to restore the operational database that you previously backed up.

   For more information, see How to: Restore a Database Backup (SQL Server Management Studio).
6. On the server hosting the Operations Manager Reporting component, update the registry to refer to the new SQL Server-based computer.

   Note
   Before editing the registry, follow your organization's backup policies with regard to the registry.

   a. Log on to the management server with Administrator permissions.
   b. Click **Start**, select **Run**, type **regedit** in the **Open** box, and then click **OK** to start Registry Editor.
   c. Under **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Reporting**, double-click the name **DWDBInstance**, and then change the value to the hostname of the SQL Server-based computer now hosting the operational database, and then click **OK** to save your change.
   d. Close the Registry Editor.
7. Start the System Center Data Access Service on the management server associated with the reporting server.
8. On the management server associated with the reporting server, change the connection string.
   a. Open a browser and go to the reporting webpage, http://localhost/reports_instancename.
   b. Click **Show Details** and then click **Data Warehouse Main**.
   c. Change the **Connection String** to contain the new data warehouse server name, and then click **Apply**.
   d. Close the browser.

9. On the management server associated with the reporting server, change the connection string for AppMonitoringSource.
    a. Open a browser and go to the reporting webpage, http://localhost/reports_instancename.
    b. Click **Application Monitoring**, and then click **.NET Monitoring**.
    c. Click **Show Details**, and then click **AppMonitoringSource**.
    d. On the **AppMonitoringSource** page, click **Properties** and change **Connection string** to contain the new data warehouse main data source server name, and then click **Apply**.
    e. Close the browser.
10. On the server hosting the operational database, update the OperationsManager database table.
    a. Open SQL Server Management Studio.
    b. Expand **Databases**, **OperationsManager**, and **Tables**.
    c. Right-click **dbo. MT_Microsoft$SystemCenter$DataWarehouse**, and then click **Edit Top 200 Rows**.
    d. Change the value in the **MainDatabaseServerName_2C77AA48_DB0A_5D69_F8FF_20E48F3AED0F** column to reflect the name of the new SQL Server.
    e. Close SQL Server Management Studio.
11. On the server hosting the operational database, update the OperationsManager database for Application Performance Monitoring functionality.
    a. Open SQL Server Management Studio.
    b. Expand **Databases**, **OperationsManager**, and **Tables**.
    c. Right-click **dbo. MT_Microsoft$SystemCenter$DataWarehouse$AppMonitoring**, and then click **Edit Top 200 Rows**.
    d. Change the value in the **MainDatabaseServerName_5C00C79B_6B71_6EEE_4ADE_80C11F84527A** column to reflect the name of the new SQL Server.
    e. Close SQL Server Management Studio.
12. On the new data warehouse server, update the member database.
    a. Open SQL Server Management Studio.
    b. Expand **Databases**, **OperationsManagerDW**, and **Tables**.
    c. Right-click **dbo. MemberDatabase**, and then click **Edit Top 200 Rows**.
    d. Change the value in the **ServerName** column to reflect the name of the new SQL Server.
    e. Close SQL Server Management Studio.
13. On the new server hosting the operational database, expand **Security**, then expand **Logins**, and then add the data writer account.

    For more information, see How to: Create a SQL Server Login.

14. Also in **Logins**, add the data reader account.
15. Also in **Logins**, add the Data Access Service computer account, using the form "domain\computername$".
16. For the Data Access Service (DAS) computer account, add the following user mappings:
    - db_datareader
    - OpsMgrReader
    - apm_datareader

    Note

    If an account has not existed before in the SQL instance in which you are adding it, the mapping will be picked up by SID automatically from the restored data warehouse database. If the account has existed in that SQL instance before, you receive an error indicating failure for that login, although the account appears in **Logins**. If you are creating a new login, ensure the User Mapping for that login and database are set to the same values as the previous login:

    DW Data Writer: db_owner, OpsMgrWriter, apm_datareader, apm_datawriter

    DW Data Reader: db_datareader, OpsMgrReader, apm_datareader

    DAS/Config account: db_datareader, OpsMgrReader, apm_datareader

    If DAS/Config uses the LocalSystem account, specify computer account in form "<domain>\<computername>$".
17. Start the Operations Manager services (System Center Management, System Center Data Access, and System Center Management Configuration) on all the management servers in the management group.

To verify a successful move of the data warehouse database

1. Verify that you can successfully run a report from the console.
2. Ensure that the health state of all management servers in the management group are **Healthy**.

   If the health state of any management server is **Critical**, open **Health Explorer**, expand **Availability - <***server name***>**, and then continue to expand until you can navigate to **Data Warehouse SQL RS Deployed Management Pack List Request State**. Check the associated events to determine if there is an issue accessing the data warehouse database.
3. Check operating system events:
   a. Open the operating system's Event viewer. Navigate to **Event Viewer**, and then to **Operations Manager**.
   b. In the **Operations Manager** pane, search for events with a **Source** of **Health Service Module** and a **Category** of **Data Warehouse**.

      The move was successful if event number 31570, 31558, or 31554 exists.

      There is an issue accessing the data warehouse database if event numbers 31563,

31551, 31569, or 31552 exists.

4. Check events in Operations Manager:
   a. In the Operations console, select **Monitoring**.
   b. Navigate to **Monitoring**, **Operations Manager**, **Health Service Module Events**, and then to **Performance Data Source Module Events**.
   c. Search the **Performance Data Source Module Events** pane for events with a **Date and Time** that is later than the move.

      There is a problem with the data warehouse database if events have a **Source** of **Health Service Module** and an **Event Number** of 10103.

How to Move the Audit Collection Database

After the initial deployment of System Center 2012 – Operations Manager, you might need to move the Audit Collection (OperationsManagerAC) database from one Microsoft SQL Server-based computer to another.

This procedure requires Microsoft SQL Server configuration. You need to back up a database, restore a database, and add a new Login. For more information, see SQL Server documentation.

ACS Database Relocation

Use the procedure below to move the ACS database to a different server.

To move the ACS database

1. On the original Audit Collection database server, stop Operations Manager Audit Collection Service.
2. Use Microsoft SQL Server Management Studio to create a full backup of the ACS database. The default name is OperationsManagerAC. We also recommend you back up the master database.

   For more information, see Create a Full Database Backup (SQL Server).
3. On the new SQL server, copy the backup file to a local drive or map a local drive to the folder that contains the backup file.
4. Optionally, on the original server that hosts the ACS database, delete the ACS database.
5. On the new server, use Microsoft SQL Server Management Studio to restore the ACS database that you previously backed up.

   For more information, see Restore a Database Backup (SQL Server Management Studio).
6. On the new ACS database server, use SQL Management Studio to create a login for the ACS server, as follows:
   a. In SQL Server Management Studio, navigate to **Security** and then to **Logins**. Right-click **Logins** and select **New Login**.
   b. In the **Login name** box, enter the ACS server (the system on which the ACS service

runs) in the format **domain\computername$**.

c. Under **Select a page**, click **User Mapping**.

d. Under **Users mapped to this login**, select the ACS database (default: **OperationsManagerAC**), and then, under **Database role membership for**, select db_owner.

e. Click **OK** to save your new account.

For more information, see Create a Login.

7. Update the registry on ACS server to refer to the new ACS database server.

Note
Before editing the registry, follow your organization's backup policies with regard to the registry.

a. Log on to the management server with Administrator permissions.

b. Click **Start**, select **Run**, type **regedit** in the **Open** box, and then click **OK** to start Registry Editor.

c. Under **HKEY_LOCAL_MACHINE\Software\ODBC\ODBC.INI\OpsMgrAC**, double-click the name **Server**, and then change the value to the hostname of the SQL Server-based computer now hosting the ACS database, and then click **OK** to save your change.

Warning
If you are using a named instance of SQL Server, be sure to use the `ServerName\Instance` name format.

d. Close the Registry Editor.

8. On the server on which the ACS service is running, start Operations Manager Audit Collection Service.

How to Move the Reporting Server Role

You can move the System Center 2012 – Operations Manager Reporting server component to a new server, or reinstall the component on the original server.

During this move, Operations Manager stops storing data in the OperationsManagerDW database until you complete the Operations Manager reporting server reinstall.

Use the procedures in this topic to move the reporting server to a new server and verify the success of the move. You must back up any custom reports that were authored outside of Operations Manager 2007. For more information about this, see Moving the Report Server Databases to Another Computer in the SQL Server 2008 Books Online (http://go.microsoft.com/fwlink/?LinkId=151513).

Note
Ensure that you follow all steps precisely, as not doing so might result in data corruption.

To move the Operations Manager reporting server

1. Use Microsoft SQL Server Management Studio to create a full backup of the data warehouse database. The default name is OperationsManagerDW.

   For more information, see Create a Full Database Backup (SQL Server).
2. On the current Operations Manager reporting server computer, uninstall the Operations Manager reporting server component as follows:
   a. Click **Start**, click **Control Panel**, and then click **Add or Remove Programs** if you are using Windows Server 2003, or click **Programs and Features** if you are using Windows Server 2008.
   b. In the **Add or Remove Programs** or **Programs and Features** dialog box, select **System Center 2012 - Operations Manager**, and then click **Uninstall/Change**.
   c. In the **Operations Manager Setup** wizard, click **Remove a feature**.
   d. In the **Select features to remove** page, select **Reporting server**, and then click **Uninstall**. Click **Close** when the wizard finishes.
3. On the new SQL server, copy the backup file to a local drive or map a local drive to the folder that contains the backup file.
4. Optionally, on the original server that hosts the operational database, delete the data warehouse database.
5. On the new server, use Microsoft SQL Server Management Studio to restore the data warehouse database that you previously backed up.

   For more information, see Restore a Database Backup (SQL Server Management Studio).
6. If you are reinstalling the Operations Manager reporting server component on the original server, you must remove any data that is left from the original installation by doing the following:
   a. Copy the ResetSRS.exe tool from the SupportTools folder on the product CD to a local folder.
   b. Open a command prompt window using the **Run as Administrator** option and run the tool as follows:

      ```
      ResetSRS.exe <SQL Server instance name>
      ```
   c. Here, SQL Server instance name is the SQL Server instance that SQL Reporting Services is installed on, such as 'Instance1'. If SQL Server is using the default instance, enter MSSQLSERVER.
   d. Open the Reporting Configuration Manager by clicking **Start**, pointing to **Programs**, pointing to **Microsoft SQL Server 2005** or **Microsoft SQL Server 2008**, pointing to **Configuration Tools**, and then clicking **Reporting Services Configuration**.
   e. For SQL Reporting Services 2005, in the **Configure Report Server** page, check the status of the **Web Service Identity** item. If the status is not **Configured** (green), click that item, and then click **Apply**.

      Check the status of the rest of the items on that page. Configure any items that are

designated with a red ‘X’, indicating an unhealthy configuration status.

7. On the new Operations Manager reporting server computer, install the Operations Manager Reporting server component as follows:
   a. On the **Configuration**, **SQL Server instance for reporting services** page, make sure the **SQL Server instance** refers to the restored database.
   b. On the **Configuration**, **Configure Operation Manager accounts** page, be sure the **Data Reader** account is the same account previously used for the Report server.

   For more information, see How to Install the Operations Manager Reporting Server.

Verify that you can successfully run a report from the Operations console.

Ensure that the health state of all **Management servers** is **Healthy**.

How to Remove the Management Server Role

Use the following procedure to remove the management server role from a computer. For example, you might have to do this if you have to reassign a computer that is hosting the management server role and install a gateway server.

Before you remove the management server role from a computer, you must configure any objects that are managed by that management server, to be managed by a different management server as described in the following sections.

The high-level steps to remove a management server role are as follows:

1. Delete the Management Server from the management group.
2. If the management server you are about to remove functions as a primary management server for an agent, you must configure those agents to use a new primary management server. See Change the Primary Management Server.
3. If the management server you are about to remove acts as a proxy agent for an agentless-managed computer, you must identify a new management server. See Configure an Agentless-Managed Computer to Use a Different Proxy Agent.
4. If the management server you are about to remove acts as a proxy agent for a network device, you must identify a new management server. See Configure a Network Device to Use a Different Operations Manager 2012 Proxy Agent.
5. Remove the management server role from a computer. See Remove the Management Server from a Computer.

Delete the Management Server

Use the following procedure to delete a management server role from the management group.

To delete a management server from the management group

1. Open the Operations console with an account that is a member of the Operations Manager Administrator role for the management group.
2. In the Operations console, click the **Administration** button.

Note
When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the Operations Manager management server that you want the Operations console to connect to.

3. In the **Administration** pane, click **Management Servers.**
4. Right-click the desired management server, and then click **Delete**.
5. In the **Confirm Delete Management Server** dialog box, click **Yes**.

Change the Primary Management Server

Use the following procedure to change the primary management server for agent-managed computers that are assigned to primary and secondary management servers without using Active Directory Domain Services.

To change the primary management server for agent-managed computers by using the Operations console

1. Open the Operations console with an account that is a member of the Operations Manager Administrator role for the management group.
2. In the Operations console, click the **Administration** button.

   Note
   When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the Operations Manager management server that you want the Operations console to connect to.
3. In the **Administration** pane, expand **Administration**, expand **Device Management**, and then click **Agent Managed**.
4. In the **Agent Managed** pane, select the computers for which you want to change the primary management server, right-click them, and then select **Change Primary Management Server**.

   Note
   The **Change Primary Management Server** option is unavailable if Active Directory Domain Services was used to assign any of the selected computers to the management group.
5. In the **Change Management Server** dialog box, select the desired management server in the list, and then click **OK**. The change takes effect on the agent after its next update interval.

If you are changing the primary management server for a Linux or UNIX computer, the certificate that was used to access the Linux or UNIX computer must also be copied to the new management server. You do not have to copy the certificate if you are changing the primary management server for computers that are running Windows.

To copy a certificate from one server to another server

1. Log on to the management server that has the certificate that you want to copy.
2. At the command prompt, change the directory to %ProgramFiles%\System Center 2012 – Operations Manager. Run the following command: **scxcertconfig.exe – export <filename>**.
3. While the file created by scxcertconfig.exe contains only the public key of the certificate, you should still treat it as a security-sensitive file. The file, and any copies of the file, should be explicitly deleted when the certificate is imported into the new management server in step 5 in this procedure. Verify that the new management server can access the file copy location.
4. Log on to the management server that you want to monitor agents from.
5. At the command prompt, change the directory to %ProgramFiles%\System Center 2012 – Operations Manager. Run the following command: **scxcertconfig.exe –import <filename>**.

The imported certificate is required for Operations Manager to trust agents signed with that certificate. If multiple management servers are signing certificates, the certificates must be exported from each management server, and imported to the other management servers.

Configure an Agentless-Managed Computer to Use a Different Proxy Agent

Use the following procedure to change the Operations Manager proxy agent for an agentless-managed computer. The proxy agent can be any agent-managed computer in the management group that is configured to be a proxy.

To change the proxy agent for agentless-managed computers

1. Open the Operations console with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click the **Administration** button.

   Note
   When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the Operations Manager management server that you want the Operations console to connect to.
3. In the **Administration** pane, expand **Administration**, expand **Device Management**, and then click **Agentless Managed**.
4. In the **Agentless Managed** pane, select the agentless-managed computers for which you want to change the proxy agent, right-click them, and then select **Change Proxy Agent**.
5. In the **Change Proxy Agent** dialog box, select the computer that you want to be the new proxy agent, and then click **OK**.

Configure a Network Device to Use a Different Operations Manager 2012 Proxy Agent

Use the following procedure to change the Operations Manager proxy agent for network devices. The proxy agent can be any agent-managed computer in the management group. It must have Simple Network Management Protocol (SNMP) installed, an optional Windows element, and be able to connect to the devices that use SNMP.

To change the proxy agent for network devices

1. Open the Operations console with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click the **Administration** button.

   Note
   When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the Operations Manager management server that you want the Operations console to connect to.
3. In the **Administration** pane, expand **Administration**, expand **Device Management**, and then click **Network Devices**.
4. In the **Network Devices** pane, select the network devices for which you want to change the proxy agent, right-click them, and then select **Change Proxy Agent**.
5. In the **Change Proxy Agent** dialog box, select the computer that you want to be the new proxy agent, and then click **OK**.

Remove the Management Server from a Computer

Use the following procedure to remove a management server role from a computer.

To remove a management server role from a computer

1. In Control Panel, click **Programs and Features** on the computer from which you want to remove the management server component.
2. Right-click **System Center 2012 - Operations Manager**, click **Uninstall/Change**, and then follow the instructions in the wizard.

Removing a Gateway Server from a Management Group

Throughout the life cycle of your System Center 2012 – Operations Manager implementation, you might need to modify the structure and configuration of your deployment. In the case of gateway servers, these types of changes can stem from the decommissioning of an untrusted domain so that monitoring is no longer required or from the old server hardware being replaced with new hardware. To remove a gateway server from service, complete the following steps.

Overview of Decommissioning a Gateway Server

1. Configure all objects that are being managed by the gateway server to use a different primary management server. For an agent-managed computer, this means using either another gateway server or a management server.
2. Uninstall the gateway server software from the server.
3. Delete the gateway server from the management group.

Configure Managed Objects to Use an Alternate Primary Management Server

Gateway servers can manage three different types of objects: agent-managed computers, agentless-managed computers, and network devices acting as a proxy agent.

To configure agent-managed computers to use a different primary management server using the Operations console

1. Log on to a management server with an account that is a member of the Administrators role for the Operations Manager management group.
2. In the Operations console, click the **Administration** button.
3. In the Administration pane, expand **Administration**, expand **Device Management**, and then click **Agent Managed**.
4. In the Agent Managed pane, select the computers for which you want to change the primary management server, right-click them, and then select **Change Primary Management Server**.

   Note
   The **Change Primary Management Server** option will be unavailable if Active Directory Domain Services was used to assign any of the selected computers to the management group.
5. In the **Change Management Server** dialog box, select the new management server from the list, and then click **OK**. The change takes effect on the agent after its next update interval.

Alternatively, this configuration can be changed on the agent-managed computer itself using either of the following two procedures.

To change the primary management server for agent-managed computers by using the MOMAgent.msi setup wizard

1. Log on to the agent-managed computer with an account that is a member of the Administrators security group for the computer.
2. In **Add or Remove Programs**, click **Change** for **System Center Operations Manager 2012 Agent**.

   Note
   The **Agent Setup Wizard** can also be run by double-clicking MOMAgent.msi, which is located on the Operations Manager installation media.
3. In the **System Center 2012 – Operations Manager Agent Setup** Wizard, click **Next**.

4. On the **Program Maintenance** page, select **Modify**, and then click **Next**.
5. On the **Management Group Configuration** page, leave **Specify Management Group information** selected, and then click **Next**.
6. In the next **Management Group Configuration** page, do the following:
   a. Type the name of the **Management Server**.
   b. Type in a value for **Management Server Port**, or leave the default **5723**.
   c. Click **Next**.
7. On the **Ready to Install** page, review the settings, and then click **Install** to display the **Installing the System Center 2012 - Operations Manager Agent** page.
8. When the **Completing the System Center 2012 - Operations Manager Agent Setup wizard** page displays, click **Finish**.

To change the primary management server for agent-managed computers using MOMAgent.msi from the command line

1. Log on to the agent-managed computer with an account that is a member of the Administrators security group for the computer.
2. Open the command window.
3. At the prompt, run the following command:

```
%WinDir%\System32\msiexec.exe /i
\\path\Directory\MOMAgent.msi /qn USE_SETTINGS_FROM_AD=0
MANAGEMENT_GROUP=MG1 MANAGEMENT_SERVER_DNS=MS2.Domain1.net
```

   This command reconfigures the agent to use **MS2.Domain1.net** as its primary management server for management group **MG1**.

   Note
   Microsoft Windows Installer public properties must be uppercase, such as *PROPERTY=value*. For more information about Windows Installer, see Windows Installer in the Microsoft Developer Network library.

   If the Domain Name System (DNS) and Active Directory names for the management server differ, the **MANAGEMENT_SERVER_AD_NAME** property also needs to be set to the fully qualified Active Directory Domain Services name.

Redirecting Agentless-Managed Computers and Network Devices

To change the proxy agent for agentless-managed computers and network devices

1. Log on to a management server computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click the **Administration** button.
3. In the Administration pane, expand **Administration**, expand **Device Management**, and then click **Agentless Managed**. If you are working with a network device, select **Device Management** and then **Network Devices**.

4. In the Agentless Managed pane, select the agentless-managed computers for which you want to change the proxy agent, right-click them, and then select **Change Proxy Agent**. Or if you are working with a network device, in the **Network Devices** pane, select the network devices for which you want to change the proxy agent, right-click them, and then select **Change Proxy Agent**.
5. In the **Change Proxy Agent** dialog box, select the computer you want to be the new proxy agent, and then click **OK**.

The final steps in removing a gateway server from a management group are straightforward:

- Log on to the gateway server with an account that has administrative rights.
- In **Add or Remove Programs**, select **System Center Operations Manager 2012 Gateway**, and then click **Remove**.

In the **Operations** console, in the **Administration** view, under **Device Management**, **Management Servers**, select the gateway server, right-click it, and then click **Delete**.

Deleting the Gateway Server

The final steps in removing a gateway server from a management group are straightforward:

- Log on to the gateway server with an account that has administrative rights.
- In **Add or Remove Programs**, select **System Center Operations Manager 2012 Gateway**, and then click **Remove**.

In the **Operations** console, in the **Administration** view, under **Device Management**, **Management Servers**, select the gateway server, right-click it, and then click **Delete**.

How to Remove Certificates Imported with MOMCertImport

Use the following procedure to remove certificates that have been imported using the MOMCertImport tool.

To remove certificates imported with the MOMCertImport tool

1. Log on to the computer with an account that is a member of the Administrators group.
2. On the Windows desktop, click **Start**, and then click **Run**.
3. In the **Run** dialog box, type **cmd**, and then click **OK**.
4. At the command prompt, type **<***drive_letter***>:** (where <*drive_letter*> is the drive where the System Center 2012 – Operations Manager installation media is located), and then press ENTER.
5. Type **cd\SupportTools\amd64** and then press ENTER.
6. Type the following:

   MOMCertImport /Remove, and then press ENTER.

Sending Data to Microsoft

The following topics describe the different ways that you can send data to Microsoft to improve the products and features that you use most often and to help solve issues that you might encounter. Participation is voluntary, and the information is sent anonymously. You can opt in to any of the following programs.

Program	What it does	For more information
Customer Experience Improvement Program (CEIP)	Collects information about how you use Microsoft programs and about some of the issues that you might encounter.	Customer Experience Improvement Program (CEIP)
Operational Data Reporting	Collects a summary of how System Center 2012 – Operations Manager is being used and sends reports to Microsoft on a weekly basis. Microsoft uses these reports to improve the quality of its management packs and Operations Manager.	Operational Data Reporting (ODR)
Error Reporting	Anonymously sends reports of errors that occur in Operations Manager to Microsoft.	Error Reporting

See Also

Maintaining the System Center 2012 - Operations Manager Infrastructure

Customer Experience Improvement Program (CEIP)

The Microsoft Customer Experience Improvement Program (CEIP) collects information about how you use Microsoft programs and about some of the issues you might encounter. Microsoft uses this information to improve the products and features you use most often and to help solve issues. Participation in the program is strictly voluntary.

When you choose to participate in the CEIP, you configure clients with Group Policy to redirect CEIP reports to a System Center 2012 – Operations Manager management server, instead of reporting directly to Microsoft. The management servers are configured to forward these reports to Microsoft.

Important

The CEIP reports do not contain contact information about you or your organization, such as names or an address.

The CEIP reports forwarded from your organization to Microsoft are combined with CEIP reports from other organizations and individual customers to help Microsoft solve issues and improve the Microsoft products and features that customers use most often. For more information about the CEIP, see the CEIP page.

Use the following procedure to configure CEIP settings. The management server must have access to the Internet to participate in the program.

Important

CEIP is a component of the Client Monitoring feature of Operations Manager. Client Monitoring must be enabled on at least one management server and managed computers to participate in the CEIP. For information about enabling the Client Monitoring feature of Operations Manager, see Client Monitoring Using Agentless Exception Monitoring. After a management server has been configured for client monitoring, all agents that are participating in CEIP should be configured via Group Policy to send their CEIP data to that management server.

To configure the CEIP settings for Operations Manager

1. Log on to a management server with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click the **Administration** button.
3. In the **Administration** pane, expand **Administration**, and then click **Settings**.
4. In the **Settings** pane, expand **Type: General**, right-click **Privacy**, and then click **Properties**.
5. In the **Global Management Server Group Settings - Privacy** dialog box, on the **CEIP** tab, click **Join the Customer Experience Improvement Program (recommended)** to join the CEIP program or click **I don't want to join the program at this time** to decline participation. Then click **OK**.

   Note

   You can click **Tell me more about the program** to view information about the CEIP program, including the privacy statement.

See Also

Sending Data to Microsoft

Operational Data Reporting (ODR)

The Microsoft Customer Experience Improvement Program (CEIP) collects information about how you use Microsoft programs and about some of the issues that you might encounter. Microsoft uses this information to improve the products and features you use most often and to help solve issues. Participation in the program is strictly voluntary.

During setup of System Center 2012 – Operations Manager Reporting, on the **Operational Data Reports** page, you have the option to join CEIP. If you elect to join CEIP, Operations Manager Reporting collects a summary of how Operations Manager is being used and sends reports to Microsoft on a weekly basis. Microsoft uses these reports to improve the quality of its management packs and Operations Manager. You can view the contents of these operational data reports (ODRs) by creating a Microsoft ODR Report.

Note

Before configuring operational data reports, make sure that Operations Manager Reporting is installed, and that the management server has access to the Internet so that reports can be sent to Microsoft.

To configure the operational data reports settings

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click the **Administration** button.
3. In the **Administration** pane, expand **Administration**, and then click **Settings**.
4. In the **Settings** pane, expand **Type: General**, right-click **Privacy**, and then click **Properties**.
5. In the **Global Management Server Settings - Privacy** dialog box, on the **Operational Data Reports** tab, click **Yes, send operational data reports to Microsoft (recommended)** to send reports or click **No, don't send operational data reports to Microsoft** to decline participation.
6. Click **OK**.

To create a Microsoft ODR Report

1. Log on to the computer with an account that is a member of the Operations Manager Report Operators role for the Operations Manager management group.
2. In the Operations console, click the **Reporting** button.
3. In the **Reporting** pane, expand **Reporting**, and then click **Microsoft ODR Report Library**.
4. In the **Microsoft ODR Report Library Reports** pane, right-click one of the reports (for example, **Management Packs**), and then click **Open**.
5. In the Report view, in the **Parameter** area, click the Down Arrow in the **From** box, point to **This week**, and then click **Sunday**.
6. Click the Down Arrow in the **To** box, point to **This week**, and then click **Saturday**.
7. Click **Run** to display the ODR Report.
8. Click **Close** to close the report.

See Also

Sending Data to Microsoft

Error Reporting

When error reporting is enabled for System Center 2012 – Operations Manager features, if an error occurs, information about the error is anonymously reported to Microsoft. For more information about the privacy statement for the Microsoft Error Reporting Service, see Microsoft Online Crash Analysis. This information is used with error reports from other Microsoft customers to help identify and resolve common issues with Operations Manager.

Note
This setting enables error reporting only for Operations Manager features. For information about enabling the Client Monitoring feature of Operations Manager, which includes error reporting for the specified computers, see Client Monitoring Using Agentless Exception Monitoring.

To configure error reporting settings

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click the **Administration** button.
3. In the **Administration** pane, expand **Administration**, and then click **Settings**.
4. In the **Settings** pane, expand **Type: General**, right-click **Privacy**, and then click **Properties**.
5. In the **Global Management Server Settings - Privacy** dialog box, click the **Error Reporting** tab, and then do one of the following:
   - Select **Automatically send error reports about this product to Microsoft without prompting the user (recommended)**.
   - Select **Prompt the user for approval before sending error reports to Microsoft**.

     Note
     Click **Tell me more about error reporting** if you want to view the privacy statement for the Microsoft Error Reporting Service.
6. When you have made the selection that you want, click **OK**.

Error Transmission settings let you specify which error reports are sent to Microsoft and the additional diagnostic data that is included with the error reports.

To find the Error Transmission tab of the Global Management Server Group Settings - Privacy dialog box

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click the **Administration** button.
3. In the **Administration** pane, expand **Administration**, and then click **Settings**.
4. In the **Settings** pane, expand **Type: General**, right-click **Privacy**, and then click **Properties**.

5. In the **Global Management Server Group Settings - Privacy** dialog box, click the **Error Transmission** tab.

   Note
   Click **Read the privacy statement** to view the privacy statement.

To filter errors that are sent to Microsoft

1. On the **Error Transmission** tab of the **Global Management Server Group Settings - Privacy** dialog box, click **Filter**.
2. In the **Error Forwarding Filters** dialog box, select one or more of the options for sources of errors that you do not want forwarded to Microsoft, such as **that come from specific computers**.
3. In the **Criteria description** box, click **specific**, and provide the values for the criteria of errors that you do not want forwarded to Microsoft, such as **computer.contoso.com**.
4. Click **OK** twice.

To configure diagnostic data sent to Microsoft with error reports

1. On the **Error Transmission** tab of the **Global Management Server Group Settings - Privacy** dialog box, do one or more of the following:
   a. Select **Upload diagnostic data collection request**, select the additional diagnostic data that you want to send with error reports from computers that report errors to the management servers, and then forward them from the management server to Microsoft with the error reports.
   b. Set **Maximum number of CAB files to send to Microsoft per error group** to help Microsoft diagnose the error. The recommended number is 10.
   c. Select **Display links to solutions from Microsoft on error reporting computers**. A link to available solutions is displayed to end users after the error is first encountered and the link to the solution is downloaded to the management server.
   d. Select **Display links to surveys from Microsoft on error reporting computers**.
   e. Specify the **Default solution link when no Microsoft solution is available**. This can be an internal webpage for technical support, for example.
2. Click **OK**.

See Also

Sending Data to Microsoft

Operations Guide for System Center 2012 - Operations Manager

Operations Manager, a component of System Center 2012, enables you to monitor services, devices, and operations for many computers in a single console. Operators can gain rapid insight into the state of the IT environment and the IT services running across different systems and workloads by using numerous views that show state, health, and performance information, as well as alerts generated for availability, performance, configuration and security situations.

The Operations Guide is a comprehensive resource that can be used to understand and use Operations Manager. The Operations Guide covers administrative, monitoring, reporting, and operating tasks typically performed by an administrator or operator. It follows the Operations Manager Deployment Guide in order of use during an Operations Manager implementation project, but does not assume that the administrator or operator participated in the installation of the Operations Manager infrastructure.

Before you read the Operations Guide:

If you are new to Operations Manager, you should read Key Concepts to understand what a management group is and how Operations Manager works.

If you are familiar with Operations Manager 2007, you should read What's New in System Center 2012 - Operations Manager to review the differences between Operations Manager 2007 and Operations Manager for System Center 2012.

In the Operations Guide

- Quick Reference to Operations Manager Tasks

  This topic lists common tasks, tells you where to start each task, and includes links to relevant information.

- Initial Monitoring After Operations Manager Is Installed

  This section explains the management packs and monitoring that are in place when a management group is first created, and how to extend monitoring with agents and management packs. This section also provides guidance for managing discovery and agents, and explains how to use targeting and overrides to tune monitoring.

- Managing Access in Operations Manager

  This section explains the accounts that Operations Manager uses for various actions, the user roles that are available for scoping the views and tasks available in the Operations console, and the Run As accounts and profiles that are used by management packs to run workflows.

- Operations Manager Monitoring Scenarios

  This section presents common monitoring scenarios, such as monitoring clustered servers, monitoring networks, and monitoring across untrusted boundaries, and provides instructions for discovery, monitoring, views, and reports specific to each scenario.

- Getting Information from Operations Manager

  This section explains how to use the consoles, publish data to SharePoint sites, set up and manage alert notifications, and use the reports provided in Operations Manager.
- General Tasks in Operations Manager

  This section contains procedures for tasks that are common to many monitoring scenarios, such as how to deal with alerts, how to create and manage groups, how to create a resource pool, and how to connect management groups.
- Maintenance of Operations Manager

  This section explains how to monitor the health of the management group, configure and schedule grooming settings for the Operations Manager databases, and restart a management server. It also includes recommendations for creating an inventory of your Operations Manager infrastructure and for daily, weekly, and monthly tasks.

Related Resources

- TechNet Library main page for System Center 2012 - Operations Manager
- What's New in System Center 2012 - Operations Manager
- System Center 2012 - Operations Manager Release Notes
- Deployment Guide for System Center 2012 - Operations Manager
- System Center 2012 - Operations Manager Supported Configurations

Downloadable Documentation

You can download a copy of this technical documentation from the Microsoft Download Center. Always use the TechNet library for the most up-to-date information.

Quick Reference to Operations Manager Tasks

The following table gives a quick reference for where to perform common tasks and links to relevant information.

To perform this task	Do this
Check for problems in a management group	• Check the **Management Group Health** view in the Operations Manager folder in the **Monitoring** workspace • See the **State and Alerts** summary on the Monitoring Overview page • Check **Active Alerts** in the **Monitoring** workspace • Check **Task Status** in the **Monitoring** workspace

To perform this task	Do this
Start monitoring a computer	On the Administration Overview page, click **Configure computers and devices to manage**. For more information, see Managing Discovery and Agents.
Create or modify a resource pool	In the **Administration** workspace, click **Resource Pools**. For more information, see How to Create a Resource Pool and Managing Resource Pools for UNIX and Linux Computers.
• Create a group • View available groups • View group members • View state of a group • View diagram of a group • Modify a group	Click **Groups** in the **Authoring** workspace For instructions, see Creating and Managing Groups
Create a view	In the **Monitoring** workspace or **My Workspace**, at the bottom of the navigation pane, click **New View**. For more information, see Using Views in Operations Manager.
Customize the settings of a view for your own use	In the **Monitoring** workspace, right-click a view in the navigation pane, and then click **Personalize view**. For more information, see How to Personalize a View in Operations Manager.
Change the interval for heartbeats.	In the **Administration** workspace, click **Settings**, and then under **Agent**, click **Heartbeat**. For more information, see How Heartbeats Work in Operations Manager.
Change the number of missed heartbeats allowed	In the **Administration** workspace, click **Settings**, and then under **Server**, click **Heartbeat**. For more information, see How Heartbeats Work in Operations Manager.
Change a setting for a rule, monitor, or alert.	Make changes to rules, monitors, or alerts by creating an override. Select a rule, monitor, or alert, and then access the overrides options by right-clicking, or clicking **Overrides** on the toolbar, or clicking **Overrides** in the Tasks

To perform this task	Do this
	pane. For more information, see Tuning Monitoring by Using Targeting and Overrides and Creating a Management Pack for Overrides.
Change how frequently records are removed from the operational database.	In the **Administration** workspace, click **Settings**, right-click **Database Grooming**, and then click **Properties**. For more information, see **How to Configure Grooming Settings for the Operations Manager Database**.
Give a user permissions to view Operations Manager information or perform tasks.	In the **Administration** workspace, click **User Roles**, and then right-click a specific role and click **Properties**. For more information, see Implementing User Roles and How to Assign Members to User Roles.
Display a dashboard view on a SharePoint site.	You must deploy the Operations Manager Web Part to a SharePoint site, configure the Web Part to connect to a web console, and add the Web Part to a SharePoint page. For more information, see Using SharePoint to View Operations Manager Data.
Receive notifications of an alert in email, instant message, or text message.	Right-click an alert, point to **Notification subscription**, and then click **Create**. For more information, see Subscribing to Alert Notifications.
Investigate a gray agent.	In the **Monitoring** workspace, in the **Operations Manager\Agent Details\Agent Health State** view, in the **Agent State from Health Service Watcher** section, click the gray agent, and then in the **Tasks** pane, click **Show Gray Agent Connectivity Data**. For more information, see Not Monitored and Gray Agents.
Stop monitoring a computer temporarily.	In the **Monitoring** workspace, click **Windows Computers**, right-click the computer you want to stop monitoring, and click **Maintenance Mode**. For more information, see How to Suspend Monitoring Temporarily by Using Maintenance Mode.

To perform this task	Do this

See Also

Operations Guide for System Center 2012 - Operations Manager

Initial Monitoring After Operations Manager Is Installed

When Operations Manager, a component of System Center 2012, is first installed, only the features of the Operations Manager infrastructure such as management servers, reporting servers, and databases are monitored. Monitoring of the infrastructure is provided by the Monitoring Pack for Operations Manager, one of the management packs that is installed with Operations Manager. You can view details for the Monitoring Pack for Operations Manager in its guide at http://go.microsoft.com/fwlink/p/?LinkId=226940.

After Operations Manager is installed, you must decide which objects—computers and devices—should be monitored, and which applications, features, and services should be monitored on those objects.

Initial Monitoring After Operations Manager Is Installed topics

- Managing Discovery and Agents

  This section provides the information you need for discovering objects and configuring the objects to be monitoed by Operations Manager.
- Using Management Packs

  Monitoring for applications, features, and services is enabled by importing management packs. This section explains what management packs do, and how to import and manage them.
- Tuning Monitoring by Using Targeting and Overrides

  The monitoring provided by management packs creates a useful starting point, however most businesses will want to tailor the monitoring to meet their needs. This section explains how to tune monitoring by using overrides and how to use classes and groups as override targets.

Tip

As you install agents and import management packs, you should document your actions. For more information, see **Inventory of Operations Manager Infrastructure**.

Other resources for this component

- TechNet Library main page for Operations Manager

- Operations Guide for System Center 2012 - Operations Manager
- Managing Access in Operations Manager
- Operations Manager Monitoring Scenarios
- Getting Information from Operations Manager
- General Tasks in Operations Manager
- Maintenance of Operations Manager

Managing Discovery and Agents

System Center 2012 – Operations Manager can monitor computers running Windows, UNIX, and Linux operating systems. For a list of the supported operating system versions, see Supported Configurations.

To begin monitoring, computers must be discovered. For a description of the discovery process, see “How Objects Are Discovered and Monitored” in Key Concepts.

Comprehensive monitoring requires that an agent be installed on the discovered computer. This section explains how to discover computers, install agents on discovered computers, and configure agents. It also provides instructions for uninstalling agents. For information about monitoring computers without installing an agent, see Agentless Monitoring in Operations Manager and Client Monitoring Using Agentless Exception Monitoring in Operations Manager.

Note

For problems with discovery, see Troubleshooting Discovery in Operations Manager.

Managing Discovery and Agents topics

- Operations Manager Agent Installation Methods
- Install Agent on Windows Using the Discovery Wizard
- Install Agent on UNIX and Linux Using the Discovery Wizard
- Install Agent Using the MOMAgent.msi Setup Wizard
- Install Agent Using the Command Line
- Install Agent and Certificate on UNIX and Linux Computers Using the Command Line
- Managing Certificates for UNIX and Linux Computers
- Process Manual Agent Installations
- Applying Overrides to Object Discoveries
- Configuring Agents
- Examples of Using MOMAgent Command to Manage Agents
- Upgrading and Uninstalling Agents on UNIX and Linux Computers
- Upgrading Agents on UNIX and Linux Computers Using the Command Line
- Manually Uninstalling Agents from UNIX and Linux Computers
- Uninstall Agent from Windows-based Computers

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- How to Discover Network Devices in Operations Manager
- Managing Access in Operations Manager
- Operations Manager Monitoring Scenarios
- Getting Information from Operations Manager
- General Tasks in Operations Manager
- Maintenance of Operations Manager

Operations Manager Agent Installation Methods

An Operations Manager *agent* is a service that is installed on a computer. The agent collects data, compares sampled data to predefined values, creates alerts, and runs responses. A management server receives and distributes configurations to agents on monitored computers. There are several methods you can use to install an Operations Manager agent on a computer.

- You can use the Discovery Wizard in the Operations console, sometimes called a *push installation*. (All other methods are considered manual installations.) This method works for computers running Windows, UNIX, and Linux operating systems.
- You can run the Setup Wizard from the Operations Manager installation media and install the agent directly on a computer running Windows.
- You can install an agent directly on a computer running Windows, UNIX, and Linux operating systems by using a command line.

To install the agent by using the Discovery Wizard, firewall ports must be open on the agent-managed computers. Also, you must have an account that is a local administrator on the computer on which you want to install the agent.

Note

For information about port requirements for agents, see Agent and Agentless Monitoring in the Deployment Guide.

Agents that are installed by using the Discovery Wizard can be managed from the Operations console, such as updating agent versions, applying patches, and configuring the management server that the agent reports to.

When you install the agent using a manual method, updates to the agent must also be performed manually. You will be able to use Active Directory integration to assign agents to management groups. For more information, see Integrating Active Directory and Operations Manager.

See Also

Install Agent on Windows Using the Discovery Wizard

Install Agent on UNIX and Linux Using the Discovery Wizard

Install Agent Using the MOMAgent.msi Setup Wizard

Install Agent Using the Command Line

Install Agent and Certificate on UNIX and Linux Computers Using the Command Line

Managing Certificates for UNIX and Linux Computers

Process Manual Agent Installations

Applying Overrides to Object Discoveries

Configuring Agents

Examples of Using MOMAgent Command to Manage Agents

Upgrading and Uninstalling Agents on UNIX and Linux Computers

Manually Uninstalling Agents from UNIX and Linux Computers

Uninstall Agent from Windows-based Computers

Install Agent on Windows Using the Discovery Wizard

You can use the Operations console to search your environment for manageable objects and then deploy an agent to any object that you want to monitor. The process of searching your environment is called “discovery.” One of the advantages of using discovery is that it lists *all* manageable objects, including any that you might not be aware of.

The Discovery Wizard does not show computers that the management group is already monitoring. If you are doing a phased rollout of your management group, you can run the wizard to add new computers to the group. Also, after your initial deployment, you can use the Discovery Wizard to add newly installed computers to be managed.

When agents are pushed out to computers, System Center 2012 – Operations Manager sends credentials that have local administrator rights for that computer; this is required to install the agent.

If the Discovery Wizard is not right for your needs (for example, if you have a set list of computers to which you want to deploy agents), you have the option of manually installing agents on systems to be managed. Agents can also be embedded in the host image of the monitored computer.

Use the following procedure to discover computers running Windows and to deploy the Operations Manager agent to the discovered computers from the Operations console. For a list of the supported operating system versions, see Supported Configurations.

Note
For information about port requirements for agents, see Agent and Agentless Monitoring in the Deployment Guide.

To install an agent on a computer running Windows by using the Discovery Wizard

1. Log on to the Operations console with an account that is a member of the Operations Manager Administrators role.
2. Click **Administration**.
3. At the bottom of the navigation pane, click **Discovery Wizard**.

Note

The Discovery Wizard links in the Operations console open the Computer and Device Management Wizard.

4. On the **Discovery Type** page, click **Windows computers**.
5. On the **Auto or Advanced?** page, do the following:
   a. Select either **Automatic computer discovery** or **Advanced discovery**. If you select **Automatic computer discovery**, click **Next**, and then go to step 7. If you select **Advanced discovery**, continue with the following steps.

      Note

      Automatic computer discovery scans for Windows-based computers in the domain. Advanced discovery allows you to specify criteria for the computers that the wizard will return, such as computer names starting with NY.

   b. In the **Computer and Device Classes** list, select **Servers and Clients**, **Servers Only**, or **Clients Only**.
   c. In the **Management Server** list, click the management server or gateway server to discover the computers.
   d. If you selected **Servers and Clients**, you can select the **Verify discovered computers can be contacted** check box. This is likely to increase the success rate of agent deployment, but discovery can take longer.

      Note

      If the Active Directory catalog does not contain the NetBIOS names for computers in a domain, select **Verify discovered computers can be contacted**. Otherwise, the **Browse, or Type In** option fails to find computers. This affects computers in the same domain as the management server, in another domain with a full trust relationship, and in untrusted domains by using a gateway server.

   e. Click **Next**.

Note

The wizard can return approximately 4000 computers if **Verify discovered computers can be contacted** is selected, and it can return 10,000 computers if this option is not selected. Automatic computer discovery verifies that discovered computers can be contacted. A computer that is already managed by the management group is not returned.

6. On the **Discovery Method** page, you can locate the computers that you want to manage by either scanning or browsing Active Directory Domain Services or typing the computer names.

   If you want to scan, do the following:

   a. If it is not already selected, select **Scan Active Directory** and then click **Configure**.
   b. In the **Find Computers** dialog box, type the criteria that you want to use for

discovering computers, and then click **OK**.

c. In the **Domain** list, click the domain of the computers that you want to discover.

If you want to browse Active Directory Domain Services or type the computer names, do the following:

- Select **Browse for, or type-in computer names**, click **Browse**, specify the names of the computers that you want to manage, and then click **OK**.
- In the **Browse for, or type-in computer names** box, type the computer names, separated by a semi-colon, comma, or a new line. You can use NetBIOS computer names or fully qualified domain names (FQDN).

7. Click **Next**, and on the **Administrator Account** page, do one of the following:
   - Select **Use selected Management Server Action Account** if it is not already selected.
   - Select **Other user account**, type the **User name** and **Password**, and then select the **Domain** from the list. If the user name is not a domain account, select **This is a local computer account, not a domain account**.

     Important
     The account must have administrative privileges on the targeted computers. If **This is a local computer account, not a domain account** is selected, the management server action account will be used to perform discovery.
8. Click **Discover** to display the **Discovery Progress** page. The time it takes discovery to finish depends on many factors, such as the criteria specified and the configuration of the IT environment. If a large number (100 or more) of computers are being discovered or agents are being installed, the Operations console will not be usable during discovery and agent installation.

   Note
   Computers that are already managed by the management group will not be returned by the wizard.
9. On the **Select Objects to Manage** page, do the following:
   a. Select the computers that you want to be agent-managed computers.
   b. In the **Management Mode** list, click **Agent** and then click **Next**.

   Note
   The discovery results show virtual nodes of clusters. Do not select any virtual nodes to be managed.
10. On the **Summary** page, do the following:
    a. Leave the **Agent installation directory** set to the default of **%ProgramFiles%\System Center Operations Manager** or type an installation path.

       Important
       If a different **Agent installation directory** is specified, the root of the path must exist on the targeted computer or the agent installation fails.

Subdirectories, such as **\Agent**, are created if they do not exist.

b. Leave **Agent Action Account** set to the default, **Local System**, or select **Other** and type the **User name**, **Password**, and **Domain**. The Agent Action Account is the default account that the agent will use to perform actions.

c. Click **Finish**.

11. In the **Agent Management Task Status** dialog box, the **Status** for each selected computer changes from **Queued** to **Success**; the computers are ready to be managed.

    Note
    If the task fails for a computer, click the targeted computer. The reason for the failure is displayed in the **Task Output** text box.

12. Click **Close**.

See Also

Operations Manager Agent Installation Methods

Install Agent on UNIX and Linux Using the Discovery Wizard

Install Agent Using the MOMAgent.msi Setup Wizard

Install Agent Using the Command Line

Install Agent and Certificate on UNIX and Linux Computers Using the Command Line

Managing Certificates for UNIX and Linux Computers

Process Manual Agent Installations

Applying Overrides to Object Discoveries

Configuring Agents

Examples of Using MOMAgent Command to Manage Agents

Upgrading and Uninstalling Agents on UNIX and Linux Computers

Manually Uninstalling Agents from UNIX and Linux Computers

Uninstall Agent from Windows-based Computers

Install Agent on UNIX and Linux Using the Discovery Wizard

Use the **Computer and Device Management Wizard** to discover and install agents on UNIX and Linux computers. For a list of the supported operating system versions, see Supported Configurations.

Before you run the wizard, gather the following information:

- The host name, IP address, or range of IP addresses of the UNIX or Linux computers that you want to discover.
- At a minimum, you will need a low-privileged account established on the UNIX or Linux computer to discover it. To install an agent, you will need privileged access. For more information, see Accessing UNIX and Linux Computers in Operations Manager.
- If defined, the name of the resource pool created to monitor UNIX or Linux computers. For more information, see Managing Resource Pools for UNIX and Linux Computers.

To discover and install an agent on a UNIX or Linux Computer

1. Log on to the Operations console with an account that is a member of the Operations Manager Administrators role.
2. Click **Administration**.
3. At the bottom of the navigation pane, click **Discovery Wizard**.
4. On the **Discovery Type** page, click **Unix/Linux computers**.
5. On the **Discovery Criteria** page, do the following:
   a. Click **Add** to define a discovery scope. In the **Discovery Criteria** dialog box, do the following:
      i. For the **Discovery scope**, click the ellipsis button **…** to specify the host name, IP address, or range of IP addresses of the UNIX- or Linux-based computers to be discovered.
      ii. For the **Discovery type** select **Discover all computers** or **Discover only computers with the UNIX/Linux agent installed**.

      If you choose to discover only computers with the agent installed, the only credential that you will need to provide is for the agent verification. This can be a low-privileged account on the UNIX or Linux computer.

      Security
      Discovering only computers with the agent installed requires that the agent is currently installed and configured with a signed certificate.

      iii. To specify the credentials for installing an agent, click **Set credentials**. For detailed instructions, see “Credentials for Installing Agents” in Setting Credentials for Accessing UNIX and Linux Computers.
      iv. Click **Save**.
   b. Select a management pool to monitor the UNIX or Linux computer.

      Note
      The option will be changed from **management pool** to **resource pool** in the final release of Operations Manager.
6. Click **Discover** to display the **Discovery Progress** page. The time it takes to finish discovery depends on many factors, such as the criteria specified and the configuration of the environment. If a large number (100 or more) of computers are being discovered or agents are being installed, the Operations console will not be usable during discovery and agent installation.
7. On the **Computer Selection** page, on the **Manageable computers** tab, select the computers that you want to be managed. The **Additional results** tab lists any errors and computers that are already being managed.
8. Click **Manage**.
9. On the **Computer Management** page, after the deployment process is completed, click

Done.

You must have, at a minimum, a UNIX/Linux Action Account profile configured with a Monitoring Run As Account to monitor the UNIX or Linux computer. For more information, see How to Configure Run As Accounts and Profiles for UNIX and Linux Access.

Note

Solaris Zones are supported on Solaris 10 or newer versions. In monitoring a computer with Zones, each Zone is treated like a separate computer. You must install the agent on each computer that you want to monitor. Install the agent on the global zone first, because sparse zones share files with the global zone. If you try to install on a sparse zone first, the installation fails. For more information about troubleshooting, see Operating System Issues.

See Also

Operations Manager Agent Installation Methods

Install Agent on Windows Using the Discovery Wizard

Install Agent Using the MOMAgent.msi Setup Wizard

Install Agent Using the Command Line

Install Agent and Certificate on UNIX and Linux Computers Using the Command Line

Managing Certificates for UNIX and Linux Computers

Process Manual Agent Installations

Applying Overrides to Object Discoveries

Configuring Agents

Examples of Using MOMAgent Command to Manage Agents

Upgrading and Uninstalling Agents on UNIX and Linux Computers

Manually Uninstalling Agents from UNIX and Linux Computers

Uninstall Agent from Windows-based Computers

Install Agent Using the MOMAgent.msi Setup Wizard

Use the following procedure to deploy the System Center 2012 – Operations Manager agent on computers running Windows by using the MOMAgent.msi setup wizard. For a list of the supported operating system versions, see Supported Configurations.

Before you use the Setup Wizard, ensure the following conditions are met:

- Each agent that is installed with the Setup Wizard must be approved by a management group. For more information, see Process Manual Agent Installations.
- If an agent is manually deployed to a domain controller and an Active Directory management pack is later deployed, errors might occur during deployment of the management pack. To prevent errors from occurring before deploying the Active Directory management pack, or to recover from errors that might have already occurred, you need to deploy the Active Directory management pack helper object by running the file OomADs.msi on the affected domain

controller. The file OomADs.msi is on the computer that is hosting the agent at C:\Program Files\System Center Operations Manager\Agent\HelperObjects. After an agent has been manually deployed to a domain controller, locate OomADs.msi and double-click the file to install the Active Directory Management Pack helper object. The Active Directory Management Pack helper object is automatically installed when the agent is deployed using the Discovery Wizard.

Note
For information about port requirements for agents, see Agent and Agentless Monitoring in the Deployment Guide.

To deploy the Operations Manager agent with the Agent Setup Wizard

1. Use local administrator privileges to log on to the computer where you want to install the agent.
2. On the Operations Manager installation media, double-click **Setup.exe**.
3. In **Optional Installations**, click **Local agent**.
4. On the **Welcome** page, click **Next**.
5. On the **Destination Folder** page, leave the installation folder set to the default, or click **Change** and type a path, and then click **Next**.
6. On the **Management Group Configuration** page, do one of the following:
   - Leave the **Specify Management Group information** check box selected, and then click **Next**.
   - Clear the **Specify Management Group information** check box if management group information has been published to Active Directory Domain Services, and then click **Next**.

     Note
     Step 7 is bypassed by the Agent Setup Wizard if the **Specify Management Group information** check box is cleared.
7. On the **Management Group Configuration** page, do the following:
   a. Type the name of the management group in the **Management Group Name** field and the (which server?) server name in the **Management Server** field.

      Note
      To use a gateway server, enter the gateway server name in the **Management Server** text box.
   b. Type a value for **Management Server Port**, or leave the default of 5723.
   c. Click **Next**.
8. On the **Agent Action Account** page, leave it set to the default of **Local System**, or select **Domain or Local Computer Account**; type the **User Account**, **Password**, and **Domain or local computer**; and then click **Next**.
9. On the **Microsoft Update** page, select **Use Microsoft Update when I check for updates (recommended)** or **I don't want to use Microsoft Update**, and then click

Next.

10. On the **Ready to Install** page, review the settings and then click **Install** to display the **Installing System Center Operations Manager Agent** page.
11. When the **Completing the Operations Manager Agent Setup Wizard** page appears, click **Finish**.

See Also

Operations Manager Agent Installation Methods

Install Agent on Windows Using the Discovery Wizard

Install Agent on UNIX and Linux Using the Discovery Wizard

Install Agent Using the Command Line

Install Agent and Certificate on UNIX and Linux Computers Using the Command Line

Managing Certificates for UNIX and Linux Computers

Process Manual Agent Installations

Applying Overrides to Object Discoveries

Configuring Agents

Examples of Using MOMAgent Command to Manage Agents

Upgrading and Uninstalling Agents on UNIX and Linux Computers

Manually Uninstalling Agents from UNIX and Linux Computers

Uninstall Agent from Windows-based Computers

Install Agent Using the Command Line

You can use MOMAgent.msi to deploy System Center 2012 – Operations Manager agents from the command line. Deploying agents from the command line is also referred to as a manual install.

Before you begin deployment, ensure the following conditions have been met:

- The account that is used to run MOMAgent.msi must have administrative privileges on the computers on which you are installing agents.
- A management group (or single management server) must be configured to accept agents installed with MOMAgent.msi or they will be automatically rejected and therefore not display in the Operations console. For more information, see Process Manual Agent Installations. If the management group or server is configured to accept manually installed agents after the agents have been manually installed, the agents will display in the console after approximately one hour.
- If an agent is manually deployed to a domain controller and an Active Directory management pack is later deployed, errors might occur during deployment of the management pack. To prevent errors from occurring before deploying the Active Directory management pack, or to recover from errors that might have already occurred, you need to deploy the Active Directory management pack helper object by running the file OomADs.msi on the affected domain controller. The file OomADs.msi is on the computer that is hosting the agent at C:\Program

Files\System Center Operations Manager\Agent\HelperObjects. After an agent has been manually deployed to a domain controller, locate OomADs.msi and double-click the file to install the Active Directory Management Pack helper object. The Active Directory Management Pack helper object is automatically installed when the agent is deployed using the Discovery Wizard.

- Each agent that is installed with MOMAgent.msi must be approved for a management group.

MOMAgent.msi can be found in the Operations Manager installation media and the management server installation directory.

Use the following procedure to deploy an agent. For examples of ways in which you can customize the MOMAgent.msi command, see Examples of Using MOMAgent Command to Manage Agents.

To deploy the Operations Manager agent from the command line

1. Log on to the computer where you want to install the agent by using an account with local administrator privileges.
2. Open a command window.
3. Run the following command:

```
%WinDir%\System32\msiexec.exe /i path\Directory\MOMAgent.msi
/qn USE_SETTINGS_FROM_AD={0|1}
USE_MANUALLY_SPECIFIED_SETTINGS={0|1} MANAGEMENT_GROUP=MGname
MANAGEMENT_SERVER_DNS=MSname MANAGEMENT_SERVER_AD_NAME
=MSname SECURE_PORT=PortNumber
ACTIONS_USE_COMPUTER_ACCOUNT={0|1} ACTIONSUSER=UserName
ACTIONSDOMAIN=DomainName ACTIONSPASSWORD=Password
AcceptEndUserLicenseAgreement=1
```

Note
Ensure you use the correct 32-bit or 64-bit version of MOMAgent.msi for the computer you are installing the agent on.

where:

USE_SETTINGS_FROM_AD={0|1}	Indicates whether the management group settings properties will be set on the command line. Use 0 if you want to set the properties at the command line. Use 1 to use the management group settings from Active Directory.
USE_MANUALLY_SPECIFIED_SETTINGS ==={0|1}	If USE_SETTINGS_FROM_AD=1, then USE_MANUALLY_SPECIFIED_SETTI

	NGS must equal 0.
MANAGEMENT_GROUP=*MGname*	Specifies the management group that will manage the computer.
MANAGEMENT_SERVER_DNS=*MSname*	Specifies the fully qualified domain name for the management server. To use a gateway server, enter the gateway server FQDN as **MANAGEMENT_SERVER_DNS**.
MANAGEMENT_SERVER_AD_NAME=*ADname*	Use this parameter if the computer's DNS and Active Directory names differ to set to the fully qualified Active Directory Domain Services name.
SECURE_PORT=*PortNumber*	Sets the health service port number.
ENABLE_ERROR_REPORTING={0|1}	Optional parameter. Use this parameter with “1” to opt in to error report forwarding to Microsoft. If you do not include this parameter, the agent installation defaults to “0”, which opts out of error report forwarding.
QUEUE_ERROR_REPORTS={0|1}	Optional parameter. Use this parameter with “1” to queue error reports or with “0” to send reports immediately. If you do not include this parameter, the agent installation defaults to “0”.
INSTALLDIR=*path*	Optional parameter. Use this parameter if you want to install the agent to a folder other than the default installation path. Note that \Agent will be appended to this value.
ACTIONS_USE_COMPUTER_ACCOUNT={0|1}	Indicates whether to use a specified user account (0) or the Local System account (1).
ACTIONSUSER=*UserName*	Sets the Agent Action account to *UserName*. This parameter is required if you specified ACTIONS_USE_COMPUTER_ACCOUNT=0.
ACTIONSDOMAIN= *DomainName*	Sets the domain for the Agent Action

	account identified with the ACTIONSUSER parameter.
ACTIONSPASSWORD= *Password*	The password for the user identified with the ACTIONSUSER parameter.
NOAPM=1	Optional parameter. Installs the Operations Manager agent without .NET Application Performance Monitoring. If you are using AVIcode 5.7, NOAPM=1 leaves the AVIcode agent in place. If you are using AVIcode 5.7 and install the Operations Manager agent by using momagent.msi without NOAPM=1, the AVIcode agent will not work correctly and an alert will be generated.
AcceptEndUserLicenseAgreement=1	Used to specify that you accept the End User License Agreement (EULA).

See Also

Operations Manager Agent Installation Methods

Install Agent on Windows Using the Discovery Wizard

Install Agent on UNIX and Linux Using the Discovery Wizard

Install Agent Using the MOMAgent.msi Setup Wizard

Install Agent and Certificate on UNIX and Linux Computers Using the Command Line

Managing Certificates for UNIX and Linux Computers

Process Manual Agent Installations

Applying Overrides to Object Discoveries

Configuring Agents

Examples of Using MOMAgent Command to Manage Agents

Upgrading and Uninstalling Agents on UNIX and Linux Computers

Manually Uninstalling Agents from UNIX and Linux Computers

Uninstall Agent from Windows-based Computers

Install Agent and Certificate on UNIX and Linux Computers Using the Command Line

Your environment may require that you manually install the agent. Use the following procedures to manually install agents to UNIX and Linux computers for monitoring in System Center 2012 – Operations Manager and System Center 2012 Service Pack 1 (SP1), Operations Manager.

To install the agent on Red Hat Enterprise Linux and SUSE Linux Enterprise Server

1. Transfer the agent (`scx-<version>-<os>-<arch>.rpm`) to the Linux server, type:

   ```
   scx-<version>-<os>-<arch>.rpm
   ```

2. To install the package, type:

   ```
   rpm -i scx-<version>-<os>-<arch>.rpm
   ```

3. To verify that the package is installed, type:

   ```
   rpm -q scx
   ```

4. To verify that the Microsoft SCX CIM Server is running, type:

   ```
   service scx-cmid status
   ```

To install the agent on RPM based Universal Linux Servers (Oracle and Centos)

1. Transfer the agent (`scx-<version>-universalr-<arch>.rpm`) to the Linux server. This should be done via SCP or FTP in binary mode.
2. To install the package, type:

   ```
   rpm -i scx-<version>-universalr-<arch>.rpm
   ```

3. To verify that the package is installed, type:

   ```
   rpm -q scx
   ```

4. To verify that the Microsoft SCX CIM Server is running, type:

   ```
   scxadmin -status
   ```

To install the agent on DPKG-based Universal Linux Servers (Debian and Utuntu)

1. Transfer the agent (`scx-<version>-universald-<arch>.rpm`) to the Linux server. This should be done via SCP or FTP in binary mode.
2. To install the package, type:

   ```
   dpkg -i scx-<version>-universald-<arch>.deb
   ```

3. To verify that the package is installed, type:

   ```
   dpkg -l scx
   ```

4. To verify that the Microsoft SCX CIM Server is running, type:

   ```
   scxadmin -status
   ```

To install the agent on Solaris

1. Transfer the agent (`scx-<version>-<os>-<arch>.pkg.Z`) to the Solaris server, type:

   ```
   scx-<version>-<os>-<arch>.pkg.Z
   ```

2. Run the following command:

   ```
   uncompress scx-<version>-<os>-<arch>.pkg.Z
   ```

3. To install the package, type:

```
pkgadd -d scx-<version>-<os>-<arch>.pkg MSFTscx
```

4. To verify that the package is installed, type:

   ```
   pkginfo -l MSFTscx
   ```

5. To verify that the Microsoft SCX CIM Server is running, type:

   ```
   svcs scx-cimd
   ```

To install the agent on HP-UX

1. Transfer the agent (`scx-<version>-<os>-<arch>.gz`) to the HP server:

   ```
   cp scx-<version>-<os>-<arch>.gz
   ```

2. To unzip the package, type:

   ```
   gzip -d scx-<version>-<os>-<arch>.gz
   ```

3. To install the package, type:

   ```
   swinstall -s /path/scx-<version>-<os>-<arch> scx
   ```

4. To verify that the package is installed, type:

   ```
   swlist scx
   ```

5. To verify that the Microsoft SCX CIM Server is running, type:

   ```
   ps -ef|grep scx
   ```

   Look for the following process in the list:

   ```
   scxcimserver
   ```

To install the agent on AIX

1. Transfer the agent (`scx-<version>-<os>-<arch>.gz`) to the AIX server, type:

   ```
   cp scx-<version>-<os>-<arch>.gz
   ```

2. To unzip the package, type:

   ```
   gzip -d scx-<version>-<os>-<arch>.gz
   ```

3. To install the package, type:

   ```
   /usr/sbin/installp -a -d scx-<version>-<os>-<arch> scx
   ```

4. To verify that the package is installed, type:

   ```
   swlist scx
   ```

5. To verify that the Microsoft SCX CIM Server is running, type:

   ```
   ps -ef|grep scx
   ```

   Look for the following process in the list:

   scxcimserver

Signing Agent Certificates

When you manually deploy an agent, you perform the first two steps that are typically handled by the Discovery Wizard, deployment and certificate signing. Then, you use the Discovery Wizard to add the computer to the Operations Manager database.

If there are existing certificates on the system, they are reused during agent installation. New certificates are not created. Certificates are not automatically deleted when you uninstall an agent. You must manually delete the certificates that are listed in the `/etc/opt/microsoft/scx/ssl` folder. To regenerate the certificates at install, you must remove this folder before agent installation.

You must have already manually installed an agent before you start this procedure. You will need a root or elevated account to perform the procedure.

To install certificates for UNIX and Linux support

1. On the computer that is running the UNIX or Linux operating system, locate the file `/etc/opt/microsoft/scx/ssl/scx-host-<hostname>.pem` and securely copy or transfer it to any location on the computer that is hosting Operations Manager.
2. On the computer that is hosting Operations Manager, on the Windows desktop, click **Start**, and then click **Run**.
3. In the **Run** dialog box, type **cmd**, and then press **Enter**.
4. Change directories to the location where you copied the `pem` file.
5. Type the command `scxcertconfig -sign scx-host-<hostname>.pem scx_new.pem`, and then press **Enter**. This command will self-sign your certificate (`scx-host-<hostname>.pem`) and then save the new certificate (`scx-host-<hostname>_new.pem`).

   Note
   Ensure that the location where Operations Manager is installed is in your path statement, or use the fully qualified path of the `scxcertconfig.exe` file.
6. Securely copy or transfer the `scx_new.pem` file into the `/etc/opt/microsoft/scx/ssl` folder on the computer that is hosting the UNIX or Linux operating system. This replaces the `original scx-host-<hostname>.pem` file.
7. Restart the agent by typing `scxadmin -restart`.

Discovering Computers after Manual Deployment

After you have manually deployed agents to UNIX and Linux computers, they still need to be discovered by Operations Manager by using the Discovery Wizard. For the **Discovery type**, select **Discover only computers with the UNIX/Linux agent installed**. For more information see Install Agent on UNIX and Linux Using the Discovery Wizard.

See Also

Operations Manager Agent Installation Methods

Install Agent on Windows Using the Discovery Wizard

Install Agent on UNIX and Linux Using the Discovery Wizard

Install Agent Using the MOMAgent.msi Setup Wizard

Install Agent Using the Command Line

Process Manual Agent Installations

Applying Overrides to Object Discoveries

Configuring Agents

Examples of Using MOMAgent Command to Manage Agents

Managing Certificates for UNIX and Linux Computers

Upgrading and Uninstalling Agents on UNIX and Linux Computers

Manually Uninstalling Agents from UNIX and Linux Computers

Uninstall Agent from Windows-based Computers

Managing Certificates for UNIX and Linux Computers

With System Center 2012 – Operations Manager, you can deploy agents to UNIX or Linux computers. Kerberos authentication is not possible. Therefore, certificates are used between the management server and the UNIX or Linux computers. In this scenario, the certificates are self-signed by the management server. (Although it is possible to use third-party certificates, they are not needed.)

There are two methods you can use to deploy agents. You can use the Discovery Wizard or you can manually install an agent. Of these two methods, manually installing an agent is the more secure option. When you use the Discovery Wizard to push agents to UNIX or Linux computers, you trust that the computer that you are deploying to is really the computer that you think it is. When you use the Discovery Wizard to deploy agents, it involves greater risk than when you deploy to computers on the public network or in a perimeter network.

When you use the Discovery Wizard to deploy an agent, the Discovery Wizard performs the following functions:

Deployment	The Discovery Wizard copies the agent package to the UNIX or Linux computer and then starts the installation process.
Certificate Signing	Operations Manager retrieves the certificate from the agent, signs the certificate, deploys the certificate back to the agent, and then restarts the agent.
Discovery	The Discovery Wizard discovers the computer and tests to see that the certificate is valid. If the Discovery Wizard verifies that the computer can be discovered and that the certificate is valid, the Discovery Wizard adds the newly

	discovered computer to the Operations Manager database.

When you manually deploy an agent, you perform the first two steps that are typically handled by the Discovery Wizard: deployment and certificate signing. Then, you use the Discovery Wizard to add the computer to the Operations Manager database.

If there are existing certificates on the system, they are reused during agent installation. New certificates are not created. Certificates are not automatically deleted when you uninstall an agent. You must manually delete the certificates that are listed in the /etc/opt/microsoft/scx/ssl folder. To regenerate the certificates during instalation, you must remove this folder before agent installation.

For instructions on how to manually deploy an agent, see Install Agent and Certificate on UNIX and Linux Computers Using the Command Line, and then use the following procedure to install the certificates.

UNIX and Linux Firewall Considerations

If you have a firewall on your UNIX or Linux computer, you must open port 1270 (inbound). This port number is not configurable. If you are deploying agents in a low security environment and you use the Discovery Wizard to deploy and sign the certificates, you must open the SSH port. The SSH port number is configurable. By default, SSH uses inbound TCP port 22.

See Also

Operations Manager Agent Installation Methods

Install Agent on Windows Using the Discovery Wizard

Install Agent on UNIX and Linux Using the Discovery Wizard

Install Agent Using the MOMAgent.msi Setup Wizard

Install Agent Using the Command Line

Install Agent and Certificate on UNIX and Linux Computers Using the Command Line

Process Manual Agent Installations

Applying Overrides to Object Discoveries

Configuring Agents

Examples of Using MOMAgent Command to Manage Agents

Upgrading and Uninstalling Agents on UNIX and Linux Computers

Manually Uninstalling Agents from UNIX and Linux Computers

Uninstall Agent from Windows-based Computers

Process Manual Agent Installations

Manual installation of an agent refers to the process of running MOMAgent.msi locally on a computer that is to host a System Center 2012 – Operations Manager agent. When it is installed, the agent attempts to join the specified management group by contacting a specified

management server. You can use security settings at both the management group and the management server level to configure how requests from manually installed agents are processed.

The following three options are available to process manually installed agents.

Option	Action
Reject new manual agent installations	Designates that all requests from a manually installed agent will be denied by Operations Manager. This is the most secure setting and is selected by default.
Review new manual agent installations in pending management view	Designates that all requests from a manually installed agent will be directed to Pending Management before being allowed to join the management group. An administrator must review the request and manually approve the agents' request.
Auto-approve new manually installed agents	This option is available only if **Review new manual agent installations in pending management view** has been selected. This setting causes Operations Manager to automatically allow any manually installed agent to join the management group. This is the least secure option.

Important

A management group or management server must be configured to accept agents that are installed with MOMAgent.msi or they will be automatically rejected and therefore not displayed in the Operations console. If a management group is configured to accept manually installed agents, the agents will display in the console approximately one hour after they are installed.

The following procedures show you how to configure settings for manual agent installations.

To configure manual agent installation settings for a management group

1. Log on to the Operations console with an account that is a member of the Operations Manager Administrators role.
2. Click **Administration**.
3. In the Administration workspace, expand **Administration**, and then click **Settings**.
4. In the **Settings** pane, expand **Type: Server**, right-click **Security**, and then click **Properties**.
5. In the **Global Management Server Settings - Security** dialog box, on the **General** tab,

do one of the following:

- To maintain a higher level of security, click **Reject new manual agent installations**, and then click **OK**.
- To configure for manual agent installation, click **Review new manual agent installations in pending management view**, and then click **OK**.
- Optionally, select **Auto-approve new manually installed agents**.

To override the manual agent installation setting for a single management server

1. Log on to the Operations console with an account that is a member of the Operations Manager Administrators role.
2. Click **Administration**.
3. In the **Administration** workspace, expand **Administration**, expand **Device Management**, and then click **Management Servers**.
4. In the results pane, right-click the management server that you want to view the properties of, and then click **Properties**.
5. In the **Management Server Properties** dialog box, click the **Security** tab.
6. On the **Security** tab, do the following:
   - To maintain a higher level of security, select **Reject new manual agent installations**, and then click **OK**.
   - To configure for manual agent installation, click **Review new manual agent installations in pending management view**, and then click **OK**.
   - Optionally, select **Auto-approve new manually installed agents**.
7. Click **OK**.

To approve a pending agent installation when automatic approval is not configured

1. In the Operations console, click **Administration**.
2. Click **Pending Management**.
3. In the **Pending Management** pane, select computers in **Type: Manual Agent Install**.
4. Right-click the computers, and then click **Approve**.
5. In the **Manual Agent Install** dialog box, click **Approve**. The computers now appear in the **Agent Managed** node and are ready to be managed.

   Note
   Rejected agents remain in **Pending Management** until the agent is uninstalled for the management group.

See Also

Operations Manager Agent Installation Methods

Install Agent on Windows Using the Discovery Wizard

Install Agent on UNIX and Linux Using the Discovery Wizard

Install Agent Using the MOMAgent.msi Setup Wizard

Install Agent and Certificate on UNIX and Linux Computers Using the Command Line

Managing Certificates for UNIX and Linux Computers

Install Agent Using the Command Line

Applying Overrides to Object Discoveries

Configuring Agents

Examples of Using MOMAgent Command to Manage Agents

Upgrading and Uninstalling Agents on UNIX and Linux Computers

Manually Uninstalling Agents from UNIX and Linux Computers

Uninstall Agent from Windows-based Computers

Applying Overrides to Object Discoveries

System Center 2012 – Operations Manager monitors computers and devices that it has discovered, and it also discovers applications and features that it discovers on monitored computers. There may be situations where you want to limit discovery. For example, you might want only some instances of SQL Server to be discovered and monitored, or you want to remove a computer that has already been discovered.

The precise steps to limit or restrict discovery depend on the object, application, or feature that you want to exclude from discovery. However, the general procedure is the same: identify the discovery that you want to limit and create an override to disable the discovery. For information on how to create an override, see How to Override a Rule or Monitor.

The override to disable the discovery can apply to:

- All objects in the class that the discovery applies to. If you use this selection for your override, you disable the discovery completely.
- A group. Group membership can be defined explicitly or dynamically. When you create a group, you save it to an unsealed management pack. However, an element in an unsealed management pack, such as an override, cannot reference an element in a different unsealed management pack, such as a group. If you are going to use a group to limit the application of an override, you must either save the group to the same unsealed management pack as the override, or you must seal the management pack that contains the group. For more information, see Creating and Managing Groups.
- One or more specific objects in the class that the discovery applies to. Using this method, you can select from discovered objects.
- All objects of another class. Using this method, you specify a class of objects to apply the override to.

Choosing how to apply the override to disable the discovery depends on your situation. The simplest situation is when you want to disable discovery for a specific object or for all objects in a class. When you want to disable the discovery for any object that meets certain criteria, you must use a group that contains those objects or create a group that will identify those objects.

For example, you want to disable discovery of logical disks on management servers. You can configure an override to disable the discovery of Windows Server 2008 logical disks and apply it to the Operations Manager Management Servers group which is created automatically when you install Operations Manager. If, instead, you want to disable discovery of logical disks on computers in a specific organizational unit, there is no built-in group that satisfies that definition and so you would need to create a group that identifies those computers.

After an object has been already discovered, if you want to delete the object and not let it be discovered again, disable the discovery for that object and then run the **Remove-SCOMDisabledClassInstance** cmdlet in Operations Manager Shell. For help with this cmdlet, open Operations Manager Shell, and then type **Get-Help Remove-SCOMDisabledClassInstance**.

See Also

Operations Manager Agent Installation Methods

Install Agent on Windows Using the Discovery Wizard

Install Agent on UNIX and Linux Using the Discovery Wizard

Install Agent Using the MOMAgent.msi Setup Wizard

Install Agent and Certificate on UNIX and Linux Computers Using the Command Line

Managing Certificates for UNIX and Linux Computers

Process Manual Agent Installations

Install Agent Using the Command Line

Configuring Agents

Examples of Using MOMAgent Command to Manage Agents

Upgrading and Uninstalling Agents on UNIX and Linux Computers

Manually Uninstalling Agents from UNIX and Linux Computers

Uninstall Agent from Windows-based Computers

Configuring Agents

In System Center 2012 – Operations Manager, when you install an agent on a computer, an Operations Manager Agent application is added to Control Panel. You can use the application to change the account that the agent will use when performing actions requested by the management server, to remove a management group from an agent configuration, and to configure the Active Directory integration setting for the agent. To perform these tasks, you must have local Administrator permissions on the computer.

Note

If you want to automate the process of adding or removing management groups from an agent, you can use the Agent API that allows you to write scripts that can automate the agent configuration process. For more information, see Using the Operations Manager Agent Configuration Library.

Note

When you save changes in the Operations Manager Agent application, the Health service will be stopped and restarted.

- Configuring an Agent to Report to Multiple Management Groups
- Changing the Account Configuration for an Agent
- Removing a Management Group from an Agent
- Changing the Active Directory Integration Setting for an Agent

Configuring an Agent to Report to Multiple Management Groups

Use the following procedure to make an Operations Manager agent a member of multiple management groups, also referred to as *multihoming*. For example, an agent can be configured to report Active Directory data to the Networking Management Group and Exchange data to the Messaging Management Group. An agent can be a member of up to four management groups.

You do not need to use the same deployment method for all of the management groups.

Note

It might take one day or longer for the discovered instances of the agent to be made part of the new management group. They will be added after the next discovery interval.

To make an Operations Manager agent a member of multiple management groups

- Do one of the following:
  - On the agent-managed computer, in Control Panel, double-click Operations Manager Agent. (In the category view of Control Panel in Windows Server 2008, Operations Manager Agent is in the **System and Security** category.) In **Operations Manager Agent**, on the **Management Groups** tab, click **Add**, enter the information for the new management group, and then click **OK**.
  - Run the Discovery Wizard from the Operations Manager Operations console that is connected to the new management group, select the desired computers, and deploy the agent to them. For more information, see Install Agent on Windows Using the Discovery Wizard. (The menu item in the Operations console named Discovery Wizard opens the Computer and Device Management Wizard.)
  - Run the MOMAgent.msi on the desired computers, and modify the installation by adding a new management group. For more information, see Install Agent Using the MOMAgent.msi Setup Wizard.

Changing the Account Configuration for an Agent

You can use the following procedure to change the account that the agent will use when performing actions requested by the management server.

To change the account configuration for an agent

1. On the agent-managed computer, in Control Panel, double-click Operations Manager Agent. (In the category view of Control Panel in Windows Server 2008, Operations

Manager Agent is in the **System and Security** category.)

2. On the **Management Group** tab, select a management group and then click **Edit**.
3. In the **Agent Action Account** section, edit the account information and then click **OK**.

Removing a Management Group from an Agent

You can use the following procedure to remove a management group from the agent configuration.

To remove a management group from an agent

1. On the agent-managed computer, in Control Panel, double-click Operations Manager Agent. (In the category view of Control Panel in Windows Server 2008, Operations Manager Agent is in the **System and Security** category.)
2. On the **Management Group** tab, select a management group and then click **Remove**.
3. Click **OK**.

> **Note**
> You can remove all management groups while leaving the agent installed. This is useful in situations such as when you want to prepare a computer for imaging and want an image with the agent installed but without assignment to a specific management group.

Changing the Active Directory Integration Setting for an Agent

You can use the following procedure to change the Active Directory integration setting for an agent.

To change the Active Directory integration setting for an agent

1. On the agent-managed computer, in Control Panel, double-click Operations Manager Agent. (In the category view of Control Panel in Windows Server 2008, Operations Manager Agent is in the **System and Security** category.)
2. On the **Management Group** tab, clear or select **Automatically update management group assignments from AD DS**. If you select this option, on agent startup, the agent will query Active Directory for a list of management groups to which it has been assigned. Those management groups, if any, will be added to the list. If you clear this option, all management groups assigned to the agent in Active Directory will be removed from the list.
3. Click **OK**.

See Also

Operations Manager Agent Installation Methods

Install Agent on Windows Using the Discovery Wizard

Install Agent on UNIX and Linux Using the Discovery Wizard

Install Agent Using the MOMAgent.msi Setup Wizard

Install Agent and Certificate on UNIX and Linux Computers Using the Command Line
Managing Certificates for UNIX and Linux Computers
Process Manual Agent Installations
Applying Overrides to Object Discoveries
Install Agent Using the Command Line
Examples of Using MOMAgent Command to Manage Agents
Upgrading and Uninstalling Agents on UNIX and Linux Computers
Manually Uninstalling Agents from UNIX and Linux Computers
Uninstall Agent from Windows-based Computers

Examples of Using MOMAgent Command to Manage Agents

The following examples show different ways in which you can use the MOMAgent command. You can use this command to perform new installations of agents, upgrade agents from previous releases of Operations Manager, or change the configuration of an agent (such as the management group or management server associated with the agent).

Agent installation using a specific Action Account

The following example shows a fresh installation of an agent and uses a specific Action Account.

```
msiexec.exe /i path\Directory\MOMAgent.msi /qn /l*v %temp%
MOMAgentinstall.log USE_SETTINGS_FROM_AD=0 MANAGEMENT_GROUP=<MG_Name>
MANAGEMENT_SERVER_DNS=<MSDNSName> MANAGEMENT_SERVER_AD_NAME=<MSDNSName>
ACTIONS_USE_COMPUTER_ACCOUNT=0 ACTIONSUSER=<AccountUser> ACTIONSDOMAIN=<AccountDomain>
ACTIONSPASSWORD=<AccountPassword> USE_MANUALLY_SPECIFIED_SETTINGS=1
```

Agent installation using the Local System account

The following example shows a fresh installation of an agent and uses the Local System for the Action Account.

```
msiexec.exe /i path\Directory\MOMAgent.msi /qn /l*v
%temp%\MOMAgentinstall.log USE_SETTINGS_FROM_AD=0 MANAGEMENT_GROUP=<MG_Name>
MANAGEMENT_SERVER_DNS=<MSDNSName> MANAGEMENT_SERVER_AD_NAME=<MSDNSName>
ACTIONS_USE_COMPUTER_ACCOUNT=1 USE_MANUALLY_SPECIFIED_SETTINGS=1
```

Agent installation with Active Directory integration and using a specific Action Account

The following example installs an agent by using Active Directory and a specific Action Account.

```
msiexec /i path\Directory\MOMAgent.msi /qn /l*v %temp%mominst.NoGroupSpecified.log
USE_SETTINGS_FROM_AD=1 USE_MANUALLY_SPECIFIED_SETTINGS=0 ACTIONS_USE_COMPUTER_ACCOUNT=0
ACTIONSUSER=<AccountUser> ACTIONSDOMAIN=<AccountDomain>
ACTIONSPASSWORD=<AccountPassword>
```

Agent installation with Active Directory integration and using the Local System account

The following example installs an agent by using Active Directory and the Local system account for the Action Account.

```
msiexec /i path\Directory\MOMAgent.msi /qn /l*v %temp%\ mominst.NoGroupSpecified.log
USE_SETTINGS_FROM_AD=1 ACTIONS_USE_COMPUTER_ACCOUNT=1 USE_MANUALLY_SPECIFIED_SETTINGS=0
```

Agent upgrade from a previous release of Operations Manager

The following example upgrades an agent.

```
msiexec /i path\Directory\MOMAgent.msi /qn /l*v %temp%\MOMAgentUpgrade.log
```

Uninstall the agent

The following example uninstalls an agent.

```
msiexec /x path\Directory\MOMAgent.msi /qn %temp%\MOMAgentUpgrade.log
```

See Also

Operations Manager Agent Installation Methods

Install Agent on Windows Using the Discovery Wizard

Install Agent on UNIX and Linux Using the Discovery Wizard

Install Agent Using the MOMAgent.msi Setup Wizard

Install Agent and Certificate on UNIX and Linux Computers Using the Command Line

Managing Certificates for UNIX and Linux Computers

Process Manual Agent Installations

Applying Overrides to Object Discoveries

Configuring Agents

Install Agent Using the Command Line

Upgrading and Uninstalling Agents on UNIX and Linux Computers

Manually Uninstalling Agents from UNIX and Linux Computers

Uninstall Agent from Windows-based Computers

Upgrading and Uninstalling Agents on UNIX and Linux Computers

This topic describes how to upgrade and uninstall agents on UNIX and Linux computers, using the **UNIX/Linux Agent Upgrade Wizard** and the **UNIX/Linux Agent Uninstall Wizard**. These wizards are similar in how you select the target computers and provide credentials. Both wizards require privileged credentials on the UNIX or Linux computers to complete their tasks, for more information see Accessing UNIX and Linux Computers in Operations Manager.

Upgrading Agents

You must run the **UNIX/Linux Agent Upgrade Wizard** to upgrade agents from earlier versions, or when updates are issued by Microsoft, for of Operations Manager.

To Upgrade an Agent

1. In the Operations Console click **Administration**.
2. Click **UNIX/Linux Computers** in the **Device Management node**.
3. In the **Actions** pane, click **Upgrade Agent** to start the **UNIX/Linux Agent Upgrade Wizard**.
4. In the **Select Upgrade Targets** page, all applicable computers that have the installed agent will be selected by default for upgrade. Unselect any targets you do not want to upgrade.
5. On the **Credentials** page, select one of the credentials options.

   If you select the option to use existing credentials and are alerted that one or more of the selected target computers does not have a Run As account assigned with the required profiles, you must do one of the following:

   - Provide specified credentials with the **Provide upgrade credentials** option.
   - Click **Show Computers** (in the alert text) for a list of the computers that do not have the required credentials specified in Run As Accounts. Then click **Previous** to unselect them and try again.

   For detailed instructions on how to set credentials, see How to Set Credentials for Accessing UNIX and Linux Computers.
6. Click **Upgrade**.

Uninstalling Agents

You can uninstall an agent from the targeted computer by using the **UNIX/Linux Agent Uninstall Wizard**. For information on manually uninstalling agents, see Manually Uninstalling Agents from UNIX and Linux Computers.

To Uninstall an Agent

1. In the Operations Console click **Administration**.
2. Click **UNIX/Linux Computers** in the **Device Management** node.
3. In the **Actions** pane, click **Uninstall Agent** to start the **UNIX/Linux Agent Uninstall Wizard**.
4. In the **Select Uninstall Targets** page, all applicable computers that have the installed agent will be selected by default for uninstallation. Unselect any targets you do not want to uninstall.
5. On the **Credentials** page, select one of the credentials options.

   If you select the option to use existing credentials and are alerted that one or more of the

selected target computers does not have a Run As account assigned, you must do one of the following:

- Provide specified credentials with the **Provide uninstall credentials** option.
- Click **Show Computers** (in the alert text) for a list of the computers does not have the required credentials specified in Run As Accounts. Then click **Previous** to unselect them and try again.

For detailed instructions on how to set credentials, see How to Set Credentials for Accessing UNIX and Linux Computers.

6. Click **Uninstall**.

See Also

Operations Manager Agent Installation Methods

Install Agent on Windows Using the Discovery Wizard

Install Agent on UNIX and Linux Using the Discovery Wizard

Install Agent Using the MOMAgent.msi Setup Wizard

Install Agent and Certificate on UNIX and Linux Computers Using the Command Line

Managing Certificates for UNIX and Linux Computers

Process Manual Agent Installations

Applying Overrides to Object Discoveries

Configuring Agents

Examples of Using MOMAgent Command to Manage Agents

Install Agent Using the Command Line

Manually Uninstalling Agents from UNIX and Linux Computers

Uninstall Agent from Windows-based Computers

Upgrading Agents on UNIX and Linux Computers Using the Command Line

Your environment may require that you manually upgrade an agent. Use the following procedures to manually upgrade agents to UNIX and Linux computers for monitoring in System Center 2012 Service Pack 1 (SP1), Operations Manager.

Note

During the upgrade the certificate is not removed, and once upgraded the agent will still be managed by System Center 2012 – Operations Manager.

Once you have installed the required UNIX\Linux Management Pack Bundles [MPBs] into System Center 2012 Service Pack 1 (SP1), Operations Manager, you will find the agents under:

%Program Files%\System Center 2012\Operations Manager\Server\AgentManagement\UnixAgents\DownloadedKits

To upgrade the agent on Red Hat Enterprise Linux and SUSE Linux Enterprise

1. Transfer the agent `scx-<version>-<os>-<arch>.rpm` to the Linux server. This should be done via SCP or FTP in binary mode.
2. Upgrade the agent:

   ```
   rpm –Uvh  scx-<version>-<os>-<arch>.rpm
   ```
3. Verify that the package is installed:

   ```
   rpm -qa scx
   ```
4. Verify that the Microsoft SCX CIM Server is running:

   ```
   scxadmin -status
   ```
5. Verify that the Microsoft SCX agent was upgraded:

   ```
   scxadmin -v
   ```

To upgrade the agent on Universal RPM based supported Linux OS Servers (Oracle and Centos)

1. Transfer the agent `scx-<version>-universalr-<arch>.rpm` to the Linux server. This should be done via SCP or FTP in binary mode.
2. Upgrade the agent:

   ```
   rpm –Uvh  scx-<version>-universalr-<arch>.rpm
   ```
3. Verify that the package is installed:

   ```
   rpm -qa scx
   ```
4. Verify that the Microsoft SCX CIM Server is running:

   ```
   scxadmin -status
   ```
5. Verify that the Microsoft SCX agent was upgraded:

   ```
   scxadmin -v
   ```

To upgrade the agent on Universal DEB based supported Linux OS Servers (Debian and Ubuntu)

1. Transfer the agent `scx-<version>-universald-<arch>.deb` to the Linux server. This should be done via SCP or FTP in binary mode.
2. Remove the old agent:

   ```
   dpkg –r  scx
   ```
3. Install the new agent:

   ```
   dpkg  –i  scx-<version>-universald-<arch>.deb
   ```
4. Verify that the package is installed:

   ```
   dpkg –l scx
   ```
5. Verify that the Microsoft SCX CIM Server is running:

   ```
   scxadmin -status
   ```
6. Verify that the Microsoft SCX agent was upgraded:

```
scxadmin -v
```

To upgrade the agent on Solaris

1. Transfer the agent `scx-<version>-<os>-<arch>.pkg.Z` to the Solaris server. This should be done via SCP or FTP in binary mode.
2. Uncompress the agent file:

   ```
   uncompress scx-<version>-<os>-<arch>.pkg.Z
   ```
3. Remove the old agent:

   ```
   pkgrm MSFTscx
   ```
4. Install the new agent:

   ```
   pkgadd -d scx-<version>-<os>-<arch>.pkg MSFTscx
   ```
5. Verify that the package is installed:

   ```
   pkginfo –l MSFTscx
   ```
6. Verify that the Microsoft SCX CIM Server is running:

   ```
   scxadmin -status
   ```
7. Verify that the Microsoft SCX agent was upgraded:

   ```
   scxadmin -v
   ```

To upgrade the agent on HP-UX

1. Transfer the agent `scx-<version>-<os>-<arch>.gz` to the HP server. This should be done via SCP or FTP in binary mode.
2. Unzip the package:

   ```
   gzip –d scx-<version>-<os>-<arch>.gz
   ```
3. Remove the old agent:

   ```
   swremove scx
   ```
4. Install the new agent:

   ```
   swinstall –s /path/scx-<version>-<os>-<arch> scx
   ```
5. Verify that the package is installed:

   ```
   swlist scx
   ```
6. Verify that the Microsoft SCX CIM Server is running:

   ```
   scxadmin -status
   ```
7. Verify that the Microsoft SCX agent was upgraded:

   ```
   scxadmin –v
   ```

To install the agent on AIX

1. Transfer the agent `scx-<version>-<os>-<arch>.gz` to the AIX server. This should be done via SCP or FTP in binary mode.

2. Unzip the package:

   ```
   gzip –d scx-<version>-<os>-<arch>.gz
   ```

3. Remove the old agent:

   ```
   installp -u scx
   ```

4. Install the new agent:

   ```
   installp -X -d scx-<version>-<os>-<arch> scx
   ```

5. Verify that the package is installed:

   ```
   lslpp -l scx.rte
   ```

6. Verify that the Microsoft SCX CIM Server is running:

   ```
   scxadmin –status
   ```

7. Verify that the Microsoft SCX agent is upgraded:

   ```
   scxadmin -v
   ```

Manually Uninstalling Agents from UNIX and Linux Computers

There are three ways to uninstall the UNIX and Linux management packs and agents.

1. Delete selected UNIX or Linux system management packs from the Operations Manager Operations Console.
2. Delete an agent from Operations Manager, and uninstall the agent from the monitored computer. It will be uninstalled first from the UNIX or Linux computer.
3. Delete the agent from Operations Manager without uninstalling it on the UNIX or Linux host.

Use the following procedures to uninstall agents.

To delete an agent with the UNIX Linux Agent Uninstall Wizard

1. For more information, see Upgrading and Uninstalling Agents on UNIX and Linux Computers.

After the UNIX or Linux computer has been deleted from the list of monitored computers, you must log on to the monitored computer and manually uninstall the agent. Use the following procedures to manually uninstall agents from UNIX and Linux computers.

To uninstall the agent from Red Hat enterprise Linux and SUSE Linux enterprise servers

1. Log on as the root user, and uninstall the agent by typing

   rpm –e scx

2. To verify that the package is uninstalled, type

   rpm –q scx

To uninstall the agent from RPM based Universal Linux servers (Oracle and Centos)

1. Log on as the root user, and uninstall the agent by typing
   rpm –e scx
2. To verify that the package is uninstalled, type
   rpm –q scx

To uninstall the agent from DEB based Universal Linux servers (Debian and Ubuntu)

1. Log on as the root user, and uninstall the agent by typing
   dpkg –P scx
2. To verify that the package is uninstalled, type
   dpkg –l scx

To uninstall the agent from Solaris computers

1. Log on as the root user, and uninstall the agent by typing
   pkgrm MSFTscx
2. To verify that the package is uninstalled, type
   pkginfo –l MSFTscx

To uninstall the agent from HP-UX

1. Log on as the root user, and uninstall the agent by typing
   swremove scx
2. To verify that the package is uninstalled, type
   swlist scx

To uninstall the agent from IBM AIX

1. Log on as the root user, and uninstall the agent by typing
   installp –u scx
2. To verify that the package is uninstalled, type
   lslpp –L scx.rte

See Also

Operations Manager Agent Installation Methods

Install Agent on Windows Using the Discovery Wizard

Install Agent on UNIX and Linux Using the Discovery Wizard

Install Agent Using the MOMAgent.msi Setup Wizard

Install Agent and Certificate on UNIX and Linux Computers Using the Command Line

Managing Certificates for UNIX and Linux Computers

Process Manual Agent Installations

Applying Overrides to Object Discoveries

Configuring Agents

Examples of Using MOMAgent Command to Manage Agents

Upgrading and Uninstalling Agents on UNIX and Linux Computers

Install Agent Using the Command Line

Uninstall Agent from Windows-based Computers

Uninstall Agent from Windows-based Computers

Use one of the following procedures to uninstall an System Center 2012 – Operations Manager agent from an agent-managed computer.

To uninstall the agent by using the Operations console

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. In the **Administration** workspace, click **Agent Managed**.
4. In the **Agent Managed** pane, right-click the computers for which you want to uninstall the agent, and then select **Uninstall**.
5. In the **Uninstall Agents** dialog box, either leave **Use selected Management Server Action Account** selected or do the following:
   a. Select **Other user account**.
   b. Type the **User name** and **Password**, and type or select the **Domain** from the list. Select **This is a local computer account, not a domain account** if the account is a local computer account.

      Important
      The account must have administrative rights on the computer or the uninstall will fail.

   c. Click **Uninstall**.
6. In the **Agent Management Task Status** dialog box, the **Status** for each selected computer changes from **Queued** to **Success**.

   Note
   If the task fails for a computer, click the computer and read the reason for the failure in the **Task Output** text box.
7. Click **Close**.

To uninstall the agent by using the MOMAgent.msi agent setup wizard

1. Log on to a managed computer with an account that is a member of the administrators security group for the computer.
2. In **Control Panel**, click **Uninstall a program**.
3. In **Programs and Features**, click **System Center Operations Manager 2012 Agent**, click **Remove**, and then click **Yes**.

   Note
   The **Agent Setup Wizard** can also be run by double-clicking **MOMAgent.msi**, which is available on the Operations Manager installation media.

To uninstall the agent by using MOMAgent.msi from the command line

1. Log on to the managed computer with an account that is a member of the administrators security group for the computer.
2. Open the command window.
3. At the prompt, for example, type the following:

   %WinDir%\System32\msiexec.exe /x <path>\MOMAgent.msi /qb

To uninstall the agent from a cluster

1. Using either the Operations console method or the command line method, uninstall the agent from each node of the cluster.
2. In the Operations console, click **Administration**.
3. In the **Administration** workspace, click **Agentless Managed**.
4. In the **Agentless Managed** pane, locate all virtual instances for the cluster, right-click, and then select **Delete**.

See Also

Operations Manager Agent Installation Methods

Install Agent on Windows Using the Discovery Wizard

Install Agent on UNIX and Linux Using the Discovery Wizard

Install Agent Using the MOMAgent.msi Setup Wizard

Install Agent and Certificate on UNIX and Linux Computers Using the Command Line

Managing Certificates for UNIX and Linux Computers

Process Manual Agent Installations

Applying Overrides to Object Discoveries

Configuring Agents

Examples of Using MOMAgent Command to Manage Agents

Upgrading and Uninstalling Agents on UNIX and Linux Computers

Manually Uninstalling Agents from UNIX and Linux Computers

Install Agent Using the Command Line

Using Management Packs

Management packs contain settings that enable agents to monitor a specific service or application in System Center 2012 – Operations Manager. These settings include discovery information that allows management servers to automatically detect and begin monitoring objects, a knowledge base that contains error and troubleshooting information, rules and monitors that generate alerts, and reports.

Management packs might also contain tasks, diagnostics, and recovery tools and guidance to help fix problems.

New and updated management packs are continually being released. The recommendations in the Management Pack Life Cycle topic will help you manage the changes in your monitoring environment.

Using Management Packs topics

- What Is in an Operations Manager Management Pack?

  Provides an overview of management pack structure and components.
- Management Packs Installed with Operations Manager

  Lists the management packs that are installed with the product.
- Management Pack Life Cycle

  Provides a recommended process for administering management packs in your business environment.
- How to Import an Operations Manager Management Pack

  Provides procedures for downloading and importing management packs.
- How to Remove an Operations Manager Management Pack

  Describes how to remove or delete a management pack from a management group.
- Creating a Management Pack for Overrides

  Explains how to organize and store the overrides you configure.
- How to Export an Operations Manager Management Pack

  Describes how to export a management pack so that it can be imported to another management group.
- How to Add Knowledge to a Management Pack

  Describes how to add company knowledge to rules and monitors.

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Managing Discovery and Agents
- Tuning Monitoring by Using Targeting and Overrides

What Is in an Operations Manager Management Pack?

Management packs typically contain monitoring settings for applications and services. After a management pack is imported into a management group, System Center 2012 – Operations Manager immediately begins monitoring objects based on default configurations and thresholds that are set by the management pack.

Each management pack can contain any or all of the following parts:

- Monitors, which direct an agent to track the state of various parts of a managed component.
- Rules, which direct an agent to collect performance and discovery data, send alerts and events, and more.
- Tasks, which define activities that can be executed by either the agent or the console.
- Knowledge, which provides textual advice to help operators diagnose and fix problems.
- Views, which offer customized user interfaces for monitoring and managing this component.
- Reports, which define specialized ways to report on information about this managed component.
- Object discoveries, which identify objects to be monitored.
- Run As profiles, which allow you to run different rules, tasks, monitors, or discoveries under different accounts on different computers.

Parts of a Management Pack

Every management pack defines a model of the component that it manages. This model is expressed as one or more classes, each representing something that can be monitored and managed. When a management pack's information is sent to an agent, the agent relies on specific discovery rules in the management pack to find the actual instances of the classes this pack defines.

To reduce network utilization and storage requirements on the agent, only the parts of the management pack that are required by the agent to perform monitoring are downloaded to the agent for local storage. For example, the sections of the management packs which define rules and monitors are downloaded, while the sections for knowledge and reports are not.

Monitors

Each management pack defines one or more classes that can be managed, and then specifies a group of monitors for instances of the classes. These monitors keep track of the state of each class instance, making it easier to avoid problems before they occur.

Each monitor reflects the state of some aspect of a class instance, and changes as the state of the class instance changes. For example, a monitor that tracks disk utilization might be in one of three states: green, if the disk is less than 75 percent full; yellow, if it is between 75 and 90 percent full; and red, if the disk is more than 90 percent full. A monitor that tracks the availability of an application might have only two states: green, if the application is running; and red, if it is not. The author of each management pack defines the monitors it contains, how many states each monitor has, and what aspect of the managed class this monitor tracks.

Rules

In Operations Manager, a rule defines the events and performance data to collect from computers, and what to do with the information after it is collected. A simple way to think about rules is as an if/then statement. For example, a management pack for an application might contain rules such as the following:

- If a message indicating that the application is shutting down appears in the event log, send an alert.
- If a logon attempt fails, collect the event that indicates this failure.

As these examples show, rules can send alerts, events, or performance data. Rules can also run scripts, such as allowing a rule to attempt to restart a failed application.

Views

The Operations Manager Operations console provides standard views such as State, Alerts, and Performance. A management pack might include specialized views, unique to that management pack. In addition, you can create a personalized view in the Operations console.

Knowledge

Knowledge is content, embedded in rules and monitors, that contains information from the management pack author about the causes of an alert and suggestions on how to fix the issue that caused an alert to be raised. Knowledge appears as text in the console, and its goal is to help an operator diagnose and fix problems. The text can include links to tasks, allowing the author of this knowledge to walk an operator through the recovery process. For example, the operator might first be instructed to run task A, and then based on the result of this task, run either task B or task C. Knowledge can also contain links to performance views and to reports, giving the operator direct access to information needed to solve a problem.

Knowledge is referred to as *product knowledge* or *company knowledge*. Product knowledge is added to the management pack by the management pack author. Administrators can add their own knowledge to rules and monitors to expand the troubleshooting information and provide company-specific information for operators, which is known as company knowledge. For more information on adding company knowledge to a management pack, see How to Add Knowledge to a Management Pack.

Tasks

A task is a script or other executable code that runs either on the management server or on the server, client, or other device that is being managed. Tasks can potentially perform any kind of activity, including restarting a failed application and deleting files. Like other aspects of a management pack, each task is associated with a particular managed class. For example, running chkdsk makes sense only on a disk drive while a task that restarts Microsoft Exchange Server is meaningful only on a computer that is running Exchange Server. If necessary, an operator can also run the same task simultaneously on multiple managed systems. Monitors can have two special kinds of tasks associated with them: diagnostic tasks that try to discover the cause of a problem, and recovery tasks that try to fix the problem. These tasks can be run automatically when the monitor enters an error state, providing an automated way to solve problems. They can also be run manually, because automated recovery isn't always the preferred approach.

Reports

Just as a management pack can contain views customized for the objects that management pack targets, it can also contain custom reports. For example, a management pack might include a customized definition of one of Operations Manager's built-in reports, specifying the exact objects that the report should target.

Object Discoveries

Object discoveries are used to find the specific objects on a network that need to be monitored. Management packs define the type of objects that the management pack monitors. The object discoveries can use the registry, WMI, scripts, OLE DB, LDAP, or even custom managed code to find objects on a network. If an object discovery finds objects on your network that you do not want to monitor, you can limit the scope of object discoveries by using overrides.

Run As Profiles

A management pack can include one or more Run As profiles. Run As profiles and Run As accounts are used to select users with the privileges needed for running rules, tasks, and monitors.

Management pack authors can create a Run As profile and associate the profile with one or more rules, monitors, tasks, or discoveries. The named Run As profile is imported along with the management pack into Operations Manager . The Operations Manager administrator then creates a named Run As account and specifies users and groups. The administrator adds the Run As account to the Run As profile and specifies the target computers that the account should run on. The Run As account provides the credentials for running the rules, monitors, tasks, and discoveries that are associated with the Run As profile to which the Run As account belongs.

Sealed and Unsealed Management Packs

Management packs are either sealed or unsealed. A sealed management pack is a binary file that cannot be edited. An unsealed management pack is an XML file that can be edited. Sealed management packs should have an .mp extension, while unsealed management packs should have an .xml extension.

In general, management packs obtained from an application or hardware device vendor are sealed.

Although you cannot change the settings in a sealed management pack, you can still customize the applied settings of a management pack after it is imported by using overrides or by creating additional settings such as rules, monitors, and tasks that supersede the management pack's default settings. All customizations that you create are saved to a separate management pack file.

Management Pack Libraries and Dependencies

Certain management packs are referred to as *libraries*, because they provide a foundation of classes on which other management packs depend. A management pack that you download from the Operations Manager Catalog might include a library management pack. Several library management packs are imported as part of the Operations Manager installation process. For a

list of management packs imported during the installation of Operations Manager, see Management Packs Installed with Operations Manager.

A dependency exists when a management pack references other management packs. You must import all referenced management packs before you can import the management pack that depends on those management packs. Management packs include a management pack guide that should document the dependencies of the management pack. In addition, if you attempt to import a management pack and the management packs that it is dependent on are not present, the **Import Management Packs** dialog box will display a message that the management pack will fail to import and a list of the missing management packs. After you import a management pack, you can view its dependencies in the Operations console.

To view the dependencies for a management pack

1. In the Operations console, in the **Administration** workspace, click **Management Packs**.
2. Right-click the desired management pack, and then click **Properties**.
3. In the **Properties** dialog box for the management pack, click the **Dependencies** tab.

   The **Dependencies** tab lists any management packs that the selected management pack depends on and any management packs that depend on the selected management pack.

See Also

Creating a Management Pack for Overrides

Management Packs Installed with Operations Manager

Management Pack Life Cycle

How to Import an Operations Manager Management Pack

How to Remove an Operations Manager Management Pack

How to Export an Operations Manager Management Pack

How to Add Knowledge to a Management Pack

Management Packs Installed with Operations Manager

When you install Operations Manager, a component of System Center 2012, a number of management packs are installed as well. The following table describes the purposes of those management packs.

Purpose	Associated management packs
Core monitoring functionality	• System Center Core Library • System Center Core Monitoring • System Center Core Monitoring Agent Management • System Center Internal Library • Microsoft System Center Operations Manager Library • Operations Manager Internal Library

Purpose	Associated management packs
	• Performance Library • Process Monitoring Library • Health Internal Library • Health Library • Default Management Pack • Baselining Tasks Library • System Center Operations Manager Infrastructure Monitoring • Instance Group Library • Process Monitoring Library • System Center Hardware Library • System Library • System Software Library • Windows Cluster Library • Windows Core Library • Windows Service Library • System Center Operations Manager Data Access Service Monitoring • System Center Rule Templates • System Center Task Templates • System Center UI Executed Tasks • System Center Workflow Foundation Library • System Virtualization Library • WS-Management Library
Client monitoring, agentless exception monitoring (AEM), and Customer Experience Improvement Program (CEIP)	• Client Monitoring Internal Library • Client Monitoring Library • Client Monitoring Overrides Management Pack • Client Monitoring Views Library
Application monitoring	• Distributed Application Designer Library • Microsoft System Center Application Monitoring 360 Template Library • Operations Manager APM Infrastructure • Operations Manager APM Infrastructure Monitoring • Operations Manager APM Library • Operations Manager APM Library Resources (enu)

Purpose	Associated management packs
	• Operations Manager APM Reports Library • Operations Manager APM Wcf Library • Operations Manager APM Web • Operations Manager Application Monitoring Library • Web Application Availability Monitoring Library • Web Application Availability Monitoring Solutions Base Library • Web Application Availability Monitoring Solutions Library • Web Application Monitoring Library • System Application Log Library • Synthetic Transactions Library • Microsoft.SystemCenter.DataProviders.Library
Network monitoring	• SNMP Library • Network Device Library • Network Discovery Internal • Network Management – Core Monitoring • Network Management Library • Network Management Reports • Network Management Templates
UNIX and Linux monitoring	• UNIX/Linux Core Library • UNIX/Linux Core Console Library • UNIX View Library • UNIX Log File Template Library • Image Library (UNIX/Linux)
Enabling views and consoles	• Image Library (System Center) • Image Library (System) • Image Library (UNIX/Linux) • Image Library (Windows) • Microsoft SystemCenter OperationsManager Summary Dashboard • Microsoft SystemCenter Visualization Network Dashboard • Microsoft System Center Visualization Network Library • Microsoft.SystemCenter.Visualization.Configuration.Library • Microsoft.SystemCenter.Visualization.Internal

Purpose	Associated management packs
	• Microsoft.SystemCenter.Visualization.Library • System Center Core Monitoring Views
Notifications	• Notifications Internal Library • Notifications Library
Reporting	• Data Warehouse Internal Library • Date Warehouse Library • Microsoft Data Warehouse Reports • Microsoft Generic Report Library • Microsoft ODR Report Library • Microsoft Service Level Report Library • Microsoft.SystemCenter.Reports.Deployment
Audit collection services (ACS)	• Microsoft Audit Collection Services

The following unsealed management packs are included in Operations Manager:

- Client Monitoring Overrides Management Pack
- Default Management Pack
- Microsoft SystemCenter Virtualization Network Management Pack
- Network Discovery Internal Management Pack

Do not save any settings, views, or overrides to these management packs. You should create your own local pack, which is an unsealed management pack in which to store your customizations. As a best practice, you should create a separate local pack for each sealed management pack you customize.

See Also

Creating a Management Pack for Overrides

What Is in an Operations Manager Management Pack?

Management Pack Life Cycle

How to Import an Operations Manager Management Pack

How to Remove an Operations Manager Management Pack

How to Export an Operations Manager Management Pack

How to Add Knowledge to a Management Pack

Management Pack Life Cycle

System Center 2012 – Operations Manager uses management packs to extend monitoring functionality. Ideally, a management pack tells you everything you want to know about the application or technology that you are monitoring and nothing that you do not want to know. Management packs are designed to provide a useful monitoring experience for most

environments, however you will want to test, tune, and tailor each management pack to provide optimal results for your organization's needs.

The management pack life cycle, described in the following table, is the recommended approach to using management packs. The sections following the table provide details for each stage.

Stage	Description
Review and evaluate management packs in a pre-production environment	Before you deploy a management pack in your production environment, you should familiarize yourself with the contents of the management pack and guide, and import the management pack in a pre-production or test environment. You can also view the management pack in a virtual machine environment.
Tune the management pack settings and save in a customized management pack	Use overrides to tune the settings of a management pack—such as monitors, rules, object discoveries, and attributes—to better meet your organization's needs. You should save overrides to a management pack that you create.
Deploy management packs into a production environment	Export the management pack with overrides that is associated with the management pack that you are going to deploy, and import management packs in your production environment.
Maintain management pack	After deployment, a management pack might need additional tuning, such as in following circumstances: • Environmental changes, such as new hardware or new operating system • Adding a new application to the production environment • Upgrading a version of an application • When a new or updated version of the management pack is available • Policy changes, which result in more or less monitoring based on business needs

Review and Evaluate

Each management pack should be accompanied by a management pack guide that is installed to the same folder as the management pack. A management pack guide contains instructions for

installing and configuring the management pack, and information about the management pack, such as objects that the management pack discovers and how health rolls up. You can use this information to help you customize the management pack for your purposes. You should always review the management pack guide before you import the management pack.

A tool for reviewing the contents of a sealed management pack is the MPViewer, which can display the following contents of a management pack: rules, monitors, views, tasks, console tasks, and reports. MPViewer will also display the knowledge associated with the particular management pack item. You can install and use MPViewer on any computer on which the Operations Manager Operations console is installed. Search the MSDN Blogs at http://blogs.msdn.com/b/dmuscett/archive/2012/02/19/boris-s-tools-updated.aspx for the most recent version of MPViewer.

Note

Microsoft neither endorses nor provides support for this third-party product. Please contact the specific provider for support issues.

When you have a new management pack, you should import it to a *pre-production* environment. In Operations Manager, it is a best practice to have a production implementation that is used for monitoring your production applications and a pre-production implementation that has minimal interaction with the production environment. The pre-production management group is used for testing and tuning management pack functionality before the management pack is deployed in the production environment.

To accurately measure the data that a management pack gathers, you need to expose the agent to the demands of your production environment. The hardware of the management server in the pre-production environment should reflect the hardware that is in use in your production environment. Your pre-production management group should have the same management packs imported to the management server as the production management group. To test interoperability, your pre-production environment should also include the same types of server roles that are in your production environment, just on a smaller scale.

You can assign an Operations Manager agent to more than one management group, which is called *multihoming*. If you multihome a representative subset of agents in your production environment and your pre-production environment, the pre-production environment should give you much of the information you need to correctly tune the management pack. For more information on multihoming agents, see Configuring Agents.

Tune and Customize

You can use overrides to refine the settings of a monitoring object in Operations Manager, including monitors, rules, object discoveries, and attributes. You should create a management pack in which to save customizations that you make.

For more information about using overrides, see Tuning Monitoring by Using Targeting and Overrides. For more information about creating management packs in which to save customizations, see Best Practices for Change Control.

Deploy

When you are satisfied with the performance and results of the management pack in the pre-production environment, you can deploy the management pack and its customizations in the production environment. The management pack in which you saved the customizations must be exported so that you can import it to other computers. For more information, see How to Export an Operations Manager Management Pack. The management pack that contains the overrides that you set is dependent on the original management pack and can be imported only to management groups that have the original management pack installed.

Maintain

After a management pack has been deployed, you should periodically evaluate its performance and results in the production environment to ensure that it continues to meet business needs. The following list describes common events that might require changes to a management pack:

- **Environmental changes, such as new hardware or a new operating system**

  When you are testing new hardware or a new operating system that you plan to add to your production environment, you should include existing management packs in your test plan to identify any additional tuning that might be necessary. For a new operating system, you might need to import new management packs specific to that operating system.

- **Adding a new application to the production environment**

  A new application might require a new management pack or adjustments to existing management packs.

- **Upgrading a version of an application**

  When organizations upgrade application versions, they usually either upgrade in stages, during which both versions of the application will exist in the network, or upgrade all installations of the application at one time. After testing the management packs with the new version and making any necessary adjustments, you should use the same approach for deploying the management packs that you use for deploying the upgrades. If both versions of the application will be in use at one time, you should install management packs appropriate for each version. If all installations of the application will be upgraded at one time, remove the management pack for the old version of the application and install the management pack for the new version.

- **When a new or updated version of the management pack is available**

  You should use the pre-production environment to review and tune new or updated versions of a management pack.

- **Policy changes**

  Ongoing changes in your business or organization might require adjustments to management packs to accomplish more monitoring or less monitoring.

Best Practices for Change Control

The following are some best practices to follow when managing Operations Manager management packs:

- Maintain an archive of management pack versions to enable you to roll back changes when necessary. An efficient method for maintaining the archive is by using version control software, such as Microsoft Team Foundation Server or Windows SharePoint Services. Another method is to use a file share on the network with individual folders for each management pack version.
- When you set overrides for a management pack, save them to a management pack that is named *ManagementPack*_Override, where *ManagementPack* is the name of the sealed management pack to which the overrides apply. For example, overrides to the management pack Microsoft.InformationWorker.Office.XP.mp would be saved to Microsoft.InformationWorker.Office.XP_Overrides.xml. For more information, see Creating a Management Pack for Overrides.
- When a management pack is updated, update the corresponding _Overrides.xml file with the new version number. You must use an XML editor to update the version number of the _Overrides.xml file. If you make changes to an _Overrides.xml file but do not change the version attribute, you can import the file but the settings in the file will not be applied.
- Document the overrides that you make to management packs. When you set an override, add an explanation of the action you are taking and the reason for it to the description field by clicking **Edit** in the Details pane of the Override Properties dialog box. You may also want to maintain a spreadsheet or other form to document changes that you make to management packs.

See Also

Creating a Management Pack for Overrides

Management Packs Installed with Operations Manager

What Is in an Operations Manager Management Pack?

How to Import an Operations Manager Management Pack

How to Remove an Operations Manager Management Pack

How to Export an Operations Manager Management Pack

How to Add Knowledge to a Management Pack

How to Import an Operations Manager Management Pack

There are numerous management packs available for System Center 2012 – Operations Manager. You have several options for importing management packs:

- Import directly from the catalog on the Microsoft System Center Marketplace by using the Operations console.
- Import from disk (local storage or a network file share) by using the Operations console.
- Use the Operations console to download a management pack from the catalog to import at a later time.
- Use an Internet browser to download a management pack from the catalog to import at a later time.

Note

Using the management pack catalog service requires an Internet connection. If the computer running Operations Manager cannot be connected to the Internet, use another computer to download the management pack, and then copy the files to a shared folder that is accessible to the Operations Manager management server.

The catalog on the Microsoft System Center Marketplace contains management packs from Microsoft and some non-Microsoft companies. You can obtain management packs directly from other companies and import them by using the procedure to import from disk. You can also search for management packs created by the community, such as the packs available at the System Center Central website.

Note

Microsoft neither endorses nor provides support for third-party products. Please contact the specific provider for support issues.

You should always review the management pack guide before you import a management pack.

To import a management pack from the catalog

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. Right-click **Management Packs**, and then click **Import Management Packs**.
4. The **Import Management Packs** wizard opens. Click **Add**, and then click **Add from catalog**.

   The **Select Management Packs from Catalog** dialog box opens. The default view lists all management packs in the catalog. You can change the view to show the following management packs:

   - Updates available for management packs that are already imported on this computer
   - All management packs that have been released within the last three months
   - All management packs that have been released within the last six months

   You can also use the **Find** field to search for a specific management pack in the catalog.
5. In the list of management packs, select the management pack that you want to import, click **Select**, and then click **Add**.

   In the list of management packs, you can select a product, or expand the product name to select a specific version, or expand the product version to select a specific management pack file. For example, you can select **SQL Server** for all SQL Server management packs, or you can expand **SQL Server** and select **SQL Server 2005** for all SQL Server 2005 management packs, or you can expand **SQL Server 2005** and select **SQL Server Core Library Management Pack**.

   Note

   When a management pack is labeled “(Online Catalog Only)”, you cannot import the management pack directly from the catalog. You must download the .msi and

import from disk.

6. On the **Select Management Packs** page, the management packs that you selected for import are listed. An icon next to each management pack in the list indicates the status of the selection, as follows:
   - A green check mark indicates that the management pack can be imported. When all management packs in the list display this icon, click **Import**.
   - A yellow information icon indicates that the management pack is dependent on one or more management packs that are not in the **Import** list but are available in the catalog. To add the management pack dependencies to the **Import** list, click **Resolve** in the **Status** column. In the **Dependency Warning** dialog box that appears, click **Resolve**.
   - A red error icon indicates that the management pack is dependent on one or more management packs that are not in the **Import** list and are not available in the catalog. To view the missing management packs, click **Error** in the **Status** column. To remove the management pack with the error from the **Import** list, right-click the management pack, and then click **Remove**.

   Note
   When you click **Import**, any management packs in the **Import** list that display the Information or Error icon are not imported.
7. The **Import Management Packs** page appears and shows the progress for each management pack. Each management pack is downloaded to a temporary directory, imported to Operations Manager, and then deleted from the temporary directory. If there is a problem at any stage of the import process, select the management pack in the list to view the status details. Click **Close**.

Note
When you import a management pack that contains binary files (.mpb), you must recycle the OperationsManager application pool in Internet Information Services (IIS) Manager.

To import a management pack from disk

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. Right-click **Management Packs**, and then click **Import Management Packs**.
4. The **Import Management Packs** wizard opens. Click **Add**, and then click **Add from disk**.
5. The **Select Management Packs to import** dialog box appears. If necessary, change to the directory that holds your management pack file. Click one or more management packs to import from that directory, and then click **Open**.
6. On the **Select Management Packs** page, the management packs that you selected for import are listed. An icon next to each management pack in the list indicates the status of

the selection, as follows:

- A green check mark indicates that the management pack can be imported. When all management packs in the list display this icon, click **Import**.
- A red error icon indicates that the management pack is dependent on one or more management packs that are not in the **Import** list and are not available in the catalog. To view the missing management packs, click **Error** in the **Status** column. To remove the management pack with the error from the **Import** list, right-click the management pack, and then click **Remove**.

Note

When you click **Import**, any management packs in the **Import** list that display the Error icon are not imported.

7. The **Import Management Packs** page appears and shows the progress for each management pack. Each management pack is downloaded to a temporary directory, imported to Operations Manager, and then deleted from the temporary directory. If there is a problem at any stage of the import process, select the management pack in the list to view the status details. Click **Close**.

Note

When you import a management pack that contains binary files (.mpb), you must recycle the OperationsManager application pool in Internet Information Services (IIS) Manager.

To download a management pack by using the Operations console

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. Right-click **Management Packs**, and then click **Download Management Packs**.
4. The **Download Management Packs** wizard opens. Click **Add**.

   The **Select Management Packs from Catalog** dialog box opens. The default view lists all management packs in the catalog. You can change the view to show the following management packs:

   - Updates available for management packs that are already imported on this computer
   - All management packs that have been released within the last three months
   - All management packs that have been released within the last six months

   You can also use the **Find** field to search for a specific management pack in the catalog.
5. In the list of management packs, select the management pack that you want to import, click **Select**, and then click **Add**.

   In the list of management packs, you can select a product, or expand the product name to select a specific version, or expand the product version to select a specific management pack file. For example, you can select **SQL Server** for all SQL Server management packs, or you can expand **SQL Server** and select **SQL Server 2005** for all

SQL Server 2005 management packs, or you can expand **SQL Server 2005** and select **SQL Server Core Library Management Pack**.

6. The selected management packs are displayed in the **Download** list. In the **Download management packs to this folder** field, enter the path where the management packs should be saved, and then click **Download**.
7. The **Download Management Packs** page appears and shows the progress for each management pack. If there is a problem with a download, select the management pack in the list to view the status details. Click **Close**.

To download a management pack by using an Internet browser

1. Open a browser and go to the catalog on the Microsoft System Center Marketplace (http://go.microsoft.com/fwlink/?LinkId=82105).
2. Browse the list of management packs, or use the **Search Applications** field to locate the management pack that you want to download.
3. Click the name of the management pack that you want to download.
4. On the details page for the management pack, click **Download**.
5. On the management pack download page, click **Download**.

   Note
   Some management pack download pages contain a download link for the management pack .msi file and a download link for the management pack guide. Download both the .msi and the guide.
6. In the **File Download** dialog box, click **Run** to download and extract the management pack files. Or, click **Save** to download the .msi file without extracting the files.

   Note
   Before you can import the management pack in Operations Manager, you must run the .msi file to extract the files.

See Also

Creating a Management Pack for Overrides

Management Packs Installed with Operations Manager

What Is in an Operations Manager Management Pack?

Management Pack Life Cycle

How to Remove an Operations Manager Management Pack

How to Export an Operations Manager Management Pack

How to Add Knowledge to a Management Pack

How to Remove an Operations Manager Management Pack

When you no longer need a management pack, you can delete it using the Operations console. When you delete a management pack, all the settings and thresholds associated with it are

removed from System Center 2012 – Operations Manager. Also, the .mp or .xml file for that management pack is deleted from the hard disk of the management server. You can delete a management pack only if you have first deleted dependent management packs.

To remove a management pack

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. In **Administration**, click **Management Packs.**
4. In the **Management Packs** pane, right-click the management pack you would like to remove and then click **Delete**.
5. On the message stating that deleting the management pack might affect the scoping of some user roles, click **Yes**.

Note
If any other imported management packs depend on the management pack you are trying to remove, the **Dependent Management Packs** error message displays. You must remove the dependent management packs before you can continue.

Operations Manager removes the selected management pack.

See Also

Creating a Management Pack for Overrides

Management Packs Installed with Operations Manager

What Is in an Operations Manager Management Pack?

Management Pack Life Cycle

How to Import an Operations Manager Management Pack

How to Export an Operations Manager Management Pack

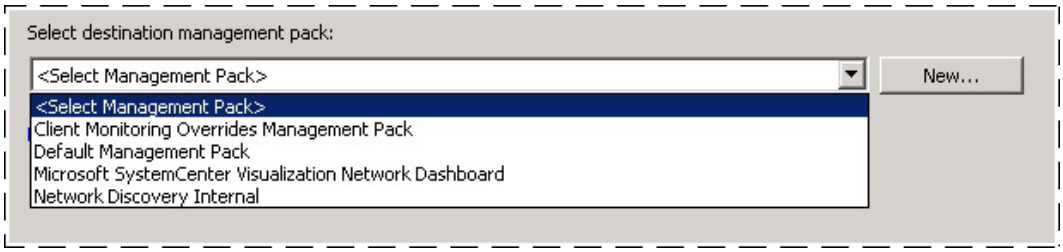
How to Add Knowledge to a Management Pack

Creating a Management Pack for Overrides

In System Center 2012 – Operations Manager, in a number of wizards and dialog boxes, you select a destination management pack in which to store the results. You can select any unsealed management pack file in your management group or create a new one.

Management packs can be sealed or unsealed. A sealed management pack cannot be modified directly. Any changes to the workflows in the sealed management pack, such as an override for a monitor, must be saved to an unsealed management pack. The unsealed management pack references the sealed management pack that it modifies.

The following illustration shows the unsealed management packs that are installed with Operations Manager.



Never use the management packs that are installed with Operations Manager to save any settings that you change or elements that you create. When you have to select a destination management pack, always select a management pack that you create.

You select a destination management pack when you create an override or disable a rule, monitor, or object discovery. You also select a destination management pack when you create or configure the following elements:

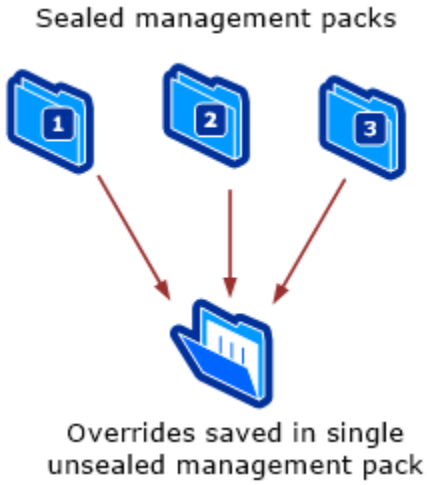
- A folder in the **Monitoring** workspace
- A unit, aggregate, or dependency monitor
- An attribute
- A group
- A rule
- A task
- A Run As profile
- Monitoring by using a management pack template
- Monitoring of a distributed application
- Tracking of service level objectives

Saving Overrides

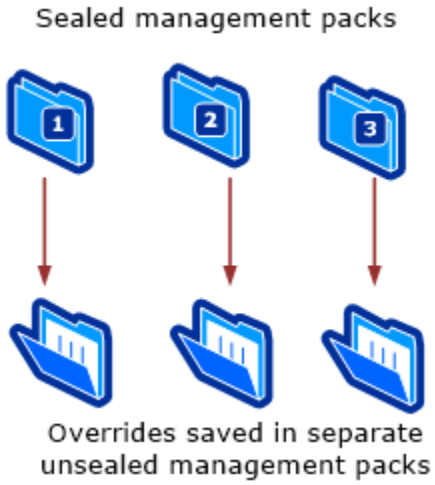
As a best practice, save all overrides for each sealed management pack to an unsealed management pack that is named ManagementPack_Override, where ManagementPack is the name of the sealed management pack to which the overrides apply. For example, overrides to the management pack Microsoft.InformationWorker.Office.XP.mp would be saved to Microsoft.InformationWorker.Office.XP_Overrides.xml.

When you want to remove a sealed management pack, you must first remove any other management packs that reference it. If the unsealed management packs that reference the sealed management pack also contain overrides or elements that apply to a different sealed management pack, you lose those overrides and elements when you remove the unsealed management pack.

In the following image, overrides for management packs 1, 2, and 3 are all saved to a single unsealed management pack. If you want to remove management pack 1, you first must remove the unsealed management pack. As you can see, you would also remove all overrides for management packs 2 and 3.



The recommended method is to create an unsealed management pack for each sealed management pack that you want to override, as shown in the following image. Removing management pack 1 and its unsealed management pack does not affect the other management packs.



How to Create a Management Pack for Overrides

You can create a management pack for overrides before you configure an override or as part of the override procedure.

To create a management pack

- In the **Administration** workspace, in the navigation pane, right-click, and then click **Create Management Pack**.

  -or-

- In the **Override Properties** dialog box for a rule or monitor, in the **Select destination management pack** section, click **New**.

See Also

How to Remove an Operations Manager Management Pack

Management Packs Installed with Operations Manager

What Is in an Operations Manager Management Pack?

Management Pack Life Cycle

How to Import an Operations Manager Management Pack

How to Export an Operations Manager Management Pack

How to Add Knowledge to a Management Pack

How to Export an Operations Manager Management Pack

Exporting a management pack allows customizations to a sealed management pack to be saved to a file. Because sealed management packs cannot be changed, the customizations made to a management pack are saved to a separate, unsealed management pack file. The unsealed management pack can then be imported to a different management group. This unsealed management pack is dependent on the original sealed management pack and can be imported only to management groups that have the original sealed management pack.

Note

Using the Operations Console, you can only export unsealed management packs. To export a sealed management pack, you must use the Export-SCOMManagementPack cmdlet. See Operations Manager Cmdlet Reference for more information.

To export management pack customizations

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. In **Administration**, click **Management Packs** to display the list of imported management packs.
4. In the **Management Packs** pane, right-click the management pack you want to export, and then click **Export Management Pack**.
5. In the **Browse For Folder** dialog box, expand the path for the location to save the file, and then click **OK**.

   The management pack is saved as an Operations Manager XML management pack file and is ready for importing into another management group.

See Also

Creating a Management Pack for Overrides

Management Packs Installed with Operations Manager

What Is in an Operations Manager Management Pack?

Management Pack Life Cycle

How to Import an Operations Manager Management Pack

How to Remove an Operations Manager Management Pack

How to Add Knowledge to a Management Pack

How to Add Knowledge to a Management Pack

System Center 2012 – Operations Manager management packs include knowledge for rules, monitors, and alerts that helps you identify problems, causes, and resolutions.

Knowledge is referred to as *product knowledge* or *company knowledge*. Product knowledge is embedded in a rule or monitor when it is authored. Company knowledge is added by management group administrators to expand the troubleshooting information and provide company-specific information for operators. Administrators can use company knowledge to document any overrides implemented for a monitor or rule, along with the explanation for the customization and any other information that might be useful.

Operations Manager stores company knowledge in a management pack. Sealed management packs cannot be modified, so Operations Manager saves customizations such as company knowledge in a custom management pack. By default, Operations Manager saves all customizations to the Default Management Pack. As a best practice, you should instead create a separate management pack for each sealed management pack you want to customize.

Tip

To avoid losing your company knowledge, be sure to back up management packs as part of your general backup routine.

To add or edit company knowledge, the computer must meet the following software requirements:

- The Operations console must be installed on a 32-bit computer. Adding and editing company knowledge must be done on this computer.
- Microsoft Office Word 2003 with the .NET Programmability feature, or Microsoft Office Word 2007 or Office Word 2010 Professional edition (Standard edition is not supported)

  Note

  Only the 32-bit version of Word 2010 is supported. The knowledge template will not work with the 64-bit version of Word 2010.
- Microsoft Visual Studio 2005 Tools for Office Second Edition Runtime at http://go.microsoft.com/fwlink/?LinkId=74969. You must use this version of the Visual Studio 2005 Tools for Office.

To add or edit company knowledge, you must have the Author or Administrator user role.

To edit company knowledge

1. Log on to the computer with an account that is a member of the Operations Manager Author or Administrator role.

2. Click **Authoring**.
3. Locate the monitor or rule to be documented.
4. Click **Properties** under **Actions**, or right-click the monitor name and select **Properties** from the shortcut menu.
5. Click the **Company Knowledge** tab.
6. In the **Management pack** section, select a management pack in which to save the company knowledge.
7. Click **Edit** to launch Microsoft Office Word.
8. Add or edit text as desired.

   The company knowledge tab displays only the sections of the Word document with custom text.
9. On the **File** menu, click **Save** to save your changes.

   Important
   Do not close Word.
10. Return to the company knowledge tab and click **Save**, and then click **Close**. This will close both the properties dialog box and Word.

See Also

Creating a Management Pack for Overrides

Management Packs Installed with Operations Manager

What Is in an Operations Manager Management Pack?

Management Pack Life Cycle

How to Import an Operations Manager Management Pack

How to Remove an Operations Manager Management Pack

How to Export an Operations Manager Management Pack

Tuning Monitoring by Using Targeting and Overrides

When you import a management pack, System Center 2012 – Operations Manager discovers the objects defined by the management pack and begins applying the management pack's rules and monitors to the discovered objects. You should always import a new management pack in a pre-production environment first so that you can evaluate the management pack and adjust or tune the management pack as necessary to meet your business needs.

To tune a management pack effectively, you should involve the service owner or subject matter experts, the operations team members who monitor the alerts and events and take action when something requires attention, and the engineering team responsible for the Operations Manager infrastructure. Depending on the service that is monitored by the management pack, you might also include the networking or security teams. Those responsible for the Operations Manager infrastructure might not have the knowledge and experience with the service to effectively tune the management pack without expert input.

Tuning Approach

For servers or applications, tune from the highest severity alerts and dependencies to the lowest. Look at alerts first, then open the Health Explorer to gather more detailed information for the problem. Validate results of the alerts generated, verify scope of monitoring against intended targets (servers or services), and ensure the health model is accurate.

Each rule should be evaluated according to the following criteria:

- **Actionability**: An alert is actionable if it tells you what went wrong and how to fix it. When alerts are generated that do not require any action, consider disabling alerting for the rule.
- **Validity**: An alert is valid if the issue that generated the alert can be confirmed and the issue actually occurred at the moment the alert was generated.
- **Suppression**: There should be only one alert stating the issue occurred.

What to Tune

- Discovery frequency
- Monitor thresholds
- Targets
- Intervals
- Parameters

Tips

- Import a single management pack at a time.
- Review any new alerts reported for servers monitored with the new management pack. You can use the Alerts and Most Common Alerts reports to help you discover your most common alerts. When you first install a management pack, it tends to discover a multitude of previously unknown issues. Monitor the alerts to determine potential areas of concern
- Override the monitor or rule as applicable for a particular object type, a group, or a specific object.
- Disable the monitor or rule if the issue is not severe enough to warrant an alert and you do not need to be made aware of the specific situation being monitored.
- Change the threshold of the monitor that is generating the alert if you want the underlying condition to be monitored, but the alert is being generated before the condition is actually a problem for your particular environment.
- When you set overrides for a management pack, save them to a management pack that is named ManagementPack_Override, where ManagementPack is the name of the sealed management pack to which the overrides apply. For example, overrides to the management pack Microsoft.InformationWorker.Office.XP.mp would be saved to Microsoft.InformationWorker.Office.XP_Overrides.xml..

Tuning Monitoring by Using Targeting and Overrides topics

- Using Classes and Groups for Overrides in Operations Manager
- How to Override a Rule or Monitor
- How to Enable or Disable a Rule or Monitor
- Using the Enforced Attribute in Overrides
- How to Enable Recovery and Diagnostic Tasks

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Managing Discovery and Agents
- Using Management Packs

Using Classes and Groups for Overrides in Operations Manager

This topic describes the differences between classes and groups in System Center 2012 – Operations Manager, and how workflows, such as rules and monitors, apply to each. The following sections define classes and groups, and provide examples for applying overrides with the available override options.

Classes

In Operations Manager, a *class* is a definition of an item that can be discovered and managed. A class can represent a computer, a database, a service, a disk, an application, or any other kind of object that requires monitoring. Monitors, rules, discoveries, overrides, and tasks can apply to a class. For example, **Windows Server 2003 Logical Disk** is a class that defines logical disks on a computer that is running the Windows Server 2003 operating system. A monitor that applies to the **Windows Server 2003 Logical Disk** class will be applied only to objects that meet that class definition.

Note

In the Operations console, the term *target* is used instead of *class*.

Classes are defined in the Operations Manager management pack libraries and in individual product management packs that you import.

Groups

In Operations Manager, a *group* is a logical set of objects that can be used to define the scope of overrides, views, user roles, and notifications. Some groups are provided in the Operations Manager installation, such as **All Windows Computers** group and **Agent Managed Computer Group**. You can create your own groups and add members to groups explicitly or dynamically.

Overrides

You have seen that classes are used to target workflows such as rules and monitors. A monitor or rule is applied to a specific class. To change the value for a parameter of a rule or monitor, you create an override. You have the following options for applying your override:

- **For all objects of class:** *Class*

  When you select this option for your override, the override settings apply to all objects in the class at which the rule or monitor is targeted.

- **For a group**

  When you select this option for your override, the override settings apply only to members of the group. The rule or monitor without the override settings continues to apply to all objects in the targeted class except for those objects that are also members of the group used for the override.

  When you create a group, you save it to an unsealed management pack. However, an element in an unsealed management pack, such as an override, cannot reference an element in a different unsealed management pack, such as a group. If you are going to use a group to limit the application of an override, you must either save the group to the same unsealed management pack as the override, or you must seal the management pack that contains the group.

- **For a specific object of class:** *Class*

  When you select this option for your override, the override settings apply only to the specified object. The rule or monitor without the override settings continues to apply to all other objects in the targeted class.

- **For all objects of another class**

  When you select this option for your override, the override settings apply only to objects of a class other than the targeted class. The rule or monitor without the override settings continues to apply to all objects in the targeted class.

Overrides that apply to a class are applied first, then overrides that apply to a group, and finally overrides that apply to a specific object. For more information, see Using the Enforced Attribute in Overrides.

How to Apply Overrides

Here are some examples of when you would use the override options.

You want to change the priority of an alert

Select to override **For all objects of class:** *Class*.

You want to change the priority of an alert for computers that meet a specific criteria

Select to override **For a group** and create a group that dynamically adds members based on specific criteria.

You want to change the priority of an alert for a specific computer only

Select to override **For a specific object of class:** *Class*. You could also select **For a group** and create a group that has the specific computer added as an explicit member.

You want to change the priority of an alert that applies to all operating systems for a specific operating system

Select **For all objects of another class** and select the class that represents the operating system for which you want to have a different alert priority.

You want the rule or monitor to apply only to specific computers

In this common scenario, you must perform the following two tasks:

1. Select to override **For all objects of class:** *Class*, and change **Enabled** to **False**. This will disable the rule or monitor.

2. Select to override **For a group**, **For a specific object of class:** *Class*, or **For all objects of another class**, and change **Enabled** to **True**. This enables the rule or monitor for members of that group, the specified object, or the selected class only.

See Also

How to Override a Rule or Monitor

How to Enable or Disable a Rule or Monitor

Using the Enforced Attribute in Overrides

How to Enable Recovery and Diagnostic Tasks

How to Override a Rule or Monitor

Overrides change the configuration of System Center 2012 – Operations Manager monitoring settings for monitors, attributes, object discoveries, and rules. When you create an override, you can apply it to a single managed object or to a group of managed objects. You must have Advanced Operator user rights to create and edit overrides.

The use of overrides is key to controlling the amount of data that is collected by Operations Manager. When you create a monitor, rule, or attribute you target it at an object type, but often the available object types are broad in scope. You can then use groups and overrides together to narrow the focus of the monitor, rule, attribute, or object discovery. You can also override existing monitors, rules, attributes, or object discoveries that are from management packs.

Overrides that apply to a class are applied first, then overrides that apply to a group, and finally overrides that apply to a specific object. For more information, see Using Classes and Groups for Overrides in Operations Manager and Using the Enforced Attribute in Overrides.

The following procedure overrides a monitor, but you can also use these steps to override a rule, attribute, or object discovery. You must have Advanced Operator or Administrator user rights to create an override.

To override a monitor

1. Log on to the computer with an account that is a member of the Operations Manager Advanced Operator role.
2. In the Operations console, click **Authoring**.

3. In the **Authoring** workspace, expand **Management Pack Objects** and then click **Monitors**.
4. In the **Monitors** pane, expand an object type completely and then click a monitor.
5. On the Operations console toolbar, click **Overrides** and then point to **Override the Monitor**. You can choose to override this monitor for objects of a specific type or for all objects within a group. After you choose which group of object type to override, the **Override Properties** dialog box opens, enabling you to view the default settings contained in this monitor. You can then choose whether to override each individual setting contained in the monitor. For more information about applying an override, see Using Classes and Groups for Overrides in Operations Manager.

   Note
   If the **Overrides** button is not available, make sure you have selected a monitor and not a container object in the **Monitors** pane.
6. Click to place a check mark in the **Override** column next to each parameter that you want to override. The **Override Value** can now be edited. Change the value in **Override Value** to the value you want the parameter to use.
7. Either select a management pack from the **Select destination management pack** list or create a new unsealed management pack by clicking **New**. For more information about selecting a destination management pack, see Creating a Management Pack for Overrides.
8. When you complete your changes, click **OK**.

See Also

Using Classes and Groups for Overrides in Operations Manager

How to Enable or Disable a Rule or Monitor

Using the Enforced Attribute in Overrides

How to Enable Recovery and Diagnostic Tasks

How to Enable or Disable a Rule or Monitor

In System Center 2012 – Operations Manager, if a management pack's default settings contain a monitor or rule that is not necessary in your environment, you can use overrides to disable this monitor or rule. In addition, some management packs ship with some rules or monitors disabled; you should read the management pack guide to identify the workflows that are disabled by default and determine if you should enable any of them for your monitoring needs. For example, the management packs for network monitoring contain rules and monitors that are vendor-specific, as listed in Tuning Network Monitoring. Many vendor-specific rules and monitors in the network management pack are disabled to avoid performance impact. You should identify the devices used in your environment and use overrides to enable the rules and monitors specific to your devices.

To enable or disable a monitor or rule using overrides

1. Log on to the computer with an account that is a member of the Operations Manager Advanced Operator role.
2. In the Operations console, click **Authoring**.
3. In the **Authoring** workspace, click **Monitors** (or **Rules** if you want to disable a rule).
4. In the **Monitors** or **Rules** section, click the monitor or rule that you want to disable.
5. On the Operations console toolbar, click **Overrides** and then point to **Override the Monitor** (or **Rule**). You can choose to override this monitor or rule for objects of a specific type or for all objects within a group. After you choose which group of object type to override, the **Override Properties** dialog box opens, enabling you to view the default settings contained in this monitor or rule. For more information about applying an override, see Using Classes and Groups for Overrides in Operations Manager.
6. In the **Override Properties** dialog box, click to select the **Override** check box that corresponds to the **Enabled** parameter.

   Note
   If you select **Disable** instead of **Override**, the **Override Properties** dialog box opens with the **Override** check box selected and the **Enabled** value set to **False**.
7. In the **Override Setting** column, click **True** to enable the rule or monitor or **False** to disable the rule or monitor.
8. In the **Select destination management pack** list, click the appropriate management pack in which to store the override or create a new unsealed management pack by clicking **New**. For more information about selecting a destination management pack, see Creating a Management Pack for Overrides.
9. When you complete your changes, click **OK**.

See Also

Using Classes and Groups for Overrides in Operations Manager

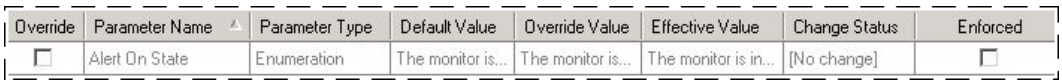
How to Override a Rule or Monitor

Using the Enforced Attribute in Overrides

How to Enable Recovery and Diagnostic Tasks

Using the Enforced Attribute in Overrides

When you configure an override to a rule, monitor, or discovery in Operations Manager for System Center 2012, you will notice an **Enforced** check box in the row for each value that you can override, as shown in the following illustration.



Override	Parameter Name	Parameter Type	Default Value	Override Value	Effective Value	Change Status	Enforced
☐	Alert On State	Enumeration	The monitor is...	The monitor is...	The monitor is in...	[No change]	☐

When the Enforced attribute is selected for an override, this setting ensures that the override will take precedence over all other overrides of the same type and context that do not have **Enforced** set.

Overrides that apply to a class are applied first, then overrides that apply to a group, and finally overrides that apply to a specific object. The Enforced attribute assures that the override will take precedence when two overrides of the same type and context conflict.

For example, you have two Windows computers, COMPUTER1 and COMPUTER2. COMPUTER1 is member of GROUP-A and is also member of GROUP-B. COMPUTER2 is not a member of any group. The default threshold for a CPU monitor is 80%.

You apply an override to the Windows Computer class that changes the CPU monitor threshold to 70%. You create another override to that monitor that applies to GROUP-A and sets the threshold to 90%. At this point, the threshold for COMPUTER1 is 90% and the threshold for COMPUTER2 is 70%.

If you create an override that applies to GROUP-B and sets the threshold to 95%, the resulting threshold for COMPUTER1, which is member of both GROUP-A and GROUP-B, is unpredictable. However, if you used the Enforced attribute on the override that applies to GROUP-B, you ensure that the 95% threshold applies to COMPUTER1.

If you create an override that applies to COMPUTER1 and sets the threshold to 60%, the resulting threshold for COMPUTER1 is 60% because the object override takes precedence over the class and group overrides.

See Also

Using Classes and Groups for Overrides in Operations Manager

How to Override a Rule or Monitor

How to Enable or Disable a Rule or Monitor

How to Enable Recovery and Diagnostic Tasks

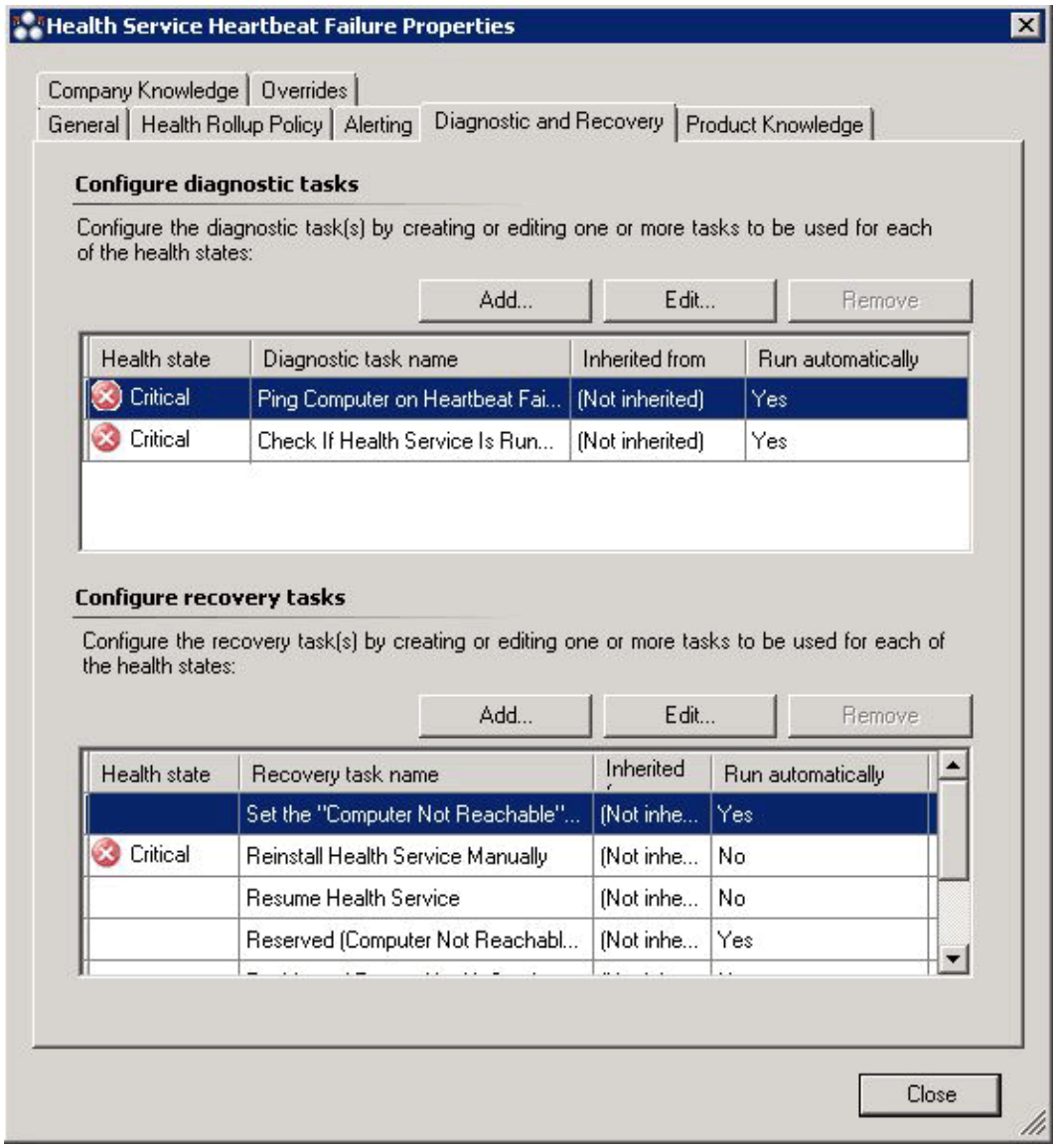
How to Enable Recovery and Diagnostic Tasks

Monitors in Operations Manager for System Center 2012 can do more than notify you of problems by sending an alert. Some monitors also provide diagnostic and recovery tasks to help investigate and resolve those problems.

A task is a script or other executable code that runs either on the computer running the Operations console or on the server, client, or device that is being managed. Tasks can potentially perform any kind of activity, including restarting a failed application and deleting files.

Monitors can have two kinds of tasks associated with them: diagnostic tasks that try to discover the cause of a problem or provide you with additional information to assist with that diagnosis, and recovery tasks that try to fix the problem.

Some monitors have diagnostic or recovery tasks that are disabled by default. You can enable any of these tasks that you want the monitor to run. For example, in the following image, you see that some recovery tasks for the **Health Service Heartbeat Failure** monitor are not configured to run automatically.



To enable a diagnostic or recovery task

1. In the Operations console, in the **Authoring** workspace, right-click a monitor and click **Properties**.
2. Click the **Diagnostic and Recovery** tab.
3. On the **Diagnostic and Recovery** tab, in the **Configure diagnostic tasks** or **Configure recovery tasks** section, ensure the desired task is selected and then click **Edit**.
4. On the **Overrides** tab, click **Override**. You can choose to override this monitor for objects of a specific type or for all objects within a group. After you choose which group or object type to override, the **Override Properties** dialog box opens. For more information about applying an override, see Using Classes and Groups for Overrides in Operations

Manager.

5. In the **Override-controlled parameters** section, click **Enabled** and set the override value to **True**.
6. Either select a management pack from the **Select destination management pack** list or create a new unsealed management pack by clicking **New**. For more information about selecting a destination management pack, see Creating a Management Pack for Overrides.
7. Click **OK**. Close the open properties windows.

See Also

Diagnostic and Recovery Tasks

Using Classes and Groups for Overrides in Operations Manager

How to Override a Rule or Monitor

How to Enable or Disable a Rule or Monitor

Using the Enforced Attribute in Overrides

Managing Access in Operations Manager

Managing Access in Operations Manager topics

- Operations Manager Accounts

  This section describes the accounts that Operations Manager uses.
- Implementing User Roles

  To enable individuals to access monitoring data and perform actions, you assign them to user roles. This section explains how to use user roles to manage access in Operations Manager.
- How to Create a New Action Account in Operations Manager

  The action account is used to gather information about, and run responses on, the managed computer. This procedure explains how to create a new action account that has access to the Operations Manager database.
- How to Manage the Report Server Unattended Execution Account in Operations Manager

  The Operations Manager Report Server unattended execution account is used to query data from the Reporting Data Warehouse and is configured through Microsoft SQL Server 2008. This procedure explains how to manage this account.
- Control Access by Using the Health Service Lockdown Tool in Operations Manager

  On computers requiring high security, such as a domain controller, you may need to deny certain identities access to rules, tasks, and monitors that might jeopardize the security of your server. The Health Service lockdown tool (HSLockdown.exe) enables you to use various command-line options to control and limit the identities used to run a rule, task, or monitor.
- Accessing UNIX and Linux Computers in Operations Manager

This section explains how to configure and manage access to computers running UNIX and Linux operating systems.

- Managing Run As Accounts and Profiles

  Operations Manager workflows, such as rules, tasks, monitors, and discoveries, require credentials to run on a targeted agent or computer. These credentials are configured by using Run As profiles and Run As accounts. This section explains how to create, configure, and manage Run As profiles and accounts.

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Initial Monitoring After Operations Manager Is Installed
- Operations Manager Monitoring Scenarios
- Getting Information from Operations Manager
- General Tasks in Operations Manager
- Maintenance of Operations Manager

Managing Access in Operations Manager

Managing Access in Operations Manager topics

- Operations Manager Accounts

  This section describes the accounts that Operations Manager uses.

- Implementing User Roles

  To enable individuals to access monitoring data and perform actions, you assign them to user roles. This section explains how to use user roles to manage access in Operations Manager.

- How to Create a New Action Account in Operations Manager

  The action account is used to gather information about, and run responses on, the managed computer. This procedure explains how to create a new action account that has access to the Operations Manager database.

- How to Manage the Report Server Unattended Execution Account in Operations Manager

  The Operations Manager Report Server unattended execution account is used to query data from the Reporting Data Warehouse and is configured through Microsoft SQL Server 2008. This procedure explains how to manage this account.

- Control Access by Using the Health Service Lockdown Tool in Operations Manager

  On computers requiring high security, such as a domain controller, you may need to deny certain identities access to rules, tasks, and monitors that might jeopardize the security of your server. The Health Service lockdown tool (HSLockdown.exe) enables you to use various command-line options to control and limit the identities used to run a rule, task, or monitor.

- Accessing UNIX and Linux Computers in Operations Manager

  This section explains how to configure and manage access to computers running UNIX and Linux operating systems.
- Managing Run As Accounts and Profiles

  Operations Manager workflows, such as rules, tasks, monitors, and discoveries, require credentials to run on a targeted agent or computer. These credentials are configured by using Run As profiles and Run As accounts. This section explains how to create, configure, and manage Run As profiles and accounts.

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Initial Monitoring After Operations Manager Is Installed
- Operations Manager Monitoring Scenarios
- Getting Information from Operations Manager
- General Tasks in Operations Manager
- Maintenance of Operations Manager

Operations Manager Accounts

To communicate with various parts of the monitoring infrastructure, the System Center 2012 – Operations Manager management group requires two accounts: the Management Server Action Account and the System Center Configuration service and System Center Data Access Service Account. You are required to specify credentials for these accounts during installation.

If you install Reporting, you need to specify credentials for two additional accounts: the Data Warehouse Write account and the Data Reader account.

When you install an agent, you will be required to provide credentials for the Computer Discovery account and the Agent action account. You are also prompted for an account that has Administrator rights on the computers you will install the agent on.

Action Account

The action account is used to gather information about, and run responses on, the managed computer (a managed computer being either a management server or a computer with an agent installed). The MonitoringHost.exe processes run under the action account or a specific Run As account. There might be more than one MonitoringHost.exe process running on the agent at any given time.

Some of the actions that MonitoringHost.exe performs include:

- Monitoring and collecting Windows event log data.

- Monitoring and collecting Windows performance counter data.
- Monitoring and collecting Windows Management Instrumentation (WMI) data.
- Running actions such as scripts or batches.

The separation of the Health Service process from the single and multiple uses of the MonitoringHost process means that if a script running on the managed computer stalls or fails, the functionality of the Operations Manager service or other responses on the managed computer will not be affected.

The action account can be managed through the Default action account located in **Run As Profiles** in the **Administration** workspace.

Using a Low-Privileged Account

When you install Operations Manager, you have the option of specifying either a domain account or using Local System. The more secure approach is to specify a domain account which allows you to select a user with the least amount of privileges necessary for your environment.

You can use a low-privileged account for the agent's action account. On computers running Windows Server 2003 and Windows Vista, the account must have the following minimum privileges:

- Member of the local Users group
- Member of the local Performance Monitor Users group
- "Allow log on locally" permission (SetInteractiveLogonRight)

Important

The minimum privileges described above are the lowest privileges that Operations Manager supports for the Action account. Other Run As accounts can have lower privileges. The actual privileges required for the Action account and the Run As accounts will depend upon which management packs are running on the computer and how they are configured. For more information about which specific privileges are required, see the appropriate management pack guide.

Keep the following points in mind when choosing an credentials for the Management Server Action Account:

- A low-privileged account can be used only on computers running Windows Server 2003 and Windows Vista. On computers running Windows 2000 and Windows XP, the action account must be a member of the local Administrators security group or Local System.
- Using a low-privileged domain account requires password updating consistent with your password expiration policies.
- You cannot enable Agentless Exception Monitoring (AEM) on a management server with a low-privileged action account.
- The Action account must be assigned the Manage Auditing and Security log privilege by using Local or Global policy, if a management pack is to read the event in the Security Event log.

Action Accounts and the Operations Manager Database

You assigned credentials to the action account when you installed. By default, the action account has access to the Operations Manager database. To increase security, you can remove access to the Operations Manager database from the action account and create a new separate Run As Account for accessing the Operations Manager database.

System Center Configuration Service and System Center Data Access Service Account

The System Center Configuration service and System Center Data Access service account is used by the System Center Data Access and System Center Management Configuration services to update information in the Operations Manager database. The credentials used for the action account will be assigned to the sdk_user role in the Operations Manager database.

The account used for the SDK and Config Service account must have local administrative rights on the root management server computer. The account should be either a Domain User or Local System. The use of Local User account is not supported. We recommended you use a different account from the one used for the Management Server Action Account.

Agent Installation Account

When implementing discovery-based agent deployment, you are prompted for an account with Administrator privileges. This account is used to install the agent on the computer, and therefore it must be a local administrator on all the computers you are deploying agents to. This account is encrypted before being used and then discarded.

Notification Action Account

This is the action account which is used for creating and sending notifications. Ensure that the credentials you use for this account have sufficient rights for the SMTP server, instant messaging server, or SIP server that you will use for notifications.

See Also

Implementing User Roles

Managing Access in Operations Manager

How to Create a New Action Account in Operations Manager

How to Manage the Report Server Unattended Execution Account in Operations Manager

Control Access by Using the Health Service Lockdown Tool in Operations Manager

Accessing UNIX and Linux Computers in Operations Manager

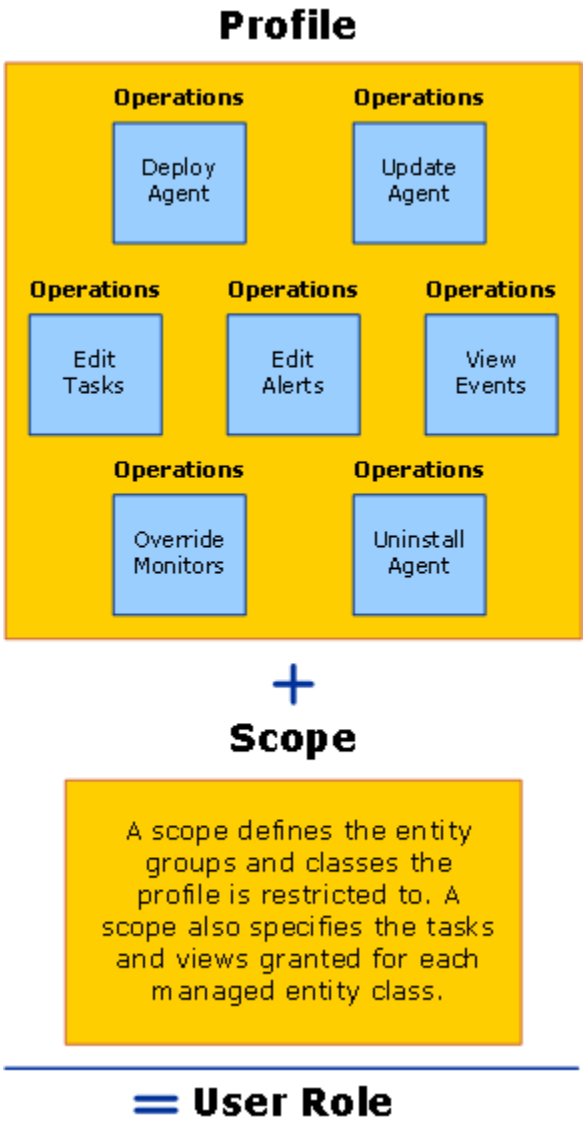
Managing Run As Accounts and Profiles

Implementing User Roles

In System Center 2012 – Operations Manager, user roles are the method you use to assign the rights needed to access monitoring data and perform actions. User roles are designed to apply to groups of users that need access to and perform actions on the same group of monitored objects. By default, only the Operations Manager Administrator account has the right to view and act on monitoring data. All other users must have a user role assigned in order to view or act on monitoring data.

User roles are created using the Create User Role Wizard. In this wizard, you configure which Active Directory security groups are assigned this user role, which Operations Manager group or groups of monitored objects this user can access, and which tasks and views this user role can access.

A user role is the combination of a profile and scope as shown in as shown in the following illustration. A user can be a part of multiple roles and the resultant scope is the union of all the user roles.



Implementing User Roles topics

- Choose a Profile
- Define a Scope Using Operations Manager Groups

- Assign Tasks and Views
- How to Assign Members to User Roles
- Operations Associated with User Role Profiles

See Also

Managing Access in Operations Manager

Operations Manager Accounts

How to Create a New Action Account in Operations Manager

How to Manage the Report Server Unattended Execution Account in Operations Manager

Control Access by Using the Health Service Lockdown Tool in Operations Manager

Accessing UNIX and Linux Computers in Operations Manager

Managing Run As Accounts and Profiles

Choose a Profile

Before you start the Create User Role Wizard, select one profile that applies to the user role you are creating. A profile determines the actions that a user can perform. Profiles have a defined set of rights and you cannot add or remove any of these assigned rights. When creating user roles for operators and other users, select the profile that most closely matches the responsibilities of the group of users in your System Center 2012 – Operations Manager deployment.

Operations Manager can monitor many types of applications in the enterprise. As the Operations Manager administrator, you want to limit access to monitoring data. Role-based security allows you to limit privileges that users have for various aspects of Operations Manager.

Important

Adding a machine account to a user role member allows all services on that computer to have software development kit (SDK) access. It is recommended that you do not add a machine account to any user role.

In Operations Manager, operations—such as resolving alerts, running tasks, overriding monitors, creating user roles, viewing alerts, viewing events, and so on—have been grouped into profiles, with each profile representing a particular job function as shown in the following table. For a list of specific operations associated with each profile, see Operations Associated with User Role Profiles.

Note

A scope defines the entity groups, object types, tasks, or views that a profile is restricted to. Not all scopes apply to all profiles.

Profile	Job Functions and Scope
Administrator	Includes full privileges available in Operations Manager.
Advanced Operator	Includes a set of privileges designed for users who need access to limited adjustment of monitoring configurations in addition to the Operator privileges. Grants members the ability to override the configuration of rules and monitors for specific targets or groups of targets within the configured scope.
Application Monitoring Operator	Includes a set of privileges designed for users that need access to Application Diagnostics. A user role based on the Application Monitoring Operator profile grants members the ability to see the Application Monitoring events in Application Diagnostics web console. **Note** Access to the **Application Advisor** feature requires the Report Operator or Administrator profile.
Author	Includes a set of privileges designed for authoring of monitoring configurations. Grants members the ability to create, edit, and delete monitoring configuration (for example, tasks, rules, monitors, and views) for specific targets or groups of targets within the configured scope.
Operator	Includes a set of privileges designed for users who need access to alerts, views, and tasks. Grants members the ability to interact with alerts, run tasks, and access views according to their configured scope. **Security** When a dashboard view uses data from the data warehouse database, operators might be able to view data that they would not otherwise have access to in views that use data from the operational database.

Profile	Job Functions and Scope
Read-only Operator	Includes a set of privileges designed for users who need read-only access to alerts and views. Grants members the ability to view alerts and access views according to their configured scope. **Note** Members of the Read-only Operator role are not assigned rights to the Task Status view. **Security** When a dashboard view uses data from the data warehouse database, operators might be able to view data that they would not otherwise have access to in views that use data from the operational database.
Report Operator	Includes a set of privileges designed for users who need access to Reports. Grants members the ability to view reports according to their configured scope. **Caution** Users assigned to this role have access to all report data in the Reporting Data Warehouse and are not limited by scope.
Report Security Administrator	Enables the integration of SQL Server Reporting Services security with Operations Manager user roles. This gives Operations Manager Administrators the ability to control access to reports. This role can have only one member account and cannot be scoped.

See Also

Implementing User Roles

Define a Scope Using Operations Manager Groups

Assign Tasks and Views

How to Assign Members to User Roles

Operations Associated with User Role Profiles

Define a Scope Using Operations Manager Groups

The scope of a user role determines which objects that user role can view and perform actions on in System Center 2012 – Operations Manager. A scope is comprised of one or more Operations Manager groups and is defined when creating a user role as part of the **Create User Role Wizard**. The **Group Scope** page of the **Create User Role Wizard** provides a list of all existing Operations Manager groups. You can choose all or some of these groups as the scope of the user role you are creating.

Groups, like other Operations Manager objects, are defined in management packs. In Operations Manager, groups are logical collections of objects, such as Windows-based computers, hard disks, or instances of Microsoft SQL Server. Several groups are created by the management packs that are imported automatically during an Operations Manager installation. If these groups do not contain the monitored objects you need for a scope, you can create a group that does. To do this, you must exit the **Create User Role Wizard**, switch to the **Monitoring** workspace and use the **Create Group Wizard** to create a group that better suits your needs.

See Also

Implementing User Roles

Choose a Profile

Assign Tasks and Views

How to Assign Members to User Roles

Assign Tasks and Views

The Create User Role Wizard contains a page that defines the tasks that the user role you are creating can perform and a page that specifies the views that the user role you are creating can open and use. The default setting is that all users assigned that user role can run all tasks and open all views as long as their profile and scope allows it. The alternative in these wizard pages is to list the specific tasks or views that the user role you are creating can access.

See Also

Implementing User Roles

Choose a Profile
Define a Scope Using Operations Manager Groups
How to Assign Members to User Roles

How to Assign Members to User Roles

System Center 2012 – Operations Manager provides eight standard user roles that are created during setup. You can assign groups and individuals to these built-in user roles to provide them with the ability to perform certain tasks and to access certain information.

The following table describes the built-in user roles, which have global scope for the management group. To limit the scope for a user, create a new user role. For more information, see Implementing User Roles.

Important
When you add a group to the Operations Manager Administrators user role, you must restart the management server for the change to take effect.

User role	Description
Administrator	Has full privileges to all Operations Manager data, services, and tools. **Note** You can only add Active Directory security groups to the Administrator role.
Advanced Operator	Has limited change access to Operations Manager configuration; ability to create overrides to rules; monitors for targets or groups of targets within the configured scope. Advanced Operator also inherits Operator privileges.
Application Monitoring Operator	Includes a set of privileges designed for users that need access to **Application Diagnostics**. The Application Monitoring Operator user role grants members the ability to see the Application Monitoring events in **Application Diagnostics**.
Author	Has ability to create, edit, and delete tasks, rules, monitors, and views within configured scope. Author also inherits Advanced Operator

User role	Description
	privileges.
Operator	Has ability to edit or delete alerts, run tasks, and access views according to configured scope. Operator also inherits Read-Only Operator privileges. **Security** When a dashboard view uses data from the data warehouse database, operators might be able to view data that they would not otherwise have access to in views that use data from the operational database.
Read-Only Operator	Has ability to view alerts and access views according to configured scope. **Security** When a dashboard view uses data from the data warehouse database, operators might be able to view data that they would not otherwise have access to in views that use data from the operational database.
Report Operator	Has ability to view reports according to configured scope.
Report Security Administrator	Enables integration of SQL Reporting Services security with Operations Manager roles.

To assign members to user roles

1. In the Operations console, click **Administration**.
2. In **Security**, click **User Roles**.
3. In the results pane, right-click any of the user roles, such as **Operations Manager Operators**, and click **Properties**.
4. On the **General Properties** tab, in **User role members**, click **Add**.
5. In **Enter the object names to select**, type in name of the user or group account that you want to add to the user role, and then click **OK** to close the dialog box.
6. Click **OK** to close the properties for the user role.

See Also

Implementing User Roles

Choose a Profile

Define a Scope Using Operations Manager Groups

Assign Tasks and Views

Operations Associated with User Role Profiles

This topic provides a list of the operations in System Center 2012 – Operations Manager that are associated with each profile.

Report Operator

The Report Operator profile includes a set of privileges designed for users who need access to reports. A role based on the Report Operator profile grants members the ability to view reports according to their configured scope.

- Retrieve the instance of the data warehouse for the management group
- Write to favorite reports
- Delete favorite reports
- Read favorite reports
- Update favorite reports
- Read reports
- Run reports
- Access Application Advisor

Read-Only Operator

The Read-Only Operator profile includes a set of privileges designed for users who need read-only access to alerts and views. A role based on the Read-Only Operators profile grants members the ability to view alerts and access views according to their configured scope.

- Read alerts
- Retrieve the instance of the data warehouse for the management group
- Read state of a resolution
- Read instance of a connector
- Read console tasks
- Enumerate diagnostic objects
- Enumerate the results of diagnostics

- Enumerate discovery objects as defined in a management pack
- Read discovery rules
- Read events
- Write to favorite console tasks
- Delete favorite console tasks
- Enumerate favorite console tasks
- Update favorite console tasks
- Write favorite views
- Delete favorite views
- Enumerate favorite views
- Update favorite views
- Enumerate monitoring objects
- Enumerate monitoring classes
- Enumerate monitoring relationship classes
- Enumerate management packs
- Enumerate monitor types
- Enumerate module types
- Enumerate monitors
- Enumerate overrides
- Enumerate performance data
- Enumerate discovery objects as defined in a management pack
- Enumerate the status of past recoveries
- Enumerate relationship between monitored objects
- Enumerate rules
- Enumerate saved searches
- Update saved searches
- Write to saved searches
- Delete saved searches
- Enumerate state
- Allows access to connected management groups
- Enumerate views
- Enumerate view types
- Review application monitoring alerts[1]

[1] Permissions scope can be fine-tuned for the role.

Operator

The Operator profile includes a set of privileges designed for users who need access to alerts, views, and tasks. A role based on the Operators profile grants members the ability to interact with

alerts, run tasks, and access views according to their configured scope. The Operator profile contains all of the privileges found in the Read-Only Operator profile in addition to those listed below.

- Update alerts
- Run diagnostics
- Create favorite tasks
- Delete favorite tasks
- Enumerate favorite tasks
- Update favorite tasks
- Run recovery routines
- Update maintenance mode settings
- Enumerate notification actions
- Delete notification actions
- Update notification actions
- Enumerate notification endpoints
- Enumerate notification recipients
- Delete notification recipients
- Update notification recipients
- Enumerate notification subscriptions
- Delete notification subscriptions
- Update notification subscriptions
- Enumerate tasks
- Enumerate task status
- Run tasks
- Run monitoring compatibility check task[1]

  Note
  Additional permissions are required for files/folders to create report files.
- Review application monitoring alerts[1]
- Close application monitoring alerts[1]

[1] Permissions scope can be fine-tuned for the role.

Advanced Operator

The Advanced Operator profile includes a set of privileges designed for users who need access to limited tweaking of monitoring configurations in addition to the Operators privileges. A role based on the Advanced Operators profile grants members the ability to override the configuration of rules and monitors for specific targets or groups of targets within the configured scope. The Advanced Operator profile contains all of the privileges found in the Operator and Read-Only Operator profiles in addition to those listed below.

- Update management packs
- Enumerate templates
- Customize APM configuration with the overrides[1]
- Run monitoring compatibility check task[1]

  Note
  Additional permissions are required for files/folders to create report files.
- Review application monitoring alerts[1]
- Close application monitoring alerts[1]

[1] Permissions scope can be fine-tuned for the role.

Application Monitoring Operator

The Application Monitoring Operator profile includes a set of privileges designed for users that need access to Application Diagnostics. A user role based on the Application Monitoring Operator profile grants members the ability to see the Application Monitoring events in Application Diagnostics web console.

- Access Application Diagnostics

Author

The Author profile includes a set of privileges designed for authoring monitoring configurations. A role based on the Authors profile grants members the ability to create, edit, and delete monitoring configuration (tasks, rules, monitors, and views) within the configured scope. For convenience, Authors can also be configured to have Advanced Operator privileges scoped by group. The Author profile contains all of the privileges found in the Advanced Operator, Operator, and Read-Only Operator profiles in addition to those listed below.

- Create management packs
- Delete management packs
- Enumerate Run As Profiles
- Customize APM configuration with the overrides[1]
- Author new APM workflows[1]
- Run monitoring compatibility check task[1]

  Note
  Additional permissions are required for files/folders to create report files.
- Review application monitoring alerts[1]
- Close application monitoring alerts[1]

[1] Permissions scope can be fine-tuned for the role.

Administrator

The Administrator profile includes full privileges to Operations Manager. No scoping of the Administrator profile is supported. The Administrator profile contains all of the privileges found in the Author, Advanced Operator, Operator, and Read-Only Operator profiles in addition to those listed below.

- Create a resolution state
- Delete a resolution state
- Update a resolution state
- Deploy an agent
- Repair or update an installed agent
- Uninstall an agent
- Enumerate agent settings
- Update agent settings
- Enumerate agents
- Start or stop managing computers or devices via a proxy health service
- Enumerate computers or devices managed via a proxy health service
- Insert a new instance of a computer or device
- Delete an instance of a computer or device
- Run discovery task
- Create events
- Enumerate global settings
- Update global settings
- Export management packs
- Enumerate management servers
- Delete notification endpoint
- Update notification endpoint
- Create performance data
- Create Run As Accounts
- Delete Run As Accounts
- Enumerate Run As Accounts
- Update Run As Accounts
- Create mappings between Run As Accounts and Run As Profiles
- Delete mappings between Run As Accounts and Run As Profiles
- Enumerate mappings between Run As Accounts and Run As Profiles
- Update mappings between Run As Accounts and Run As Profiles
- Create connected management groups
- Delete connected management groups
- Enumerate user roles

- Delete user roles
- Update user roles
- Write favorite reports
- Delete favorite reports
- Read favorite reports
- Update favorite reports
- Read reports
- Run reports
- Run APM Wizard or change APM settings
- Access Application Diagnostics
- Access Application Advisor
- Author new APM workflows
- Customize APM configuration with the overrides
- Run monitoring compatibility check task
- Review application monitoring alerts
- Close application monitoring alerts
- Control access rights to application monitoring
- Create group
- Edit group
- Delete group

Report Security Administrator

The Report Security Administrator profile includes a set of privileges designed to enable the integration of SQL Server Reporting Services security with Operations Manager.

- Export management packs
- Enumerate classes as defined in the management packs
- Enumerate management packs
- Run reports
- Enumerate rules
- Access Application Advisor

See Also

Implementing User Roles

Define a Scope Using Operations Manager Groups

Assign Tasks and Views

How to Assign Members to User Roles

Choose a Profile

How to Create a New Action Account in Operations Manager

Use the following procedure to create a new action account. The new action account will not, by default, have access to the Operations Manager database unless access is inherited in the credentials you assign to the action account. If not, a new account for accessing the Operations Manager database will need to be created.

To create a new action account

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. In the Administration workspace, right-click **Run As Accounts**, and then click **Create Run As Account**.
4. In the **Create Run As Account Wizard**, on the **Introduction** page, click **Next**.
5. On the **General** page, do the following:
   a. In the **Run As Account type** list, select **Action Account**.
   b. Type a display name in the **Display Name** text box.

      Note
      The display name you enter here becomes the Run As account you will add to a new Run As profile in the following procedure.

   c. You can also type a description in the **Description** text box.
   d. Click **Next**.
6. On the **Account** page, type a user name, password, and then select the domain for the account that you want to make a member of this Run As account, and then click **Next**.
7. On the **Distribution Security** page, the **More secure** option is selected and cannot be changed. Click **Create**.
8. In the **Administration** workspace, click **Run As Profiles**.
9. In **Run As Profiles**, right-click **Default Action Account**, and then click **Properties**.
10. On the **Introduction** and **General Properties** pages, click **Next**.
11. On the **Run As Accounts** page, click **Add**, select the Run As account you created, and then click **OK** twice.
12. Click **Save**.

See Also

Managing Access in Operations Manager

Operations Manager Accounts

Implementing User Roles

How to Manage the Report Server Unattended Execution Account in Operations Manager
Control Access by Using the Health Service Lockdown Tool in Operations Manager
Accessing UNIX and Linux Computers in Operations Manager
Managing Run As Accounts and Profiles

How to Manage the Report Server Unattended Execution Account in Operations Manager

The Operations Manager Report Server unattended execution account is used to query data from the Reporting Data Warehouse. Users that manage this account require only the Read user right. This account is not managed from within the Operations Manager user interface. Use this procedure to change the user name or password for this account.

To manage the Report Server unattended execution account

1. On the Windows desktop, click **Start**, point to **Programs**, point to **Microsoft SQL Server 2008**, point to **Configuration Tools**, and then click **Reporting Services Configuration Manager**.
2. In **Reporting Services Configuration Manager**, in the **Report Server Installation Instance Selection** dialog box, click **Connect**.
3. In the navigation pane, click **Execution Account**.
4. In the **Execution Account** pane, type a new user name or password as required.
5. Click **Apply**, and then click **Exit**.

See Also

Managing Access in Operations Manager
Operations Manager Accounts
Implementing User Roles
How to Create a New Action Account in Operations Manager
Control Access by Using the Health Service Lockdown Tool in Operations Manager
Accessing UNIX and Linux Computers in Operations Manager
Managing Run As Accounts and Profiles

Control Access by Using the Health Service Lockdown Tool in Operations Manager

On computers requiring high security, for example a domain controller, you may need to deny certain identities access to rules, tasks, and monitors that might jeopardize the security of your server. The Health Service lockdown tool (HSLockdown.exe) enables you to use various command-line options to control and limit the identities used to run a rule, task, or monitor.

Note
You will be unable to start the System Center Management service if you have used the Health Service Lockdown tool to lock out the Action Account. To be able to restart the System Center Management service, follow the second procedure in this topic to unlock the Action Account.

The following command-line options are available:

- HSLockdown [ManagementGroupName] /L - List Accounts/groups
- HSLockdown [ManagementGroupName] /A - Add an allowed account|group
- HSLockdown [ManagementGroupName] /D - Add a denied account|group
- HSLockdown [ManagementGroupName] /R - Remove an allowed/denied account|group

Accounts must be specified in one of the following fully qualified domain name (FQDN) formats:

- NetBios : DOMAIN\username
- UPN : username@fqdn.com

If you used the add or deny options when running the Health Service Lockdown tool, you will need to restart the System Center Management service before the changes take effect.

When evaluating allowed and denied listings, know that denies takes priority over allows. If a user is listed as allowed, and the same user is a member of a group that is listed as denied, the user will be denied.

To use the health service lockdown tool

1. Log on to the computer with an account that is a member of the Administrators group.
2. On the Windows desktop, click **Start**, and then click **Run**.
3. In the **Run** dialog box, type **cmd** and then click **OK**.
4. At the command prompt, type <drive_letter>: (where <drive_letter> is the drive where the Operations Manager installation media is located) and then press ENTER.
5. Type **cd\Program Files\System Center Operations Manager 2012\Server** and then press ENTER.
6. Type **HSLockdown [Management Group Name] /D [account or group]** to deny the group or account, and then press ENTER.

To unlock the Action Account

1. Log on to the computer with an account that is a member of the Administrators group.
2. On the Windows desktop, click **Start**, and then click **Run**.
3. In the **Run** dialog box, type **cmd** and then click **OK**.
4. At the command prompt, type <drive_letter>: (where <drive_letter> is the drive where the Operations Manager installation media is located) and then press **ENTER**.
5. Type **cd\Program Files\System Center Operations Manager 2012** and then press ENTER.
6. Type **HSLockdown [Management Group Name] /A <Action Account>** and then press ENTER.

See Also

Managing Access in Operations Manager

Operations Manager Accounts

Implementing User Roles

How to Create a New Action Account in Operations Manager

How to Manage the Report Server Unattended Execution Account in Operations Manager

Accessing UNIX and Linux Computers in Operations Manager

Managing Run As Accounts and Profiles

Accessing UNIX and Linux Computers in Operations Manager

In System Center 2012 – Operations Manager, the management server uses two protocols to communicate with the UNIX or Linux computer:

- Secure Shell (SSH)

  Used for installing, upgrading, and removing agents.
- Web Services for Management (WS-Management)

  Used for all monitoring operations and include the discovery of agents that were already installed.

The protocol that is used depends on the action or information that is requested on the management server. All actions, such as agent maintenance, monitors, rules, tasks, and recoveries, are configured to use predefined profiles according to their requirement for an unprivileged or privileged account.

Note

All credentials referred to in this topic pertain to accounts that have been established on the UNIX or Linux computer, not to the Operations Manager accounts that are configured

during the installation of Operations Manager. Contact your system administrator for credentials and authentication information.

For detailed instructions for specifying credentials and configuring accounts, see How to Set Credentials for Accessing UNIX and Linux Computers.

Authentication on the UNIX or Linux Computer

In Operations Manager, the system administrator is no longer is required to provide the root password of the UNIX or Linux computer to the management server. Now by elevation, an unprivileged account can assume the identity of a privileged account on the UNIX or Linux computer. The elevation process is performed by the UNIX su (superuser) and sudo programs that use the credentials that the management server supplies. For privileged agent maintenance operations that use SSH (such as discovery, deployment, upgrades, uninstallation, and agent recovery), support for su, sudo elevation, and support for SSH key authentication (with or without passphrase) is provided. For privileged WS-Management operations (such as viewing secure log files), support for sudo elevation (without password) is added.

Accessing UNIX and Linux Computers Topics

- Credentials You Must Have to Access UNIX and Linux Computers

  Provides an overview of using credentials to install and maintain agents on UNIX and Linux computers and how they are configured to use Run As accounts and Run As profiles.
- How to Set Credentials for Accessing UNIX and Linux Computers

  Contains specific procedures for specifying credentials for different wizards in Operations Manager.
- How to Configure sudo Elevation and SSH Keys

  Describes how to configure an unprivileged account to be elevated to have privileged access on a UNIX or Linux computer.
- Required Capabilities for UNIX and Linux Accounts

  Describes the permissions on the UNIX or Linux computers that are required to be configured with Run As profiles for use by Operations Manager.
- Administering and Configuring the UNIX/Linux Agent

  Describes options to administer and configure the UNIX/Linux agent for System Center – Operations Manager.

Other Resources for this Feature

- Managing Access in Operations Manager
- Credentials You Must Have to Access UNIX and Linux Computers
- Implementing User Roles
- How to Create a New Action Account in Operations Manager

- How to Manage the Report Server Unattended Execution Account in Operations Manager
- Control Access by Using the Health Service Lockdown Tool in Operations Manager
- Managing Run As Accounts and Profiles

Credentials You Must Have to Access UNIX and Linux Computers

This topic describes how you use credentials to install, maintain, upgrade, and uninstall agents.

Credentials for Installing Agents

Operations Manager uses the Secure Shell (SSH) protocol to install an agent and Web Services for Management (WS-Management) to discover previously installed agents. Installation requires a privileged account on the UNIX or Linux computer. There are two ways to provide credentials to the targeted computer, as obtained by the **Computer and Device Management Wizard**:

- Specify a user name and password.

  The SSH protocol uses the password to install an agent or the WS-Management protocol if the agent was already installed by using a signed certificate.
- Specify a user name and an SSH key. The key can include an optional passphrase.

If you are not using the credentials for a privileged account, you can provide additional credentials so that your account becomes a privileged account through elevation of privilege on the UNIX or Linux computer.

The installation is not completed until the agent is verified. Agent verification is performed by the WS-Management protocol that uses credentials maintained on the management server, separate from the privileged account that is used to install the agent. You are required to provide a user name and password for agent verification if you have done one of the following:

- Provided a privileged account by using a key.
- Provided an unprivileged account to be elevated by using sudo with a key.
- Ran the wizard with the **Discovery Type** set to **Discover only computers with the UNIX/Linux agent installed**.

Alternatively, you can install the agent, including its certificate, manually on the UNIX or Linux computer and then discover that computer. This method is the most secure way to install agents. For more information, see Install Agent and Certificate on UNIX and Linux Computers Using the Command Line.

Credentials for Monitoring Operations and Performing Agent Maintenance

Operations Manager contains three predefined profiles to use in monitoring UNIX and Linux computers and performing agent maintenance:

- UNIX/Linux action account

  This profile is an unprivileged account profile that is required for basic health and performance monitoring.
- UNIX/Linux privileged account

  This profile is a privileged account profile used for monitoring protected resources such as log files.
- UNIX/Linux maintenance account

  This profile is used for privileged maintenance operations, such as updating and removing agents.

In the UNIX and Linux management packs, all the rules, monitors, tasks, recoveries, and other management pack elements are configured to use these profiles. Consequently, there is no requirement to define additional profiles by using the Run As Profiles Wizard unless special circumstances dictate it. The profiles are not cumulative in the scope. For example, the UNIX/Linux maintenance account profile cannot be used in place of the other profiles simply because it is configured by using a privileged account.

In Operations Manager, a profile cannot function until it is associated with at least one Run As account. The credentials for accessing the UNIX or Linux computers are configured in the Run As accounts. Because there are no predefined Run As accounts for UNIX and Linux monitoring, you must create them.

To create a Run As account, you must run the **UNIX/Linux Run As Account Wizard** that is available when you select **UNIX/Linux Accounts** in the **Administration** workspace. The wizard creates a Run As account based on the choice of a Run As account type. There are two Run As account types:

- Monitoring account

  Use this account for ongoing health and performance monitoring in operations that communicate by using WS-Management.
- Agent maintenance account

  Use this account for agent maintenance such as updating and uninstalling in operations that communicate by using SSH.

These Run As account types can be configured for different levels of access according to the credentials that you supply. Credentials can be unprivileged or privileged accounts or unprivileged accounts that will be elevated to privileged accounts. The following table shows the relationships between profiles, Run As accounts, and levels of access.

Profiles	Run As account type	Allowable Access Levels
UNIX/Linux action account	Monitoring account	• Unprivileged • Privileged • Unprivileged, elevated to privileged
UNIX/Linux privileged account	Monitoring account	• Privileged • Unprivileged, elevated to privileged
UNIX/Linux maintenance account	Agent maintenance account	• Privileged • Unprivileged, elevated to privileged

Note that there are three profiles, but only two Run As Account types.

When you specify a Monitoring Run As Account Type, you must specify a user name and password for use by the WS-Management protocol. When you specify an Agent Maintenance Run As Account Type, you must specify how the credentials are supplied to the targeted computer by using the SSH protocol:

- Specify a user name and a password.
- Specify a user name and a key. You can include an optional passphrase.

After you created the Run As accounts, you must edit the UNIX and Linux profiles to associate them with the Run As accounts you created. For detailed instructions, see How to Configure Run As Accounts and Profiles for UNIX and Linux Access.

Credentials for Upgrading and Uninstalling Agents

The **UNIX/Linux Agent Upgrade Wizard** and the **UNIX/Linux Agent Uninstall Wizard** provide credentials to their targeted computers. The wizards first prompt you to select the targeted computers to upgrade or uninstall, followed by options on how to provide the credentials to the targeted computer:

- **Use existing associated Run As Accounts**

  Select this option to use the credentials associated with the UNIX/Linux action account profile and the UNIX/Linux maintenance account profile.

  The wizard alerts you if you or more of the selected computers do not have an associated Run As account in the required profiles, in which case you must go back and clear those computers that do not have an associated Run As account, or use the other option.

- **Specify credentials**

  Select this option to specify Secure Shell (SSH) credentials by using a user name and password or a user name and a key. You can optionally provide a passphrase with a key. If

the credentials are not for a privileged account, you can have them elevated to a privileged account on the target computered by using the UNIX su or sudo elevation programs. The ‘su’ elevation requires a password. If you use sudo elevation, you are prompted for a user name and password for agent verification by using an unprivileged account.

For more information about upgrading and uninstalling, see Upgrading and Uninstalling Agents on UNIX and Linux Computers.

See Also

How to Set Credentials for Accessing UNIX and Linux Computers

Accessing UNIX and Linux Computers in Operations Manager

How to Configure sudo Elevation and SSH Keys

Required Capabilities for UNIX and Linux Accounts

Configuring SSL Ciphers

How to Set Credentials for Accessing UNIX and Linux Computers

This topic contains procedures for how to set credentials in wizards for the following tasks, as set by wizards in System Center 2012 – Operations Manager:

- Credentials for Installing Agents or Signing Certificates of Installed Agents
- Credentials for Run As Accounts
- Credentials for Upgrading an Agent
- Credentials for Uninstalling an Agent

These wizards define credentials to be authenticated on the UNIX or Linux computer and follow a similar process. For an overview of how credentials are provided, see Accessing UNIX and Linux Computers in Operations Manager.

Credentials for Discovering UNIX and Linux Computers

The following procedure begins in **Computer and Device Management Wizard**, on the **Discovery Criteria** page, when you click the **Set Credentials** button. For more information, see Install Agent on UNIX and Linux Using the Discovery Wizard.

To set a user (unprivileged) account for discovery of an installed agent with a signed certificate.

1. On the **Credential Settings** page, click the **Default Credentials** tab, and then click the **Password** option.

2. Type a user name, a password, and the password confirmation.
3. In the **Does this account have privileged access** list, click **This account does not have privileged access**, and then click **OK**.
4. Click **OK** to return to the **Discovery Criteria** page and continue with the wizard.

Credentials for Installing Agents or Signing Certificates of Installed Agents

The following procedures begin in the **Computer and Device Management Wizard**, on the **Discovery Criteria** page, when you click the **Set Credentials** button.

To set a privileged credential by using an SSH key

1. On the **Credential Settings** page, click the **Default Credentials** tab, and then click the **SSH key** option.
2. Type a user name, the path, and name of the key, or click **Browse**.
3. Enter a passphrase if the key requires it.
4. In the **Does this account have privileged access** list, click **This account has privileged access**, and then click **OK**.
5. Click the **Agent Verification** tab, and on the **Agent Verification** page, type a user name and password for an account on the targeted computer. This can be a user (unprivileged) account.
6. Click **OK** to return to the **Discovery Criteria** page and continue with the wizard.

To set a unprivileged credential with elevation by using an SSH key

1. On the **Credential Settings** page, click the **Default Credentials** tab, and then click the **SSH key** option.
2. Type a user name, the path, and name of the key, or click **Browse**.
3. Enter a passphrase if the key requires it.
4. In the **Does this account have privileged access** list, click **This account does not have privileged access**, and then click **OK**.
5. Click the **Elevation** page, and select **su** or **sudo elevation**.

   If you select **su elevation**, type the **superuser** password as established on the UNIX or Linux computer. The **su** password is also used for agent verification.

   If you selected **sudo elevation**, click the **Agent Verification** tab, and type a user name and password for an account on the targeted computer. This can be a user (unprivileged) account.
6. Click **OK** to return to the **Discovery Criteria** page and continue with the wizard.

To set a privileged credential by using a password

1. On the **Credential Settings** page, click the **Default Credentials** tab, and then click the

Password option.

2. Type a user name, a password, and password confirmation.

   This password is used for agent verification.

3. In the **Does this account have privileged access** list, click **This account has privileged access**.
4. Click **OK** to return to the **Discovery Criteria** page and continue with the wizard.

To set an unprivileged credential with elevation by using a password

1. On the **Credential Settings** page, click the **Default Credentials** tab, and then click the **Password** option.
2. Type a user name, a password, and the password confirmation.

   This password is used for agent verification.

3. In the **Does this account have privileged access** list, click **This account does not privileged access**, and then click **OK**.
4. Click the **Elevation** page, and select **su** or **sudo elevation**.

   If you select **su elevation**, type the **superuser** password you established on the UNIX or Linux computer.

5. Click **OK** to return to the **Discovery Criteria** page and continue with the wizard.

Credentials for Run As Accounts

The following procedures begin in the **Create UNIX/Linux Run As Account Wizard** when you select the type for a **Run As Account** (**Monitoring Account** or **Agent Maintenance Account**), a name and password and provided a description. For more information, see How to Configure Run As Accounts and Profiles for UNIX and Linux Access.

To set a privileged credential for a monitoring account

1. On the **Account Credentials** page, type a user name, a password, and the password confirmation.
2. In the **Do you want to use elevation for privileged access** list, click **Do not use elevation with this account**.
3. Click **Next** to continue with the wizard.

To set an unprivileged credential with elevation for a monitoring account

1. On the **Account Credentials** page, type a user name, a password, and the password confirmation.
2. In the **Do you want to use elevation for privileged access** list, click **Elevate this account using sudo for privileged access**.
3. Click **Next** to continue with the wizard.

To set a privileged credential by using an SSH key for an agent maintenance account

1. On the **Account Credentials** page, click the **SSH key** option.
2. Type a user name, the path, and name of the key, or click **Browse**.
3. Enter a passphrase if the key requires it.
4. In the **Does the account have privileged access** list, click **This account has privileged access**.
5. Click **Next** to continue with the wizard.

To set an unprivileged credential by using an SSH key with elevation for an agent maintenance account

1. On the **Account Credentials** page, click the **SSH key** option.
2. Type a user name, the path, and name of the key, or click **Browse**.
3. Enter a passphrase if the key requires it.
4. In the **Does this account have privileged access** list, click **This account does not have privileged access**, and then click **Next**.
5. Select the **Elevation** tab, and select **su** or **sudo elevation**.

   If you select **su elevation**, type the **superuser** password as established on the UNIX or Linux computer.
6. Click **Next** to continue with the wizard.

To set a privileged credential by using a password for an agent maintenance account

1. On the **Account Credentials** page, click the **Password** option.
2. Type a user name, a password, and the password confirmation.
3. In the **Does this account have privileged access** list, click **This account has privileged access**.
4. Click **Next** to continue with the wizard.

To set a privileged credential by using a password with elevation for an agent maintenance account

1. On the **Account Credentials** page, click the **Password** option.
2. Type a user name, a password, and the password confirmation.
3. In the **Does this account have privileged access** list, click **This account does not have privileged access**, and then click **Next**.
4. Click the **Elevation** tab, and select **su** or **sudo elevation**.

   If you select **su elevation**, type the **superuser** password as established on the UNIX or Linux computer.
5. Click **Next** to continue with the wizard.

Credentials for Upgrading an Agent

The following procedures begin in the **UNIX/Linux Agent Upgrade Wizard** on the **Credentials** page, when you select **Provide Upgrade Credentials**. For more information, see Upgrading and Uninstalling Agents on UNIX and Linux Computers.

To set a privileged credential by using an SSH key

1. On the **Credential Settings** page, click the **SSH key** option.
2. Type a user name, the path, and name of the key, or click **Browse**.
3. Enter a passphrase if the key requires it.
4. In the **Does this account have privileged access** list, click **This account has privileged access**, and then click **OK**.
5. On the **Agent Verification** page, type a user name and password for an account on the targeted computer. This can be a user (unprivileged) account.
6. Click **OK** to return to the **Credentials** page and continue with the wizard.

To set a unprivileged credential with elevation by using an SSH key

1. On the **Credential Settings** page, click the **SSH key** option.
2. Type a user name, the path, and name of the key, or click **Browse**.
3. Enter a passphrase if the key requires it.
4. In the **Does this account have privileged access** list, click **This account does not have privileged access**, and then click **OK**.
5. Click the **Elevation** page, and select **su** or **sudo elevation**.

   If you select **su elevation**, type the **superuser** password as established on the UNIX or Linux computer, and then click **OK**. The **su** password is also used for agent verification.

   If you select **sudo elevation**, click **Agent Verification**. On the **Agent Verification** page, type a user name and password for an account on the targeted computer. This can be a user (unprivileged) account.
6. Click **OK** to return to the **Credentials** page and continue with the wizard.

To set a privileged credential by using a password

1. On the **Credential Settings** page, click the **Password** option.
2. Type a user name, a password, and password confirmation.

   This password is used for agent verification.
3. In the **Does this account have privileged access** list, click **This account has privileged access** .
4. Click **OK** to return to the **Credentials** page and continue with the wizard.

To set an unprivileged credential with elevation by using a password

1. On the **Credential Settings** page, click the **Password** option.
2. Type a user name, a password, and the password confirmation.

   This password is used for agent verification.
3. In the **Does this account have privileged access** list, click **This account does not privileged access**, and then click **OK**.
4. On the **Elevation** page, select **su** or **sudo elevation**.

   If you select **su elevation**, type the **superuser** password as established on the UNIX or Linux computer.
5. Click **OK** to return to the **Credentials** page and continue with the wizard.

Credentials for Uninstalling an Agent

The following procedures begin in the **UNIX/Linux Agent Uninstall Wizard**, on the **Credentials** page, when you select **Provide Uninstall Credentials**. For more information, see, Upgrading and Uninstalling Agents on UNIX and Linux Computers.

To set a privileged credential by using an SSH key

1. On the **Credential Settings** page, click the **SSH key** option.
2. Type a user name, the path, and name of the key, or click **Browse**.
3. Enter a passphrase if the key requires it.
4. In the **Does this account have privileged access** list, click **This account has privileged access**, and then click **OK**.
5. Click **OK** to return to the **Credentials** page and continue with the wizard.

To set a unprivileged credential with elevation by using an SSH key

1. On the **Credential Settings** page, click the **SSH key** option.
2. Type a user name, the path, and name of the key, or click **Browse**.
3. Enter a passphrase if the key requires it.
4. In the **Does this account have privileged access** list, click **This account does not have privileged access**, and then click **OK**.
5. On the **Elevation** page, select **su** or **sudo elevation**.

   If you select **su elevation**, type the **superuser** password as established on the UNIX or Linux computer, and then click **OK**. The **su** password is also used for agent verification.
6. Click **OK** to return to the **Credentials** page and continue with the wizard.

To set a privileged credential by using a password

1. On the **Credential Settings** page, click the **Password** option.
2. Type a user name, a password, and password confirmation.

   This password is used for agent verification.

3. In the **Does this account have privileged access** list, select **This account has privileged access** .
4. Click **OK** to return to the **Credentials** page and continue with the wizard.

To set an unprivileged credential with elevation by using a password

1. On the **Credential Settings** page, click the **Password** option.
2. Type a user name, a password, and the password confirmation.

   This password is used for agent verification.
3. In the **Does this account have privileged access** list, click **This account does not privileged access**, and then click **OK**.
4. On the **Elevation** page, select **su** or **sudo elevation**.

   If you select **su elevation**, type the **superuser** password as established on the UNIX or Linux computer.
5. Click **OK** to return to the **Credentials** page and continue with the wizard.

See Also

Credentials You Must Have to Access UNIX and Linux Computers

Accessing UNIX and Linux Computers in Operations Manager

How to Configure sudo Elevation and SSH Keys

Required Capabilities for UNIX and Linux Accounts

Configuring SSL Ciphers

How to Configure sudo Elevation and SSH Keys

Starting with System Center 2012 – Operations Manager, you can provide credentials for an unprivileged account to be elevated on a UNIX or Linux computer by using the sudo program, which allows users to run programs that have the security privileges of another user account. You can also use Secure Shell (SSH) keys instead of a password for secure communication between Operations Manager and the targeted computer.

This topic provides examples for creating an account for a low-privileged user, implementing sudo, and creating an SSH key on a computer that is running Red Hat Enterprise Linux Server 6. These are examples only, and might not reflect your environment. The following examples provide a user with access to a full set of privileges.

To obtain and configure the SSH key from the UNIX and Linux computer, you have to install the following software on your Windows-based computer:

- A file transfer tool, such as WinSCP, to transfer files from the UNIX or Linux computer to the Windows-based computer.
- The PuTTY program, or a similar program, to run commands on the UNIX or Linux computer.
- The PuTTYgen program to save the private SHH key in OpenSSH format on the Windows-based computer.

Note

The sudo program exists at different locations on UNIX and Linux operating systems. To provide uniform access to sudo, the UNIX and Linux agent installation script creates the symbolic link `/etc/opt/microsoft/scx/conf/sudodir` to point to the directory expected to contain the sudo program. The agent uses this symbolic link to invoke sudo. The installation script automatically creates the symbolic link, so you do not need to take any action on standard UNIX and Linux configurations; however, if you have sudo installed at a non-standard location, you should change the symbolic link to point to the directory where sudo is installed. If you change the symbolic link, its value is preserved across uninstall, re-install, and upgrade operations with the agent.

Configure a Low-Privileged Account for sudo Elevation

The following procedures create a low-privileged account and sudo elevation by using `opsuser` for a user name.

To create a low-privileged user

1. Log on to the UNIX or Linux computer as `root`.
2. Add the user:

   ```
   useradd opsuser
   ```

3. Add a password and confirm the password:

   ```
   passwd opsuser
   ```

You can now configure sudo elevation and create an SSH key for `opsuser`, as described in the following procedures.

To configure sudo elevation for the low-privileged user

1. Log on to the UNIX or Linux computer as `root`.
2. Use the visudo program to edit the sudo configuration in a vi text editor. Run the following command:

   ```
   visudo
   ```

3. Find the following line:

   ```
   root ALL=(ALL)  ALL
   ```

4. Insert the following line after it:

```
opsuser ALL=(ALL) NOPASSWD: ALL
```

5. TTY allocation is not supported. Ensure the following line is commented out:

   ```
   # Defaults requiretty
   ```

   Important
   This step is required for sudo to work.

6. Save the file and exit visudo:

   Press ESC + : (colon) followed by `wq!`, and then press Enter.

7. Test the configuration by entering in the following two commands. The result should be a listing of the directory without being prompted for a password:

   ```
   su - opsuser
   ```

   ```
   sudo ls /etc
   ```

You can use the `opsuser` account by using the password and sudo elevation for specifying credentials in Operations Manager wizards and for configuring Run As accounts.

Create an SSH Key for Authentication

The following procedures create an SSH key for the `opsuser` account that was created in the previous examples.

To generate the SSH key

1. Log on as `opsuser`.
2. Generate the key by using the Digital Signature Algorithm (DSA) algorithm:

   ```
   ssh-keygen –t dsa
   ```

   Note the optional passphrase if you provided it.

The **ssh-keygen** creates the `/home/opsuser/.ssh` directory with the private key file (`id_dsa`) and the public key file (`id_dsa.pub`). You can now configure the key to be supported by `opsuser` as described in the next procedure.

To configure a user account to support the SSH key

1. At the command prompt, type the following commands. To navigate to the user account directory:

   ```
   cd /home/opsuser
   ```

2. Specify exclusive owner access to the directory:

   ```
   chmod 700 .ssh
   ```

3. Navigate to the .ssh directory:

   ```
   cd .ssh
   ```

4. Create an authorized keys file with the public key:

   ```
   cat id_dsa.pub >> authorized_keys
   ```

5. Give the user read and write permissions to the authorized keys file:

   ```
   chmod 600 authorized_keys
   ```

You can now copy the private SSH key to the Windows-based computer, as described in the next procedure.

To copy the private SSH key to the Windows-based computer and save in OpenSSH format

1. Use a tool, such as WinSCP, to transfer the private key file (`id_dsa` – with no extension) from the UNIX or Linux computer to a directory on your Windows-based computer.
2. Run PuTTYgen.
3. In the **PuTTY Key Generator** dialog box, click the **Load** button, and then select the private key (`id_dsa`) that you transferred from the UNIX or Linux computer.
4. Click **Save private key** and name and save the file to the desired directory.

You can use the `opsuser` account by using the SSH key and sudo elevation for specifying credentials in Operations Manager wizards and for configuring Run As accounts.

See Also

How to Set Credentials for Accessing UNIX and Linux Computers

Accessing UNIX and Linux Computers in Operations Manager

Credentials You Must Have to Access UNIX and Linux Computers

Required Capabilities for UNIX and Linux Accounts

Configuring SSL Ciphers

Required Capabilities for UNIX and Linux Accounts

Access to UNIX and Linux computers in System Center 2012 – Operations Manager uses three Run as profiles. One profile is associated with an unprivileged account while the other two accounts are associated with a privileged account or an unprivileged account that is elevated by using `sudo` or `su`.

In the simplest case, a privileged account has capabilities equivalent to a UNIX and Linux root account, while an unprivileged account has capabilities equivalent to a normal user account. However, with some computer versions of UNIX and Linux, and when you use `sudo` for privilege elevation, you can assign more specific capabilities to accounts. In support of such specific assignments, the following table lists the specific capabilities required by accounts that are assigned to each of the three Run as profiles. These descriptions are somewhat generic because information, such as exact file system paths, can vary among different UNIX and Linux computer versions.

Note

The following table describes the required capabilities for accounts to communicate with the Operations Manager agent on a managed UNIX or Linux computer, but the agent itself must always run under the root account on the UNIX or Linux computer.

UNIX and Linux profile	Required capabilities
Action profile	• To log the UNIX or Linux computer on to the network, authenticated by the Pluggable Authentication Modules (PAM). Must have the ability to run a background shell (not connected to a TTY). Interactive logons are not required. • To read any log file that was specified as unprivileged when a custom log file monitor was created, plus the ability to run **/opt/microsoft/scx/bin/scxlogfilereader**. • To fully run any command shell command that was specified as unprivileged when a command-line monitor, rule, or task was created. • To run **/usr/bin/vmstat** for the **Run VMStat** task.

Privileged profile	• To log the UNIX or Linux computer on to the network, authenticated by the PAM. Must have the ability to run a background shell (not connected to a TTY). Interactive logons are not required. In the case of an account that is elevated by using `sudo`, this requirement applies to the account before it is elevated.
	• To fully run any shell command line that was specified as privileged when a command-line monitor, rule, or discovery was created.
	• To have the following log file monitoring capabilities:
	  • To read the log file to be monitored.
	  By default, log files such as Syslog are usually set to be readable only by root, and accounts assigned to this profile must be able to read these files. Instead of giving accounts full root

UNIX and Linux profile	Required capabilities
	privileges, the log file permissions could be changed to grant read access to a secure group, and accounts made a member of that group. Note that if the log file is periodically rotated, you must ensure that the rotation procedure maintains the group permissions. • To read any log file that was specified as privileged when a custom log file monitor was created. • To run **/opt/microsoft/scx/bin/scxlogfilereader**. • To run tasks, recoveries, and diagnostics. These requirements must be met only if the Operations Manager operator explicitly decides to run them. • Many recoveries include stopping and restarting a daemon process. These recoveries require the ability to run the service control interfaces (such as **/etc/init.d** for Linux, and **svcadm** for Solaris) in order to stop and restart it. Such service control interfaces typically require the ability to run the **kill** command against the daemon process and to run other basic UNIX and Linux commands. • The requirements for other tasks, recoveries, and diagnostics depend on the details of that particular action.
Agent maintenance profile, and for accounts used to install agents for initial monitoring.	• To log the UNIX or Linux computer on to the network by using Secure Shell (SSH), authenticated by the PAM. Must have the ability to run a background shell (not connected to a TTY). Interactive logons are not required. In the case of an account that is elevated by using `sudo`, this requirement applies to the account before it is elevated. • To run the system package installation program, such as **rpm** on Linux, to install the Operations Manager agent.

UNIX and Linux profile	Required capabilities

	• To read and write the following directories, and to create them and any subdirectories under them if they do not exist:
	  • **/opt**
	  • **/opt/microsoft**
	  • **/opt/microsoft/scx**
	  • **/etc/opt/microsoft/scx**
	  • **/var/opt/microsoft/scx**
	• To run the **kill** command against the running Operations Manager agent processes.
	• To start the Operations Manager agent.
	• To add and remove a system daemon, including the Operations Manager agent, by using platform tools to do so.
	• To run basic UNIX and Linux commands, such as **cat**, **ls**, **pwd**, **cp**, **mv**, **rm**, **gzip** (or equivalent).

See Also

How to Set Credentials for Accessing UNIX and Linux Computers

Accessing UNIX and Linux Computers in Operations Manager

How to Configure sudo Elevation and SSH Keys

Credentials You Must Have to Access UNIX and Linux Computers

Configuring SSL Ciphers

Configuring SSL Ciphers

System Center 2012 – Operations Manager correctly manages UNIX and Linux computers without changes to the default Secure Sockets Layer (SSL) cipher configuration. For most organizations, the default configuration is acceptable, but you should check your organization's security policies to determine whether changes are required.

Using the SSL Cipher Configuration

The Operations Manager UNIX and Linux agent communicates with the Operations Manager management server by accepting requests on port 1270 and supplying information in response to

those requests. Requests are made by using the WS-Management protocol that is running on an SSL connection.

When the SSL connection is first established for each request, the standard SSL protocol negotiates the encryption algorithm, known as a cipher for the connection to use. For Operations Manager, the management server always negotiates to use a high strength cipher so that strong encryption is used on the network connection between the management server and the UNIX or Linux computer.

The default SSL cipher configuration on UNIX or Linux computer is governed by the SSL package that is installed as part of the operating system. The SSL cipher configuration typically allows connections with a variety of ciphers, including older ciphers of lower strength. While Operations Manager does not use these lower strength ciphers, having port 1270 open with the possibility of using a lower strength cipher contradicts the security policy of some organizations.

If the default SSL cipher configuration meets your organization's security policy, no action is needed.

If the default SSL cipher configuration contradicts your organization's security policy, the Operations Manager UNIX and Linux agent provides a configuration option to specify the ciphers that SSL can accept on port 1270. This option can be used to control the ciphers and bring the SSL configuration into conformance with your policies. After the Operations Manager UNIX and Linux agent is installed on each managed computer, the configuration option must be set by using the procedures described in the next section. Operations Manager does not provide any automatic or built-in way to apply these configurations; each organization must perform the configuration by using an external mechanism that works best for it.

Setting the sslCipherSuite Configuration Option for System Center 2012 R2

The SSL ciphers for port 1270 are controlled by setting the **sslciphersuite** option in the OMI configuration file, **omiserver.conf**. The **omiserver.conf** file is located in the directory /etc/opt/microsoft/scx/conf/.

The format for the sslciphersuite option in this file is:

```
sslciphersuite=<cipher spec>
```

where <cipher spec> specifies the ciphers that are allowed, disallowed, and the order in which allowed ciphers are chosen.

The format for <cipher spec> is the same as the format for the **sslCipherSuite** option in the Apache HTTP Server version 2.0. For detailed information, see SSLCipherSuite Directive in the Apache documentation. All information on this site is provided by the owner or the users of the website. Microsoft makes no warranties, express, implied or statutory, as to the information at this website.

After setting the **sslCipherSuite** configuration option, you must restart the UNIX and Linux agent for the change to take effect. To restart the UNIX and Linux agent, run the following command, which is located in the **/etc/opt/microsoft/scx/bin/tools** directory.

```
. setup.sh
```

```
scxadmin -restart
```

Setting the sslCipherSuite Configuration Option for System Center 2012 SP1 and System Center 2012

The SSL ciphers for port 1270 are controlled by setting the **sslCipherSuite** option by using the **scxcimconfig** command, which is installed as part of the Operations Manager UNIX and Linux agent in the **/etc/opt/microsoft/scx/bin/tools** directory. To view the full Help, at the command prompt, type the following command.

```
scxcimconfig --help
```

To set the **sslCipherSuite** configuration option, the following syntax shows a typical command.

```
scxcimconfig -s sslCipherSuite='<cipher spec>' -p
```

where `<cipher spec>` specifies the ciphers that are allowed, disallowed, and the order in which allowed ciphers are chosen.

The format for `<cipher spec>` is the same as the format for the **sslCipherSuite** option in the Apache HTTP Server version 2.0. For detailed information, see SSLCipherSuite Directive in the Apache documentation. All information on this site is provided by the owner or the users of the website. Microsoft makes no warranties, express, implied or statutory, as to the information at this website.

After setting the **sslCipherSuite** configuration option, you must restart the UNIX and Linux agent for the change to take effect. To restart the UNIX and Linux agent, run the following command, also located in the **/etc/opt/microsoft/scx/bin/tools** directory.

```
scxadmin -restart
```

See Also

How to Set Credentials for Accessing UNIX and Linux Computers

Accessing UNIX and Linux Computers in Operations Manager

How to Configure sudo Elevation and SSH Keys

Required Capabilities for UNIX and Linux Accounts

Credentials You Must Have to Access UNIX and Linux Computers

Administering and Configuring the UNIX/Linux Agent

This topic describes options to administer and configure the UNIX/Linux agent for System Center – Operations Manager.

Agent Directories

- The UNIX/Linux agent installs to the directory: `/opt/microsoft/scx/`
- The UNIX/Linux agent maintains log files in the directory: `/var/opt/microsoft/scx/log/`
- Agent configuration files, including certificates, are stored in the directory: `/etc/opt/microsoft/scx/`

Agent Administration Tools

In this section, tools to administer and configure the UNIX/Linux agent are described.

Running the Agent Administration Tools

The tools for configuring the UNIX/Linux Agent are located in the directory:

```
/opt/microsoft/scx/bin/tools
```

Prior to running the tools, the file `/opt/microsoft/scx/bin/tools/setup.sh` must be sourced. This can be done with the following command:

```
. /opt/microsoft/scx/bin/tools/setup.sh
```

Scxadmin

The **scxadmin** tool is used to control the state of the UNIX/Linux agent (start, stop, or restart) as well as control logging performed by the agent. The usage of the tool can be displayed with the following command: `scxadmin -?`

```
# /opt/microsoft/scx/bin/tools/scxadmin -?


Usage: scxadmin

Generic options (for all commands)

  [-quiet]      Set quiet mode (no output)


        General Options

scxadmin -version


        Service Management

scxadmin {-start|-stop|-restart|-status}  [all|cimom|provider]


        Providers Management

scxadmin -config-list {RunAs}
```

```
scxadmin -config-set {RunAs}
{CWD=<directory>|ChRootPath=<directory>|AllowRoot={true|false}}
scxadmin -config-reset {RunAs} [CWD|ChRootPath|AllowRoot]


        Log Configuration Management
scxadmin {-log-list|-log-rotate|-log-reset} [all|cimom|provider]
scxadmin -log-set [all|cimom|provider] {verbose|intermediate|errors}
scxadmin -log-set provider {{FILE:<path>|STDOUT}:<module-
id>={SUPPRESS|ERROR|WARNING|INFO|TRACE|HYSTERICAL}}
scxadmin {-log-reset|-log-remove} provider [{FILE:<path>|STDOUT}]
```

Examples

Restarting the agent:

```
cd /opt/microsoft/scx/bin/tools/
./scxadmin -restart
```

Increase all logging to the Intermediate level:

```
cd /opt/microsoft/scx/bin/tools/
./scxadmin –log-set all intermediate
```

scxsslconfig

The **scxsslconfig** tool is used to generate the certificate in `/etc/opt/Microsoft/scx/ssl/`. This tool is useful in correcting issues in which the fully-qualified domain name cannot be determined from the UNIX or Linux host itself, or the FQDN known to the UNIX/Linux host does not match the FQDN used by the Operations Manager server to reach the host.

Note

The generated certificate must be signed by Operations Manager in order to be used in WS-Management communication. Overwriting a previously signed certificate will require that the certificate be signed again.

Usage for the **scxsslconfig** tool can be displayed with the following command: `scxsslconfig -?`

```
# /opt/microsoft/scx/bin/tools/scxsslconfig -?
Usage: /opt/microsoft/scx/bin/tools/.scxsslconfig [-v] [-s days] [-e days] [-d domain] [-
h host] [-g targetpath]


-v              - toggle debug flag
```

```
-g targetpath  - generate certificates in targetpath

-s days        - days to offset valid start date with (0)

-e days        - days to offset valid end date with (3650)

-f             - force certificate to be generated even if one exists

-d domain      - domain name

-h host        - host name

-b bits        - number of key bits

-?             - this help message
```

Examples

Regenerate the certificate, forcing overwrite of an existing certificate, with verbose output:

```
cd /opt/microsoft/scx/bin/tools/

. setup.sh

/opt/microsoft/scx/bin/tools/scxsslconfig -f -v
```

Regenerate the certificate, forcing overwrite of an existing certificate, with a specified hostname and DNS domain name:

```
cd /opt/microsoft/scx/bin/tools/

. setup.sh

/opt/microsoft/scx/bin/tools/scxsslconfig -f –h myserver –d contoso.com
```

Additional Configuration Topics

SSL Ciphers

If required, the SSL cipher list used by the UNIX/Linux agent can be customized. For more information about this configuration, see the Configuring SSL Ciphers topic.

Universal Linux – Operating System Name/Version

The Universal Linux Agent, which supports Linux operating systems such as CentOS, Debian GNU/Linux, Oracle Linux, and Ubuntu Server, parses release files to determine the host's operating system name and version. If required, these properties can be customized. To customize the operating system properties presented to Operations Manager for a Universal Linux Agent host, use the following procedure:

Create the file `disablereleasefileupdates` in the directory: `/etc/opt/microsoft/scx/conf/`.

```
touch /etc/opt/microsoft/scx/conf/disablereleasefileupdates
```

If this file exists, the agent will not attempt to update the operating system properties that are returned to Operations Manager. This ensures that the customizations are preserved.

Edit the file `scx-release` in the directory: `/etc/opt/microsoft/scx/conf`. This file has the format:

```
OSName=CentOS

OSVersion=6.0

OSFullName=CentOS 6.0 (x86_64)

OSAlias=UniversalR

OSManufacturer=
```

The values of the **OSName**, **OSVersion**, and **OSFullName** properties can be edited to reflect customized values.

Note

The OSAlias property should not be edited. All properties in this file (except for OSManufacturer) are mandatory and should not be null.

See Also

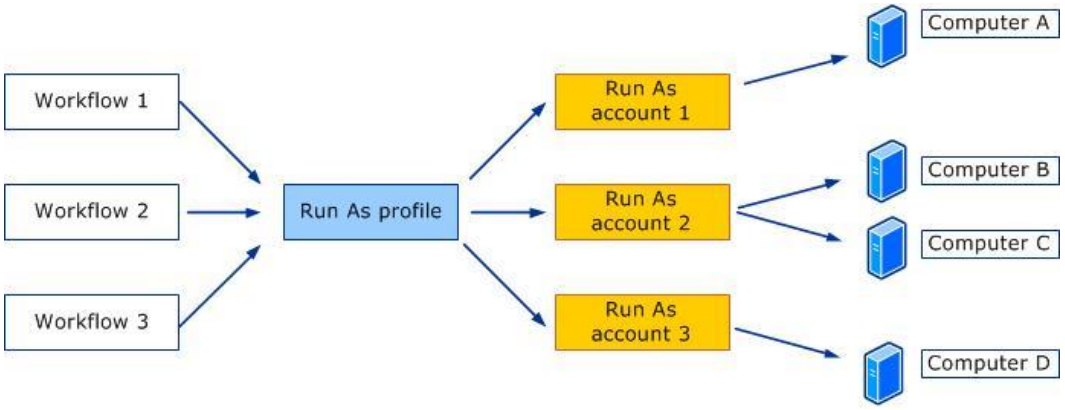
Managing Discovery and Agents

Accessing UNIX and Linux Computers in Operations Manager

Managing Run As Accounts and Profiles

System Center 2012 – Operations Manager workflows, such as rules, tasks, monitors, and discoveries, require credentials to run on a targeted agent or computer. By default, workflows use the default action account for the agent or computer. The credentials for the default action account are configured when Operations Manager is installed.

When a workflow requires rights and privileges that the default action account cannot provide, the workflow can be written to use a Run As profile. A Run As profile can have multiple Run As accounts associated with it. The Run As accounts allow you to specify the necessary credentials for specific computers. Multiple workflows can use the same Run As profile. The following image illustrates the relationship between workflows, Run As profiles, and Run As accounts.



In the image, three workflows use the same Run As profile. The Run As profile has three associated Run As accounts. In this example, each workflow that uses the Run As profile will run on Computer A using the credentials for Run As account 1, on Computer B and C using the credentials for Run As account 2, and on Computer D using the credentials for Run As account 3.

Run As profiles are defined in management packs by the management pack author. A Run As profile is used wherever its parent management pack is active. For example, the SQL Server 2005 management pack contains the SQL Run As profile, so the SQL Run As profile would be active on all servers running SQL Server 2005 that are monitored by the SQL Server 2005 management pack. The Run As profile is an association of one or more Run As accounts and the managed objects that the Run As accounts should be applied to.

In some cases, the Run As profile is imported into Operations Manager when the management pack that contains it is imported. In other cases, you may need to create it manually. In all cases, Run As profiles must be manually associated with a Run As account.

A Run As account contains a single set of credentials which are stored in the Operations Manager operational database. Each Run As account has a security classification (more secure or less secure) that controls how the credentials are distributed for use. If you elect more secure credential distribution, you must configure the mapping of which computers the credentials are distributed to.

Managing Run As Accounts and Profiles topics

- Distribution and Targeting for Run As Accounts and Profiles

  This topic explains the difference between distribution and targeting, the options for distributing Run As accounts, and the options for selecting targets for Run As profiles.
- How to Create a Run As Account

  This topic explains how to create a Run As account and how to modify an existing Run As account.
- How to Associate a Run As Account to a Run As Profile

  This topic explains how to configure a Run As profile to use a Run As account.
- How to Create a New Run As Account for Accessing the Operations Manager Database

  This topic explains how to create a Run As account that can access the operational database.
- How to Configure Run As Accounts and Profiles for UNIX and Linux Access

  This topic explains the Run As accounts you must create to monitor UNIX and Linux computers.

Other resources for Operations Manager

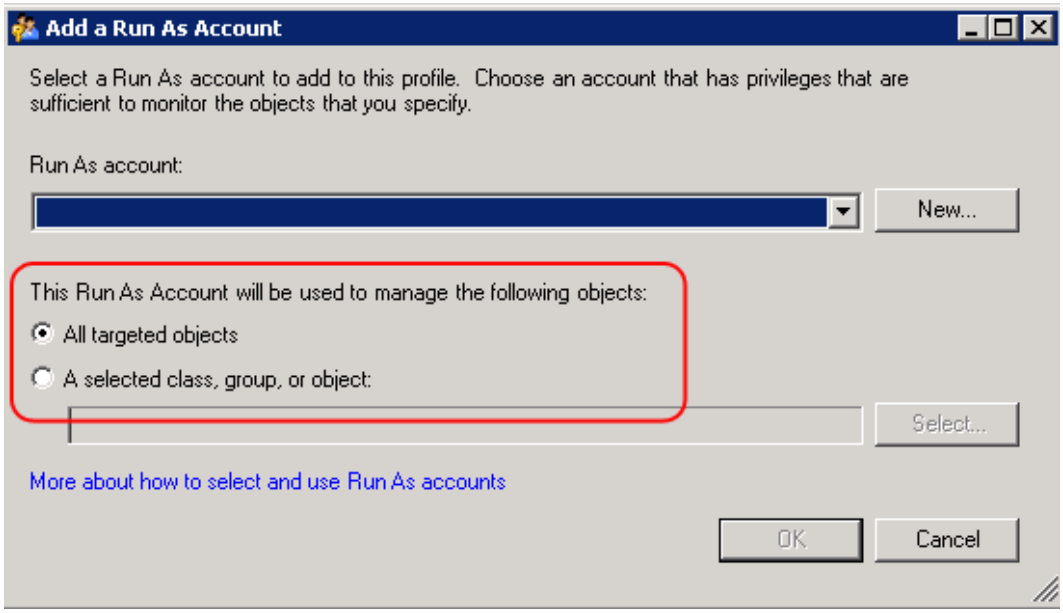
- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Managing Access in Operations Manager

- Run As Accounts for Network Monitoring in Operations Manager

Distribution and Targeting for Run As Accounts and Profiles

Run As accounts are associated with Run As profiles to provide the necessary credentials for workflows that use that Run As profile to run successfully. Both distribution and targeting of Run As accounts must be correctly configured for the Run As profile to work properly.

When you configure a Run As profile, you select the Run As accounts you want to associate with the Run As profile. When you create that association, you specify the class, group, or object that the Run As account will be used to manage, as shown in the following image. This establishes the target of the Run As account.



Distribution is an attribute of a Run As account in which you specify which computers will receive the Run As account credentials. You can choose to distribute the Run As account credentials to every agent-managed computer or only to selected computers.

Example of Run As account targeting and distribution:

Physical computer ABC hosts two instances of Microsoft SQL Server, instance X and instance Y. Each instance uses a different set of credentials for the **sa** account. You create a Run As account with the **sa** credentials for instance X, and a different Run As account with the **sa** credentials for instance Y. When you configure the SQL Server Run As profile, you associate both Run As account credentials for instance X and Y with the profile and specify that the Run As account instance X credentials are to be used for SQL Server instance X and that the Run As account Y credentials are to be used for SQL Server instance Y. Then, you configure both Run As accounts to be distributed to physical computer ABC.

Selecting a Target for a Run As Account

As shown in the previous image, your options for selecting a target for a Run As account are **All targeted objects** and **A selected class, group, or object**.

When you select **All targeted objects**, the Run As profile will use this Run As account for all objects for the workflows that use the Run As profile. …

When you select **A selected class, group, or object**, you can limit the use of the Run As account to the class, group, or object that you specify. …

Note
The Run As account credentials must be distributed to…

Comparing More Secure and Less Secure Distribution

Operations Manager distributes the Run As account credentials to either all agent-managed computers (the less secure option) or only to computers that you specify (the more secure option). If Operations Manager automatically distributed the Runs As account according to discovery a security risk would be introduced into your environment as illustrated in the following example. This is why an automatic distribution option was not included in Operations Manager.

For example, Operations Manager identifies a computer as hosting SQL Server 2005 based on the presence of a registry key. It is possible to create that same registry key on a computer that is not actually running an instance of SQL Server 2005. If Operations Manager were to automatically distribute the credentials to all agent managed computers that have been identified as SQL Server 2005 computers, then the credentials would be sent to the imposter SQL Server and they would be available to someone with administrator rights on that server.

When you create a Run As account, you are prompted to choose whether the Run As account should be treated in a **Less secure** or **More secure** fashion. More secure means that when you associate the Run As account with a Run As Profile, you have to provide the specific computer names that you want the Run As credentials distributed to. By positively identifying the destination computers, you can prevent the spoofing scenario that was described before. If you choose the less secure option, you will not have to provide any specific computers and the credentials will be distributed to all agent-managed computers.

Note
Operations Manager will perform tests to validate the Run As credentials, including whether the credentials can be used to log on locally to the computer. If the account does not have the right to log on locally, an alert will be generated.

See Also

Managing Run As Accounts and Profiles

How to Create a Run As Account

How to Associate a Run As Account to a Run As Profile
How to Create a New Run As Account for Accessing the Operations Manager Database
How to Configure Run As Accounts and Profiles for UNIX and Linux Access

How to Create a Run As Account

This procedure tells you how to create a Run As Account by using a set of Windows credentials as an example. Then it shows you how to edit the properties of the Run As Account to modify the security level and distribution of the credentials. You use this same procedure for all other account types.

The credentials that you provide in a Run As Account are used to run tasks, rules, monitors and discoveries as defined by the management pack that they are in. The management pack guide has the settings that you need for configuring the Run As Account and the Run As Profile.

When you create a Run As Account you are warned that you must associate the Run As Account with a Run As profile, and you are not presented with the option to configure Run As Account credential distribution. Both of these activities can be accomplished in the Run As Profile wizard. Alternately, you can configure Run As Account credential distribution by editing the properties of the Run As Account as shown next.

To create a Run As account

1. Log on to the Operations console with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. In the **Administration** workspace, right-click **Accounts**, and then click **Create Run As Account**.
4. In the **Create Run As Account Wizard**, on the **Introduction** page click **Next.**
5. On the **General Properties** page, do the following:
   a. Select **Windows** in the **Run As Account type:** list.
   b. Type a display name in the **Display Name** text box.
   c. Optionally, type a description in the **Description** box.
   d. Click **Next**.
6. On the **Credentials** page, type a user name, and its password, and then select the domain for the account that you want to make a member of this Run As account.
7. Click **Next**.
8. On the **Distribution Security** page, select the **Less secure** or **More secure** option as appropriate. For more information, see Distribution and Targeting for Run As Accounts and Profiles.
9. Click **Create**.
10. On the **Run As Account Creation Progress** page, click **Close**.

To modify Run As account properties

1. In the Operations console, click **Administration**.
2. In the **Administration** workspace, click **Accounts**.
3. In the results pane, double-click the Run As account that you want to edit to open its properties.
4. On the **Run As Account Properties** page, you can edit values on the **General Properties**, **Credentials**, or the **Distribution** tabs. In this case, select the **Distribution** tab.
5. On the **Distribution** tab, in the **Selected computers:** area, click **Add** to open the **Computer Search** tool.
6. On the **Computer Search** page, click the **Option:** list and select one of the following options:
   a. **Search by computer name (Default)**, then type in the computer name in the **Filter by: (Optional)** box.
   b. **Show suggested computers**, if you have already associated the Run As Account object with a Run As profile, a list of discovered computers that host the monitored service are presented here.
   c. **Show management servers**, in some cases, for example cross platform monitoring, all monitoring is performed by a management server and therefore the credentials have be distributed to the management servers that is performing the monitoring.
7. Optionally, type in a value in the **Filter by: (Optional)** box to narrow the search result set and click **Search**. A list of computers that match the search criteria is displayed in the **Available items** box.
8. Select the computers that you want to distribute the credentials to, and click **Add**. The computers appear in the **Selected Items** box.
9. Click **OK**. This returns you to the **Distribution** tab and the computers are displayed. Click **OK**.

See Also

Managing Run As Accounts and Profiles

Distribution and Targeting for Run As Accounts and Profiles

How to Associate a Run As Account to a Run As Profile

How to Create a New Run As Account for Accessing the Operations Manager Database

How to Configure Run As Accounts and Profiles for UNIX and Linux Access

How to Associate a Run As Account to a Run As Profile

In System Center 2012 – Operations Manager, Run As accounts are associated with Run As profiles to provide the necessary credentials for workflows that use that Run As profile to run successfully. Both distribution and targeting of Run As accounts must be correctly configured for the Run As profile to work properly.

1. Identify the class, group, or objects the Run As account will be applied to. For more information, see Distribution and Targeting for Run As Accounts and Profiles.
2. Create the Run As account. For more information, see How to Create a Run As Account.
3. Associate the Run As account with the Run As profile.
4. Configure the distribution of Run As account object credentials to specific computers.

This procedure can be used for creating and configuring a new Run As profile, or you can use the configuring section to modify or configure Run As profiles that are pre-existing in your management group. This procedure assumes that you have not previously created a Run As account.

To associate a Run As account to a Run As profile

1. Log on to the Operations console with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. In the **Administration** workspace, click **Profiles**.
4. In the results pane, double-click the Run As profile that you want to configure. The Run As Profile Wizard opens.
5. In the left pane, click **Run As Accounts**.
6. On the **Run As Accounts** page, click **Add**.
7. In the **Add a Run As Account** window, in the **Run As account** field, select an existing Run As account from the dropdown menu. You can also create an account by clicking **New** and following the steps in the How to Create a Run As Account topic.
8. Select **All targeted objects** or **A selected class, group, or object**. If you select **A selected class, group, or object**, click **Select**, and then locate and select the class, group, or object that you want the Run As account to be used for. For more information, see Distribution and Targeting for Run As Accounts and Profiles.
9. Click **OK** to close the **Add a Run As Account window**.
10. On the **Run As Accounts** page, click **Save**.
11. On the **Run As Profile Wizard Completion** page, if every account you associated is configured for **Less Secure distribution**, click **Close**. If you associated a Run As account that is configured for **More Secure distribution**, you will see the Run As account listed as a link. Click the link to configure credential distribution, using the following procedure.

To configure distribution of a Run As account

1. Open the properties for the Run As account using one of the following methods:
   - On the **Run As Profile Wizard Completion** page, click the account link.
   - In the Operations console, in the **Administration** workspace, under **Run As Configuration**, click **Accounts**, and then in the results pane, double-click the account you want to configure.
2. On the **Distribution** tab, click **Add** for the **Selected computers** box and do the following:
   a. Select **Search by computer name (Default)** or **Show suggested computers**, or **Show management servers**.
   b. Optionally type in a value in the **Filter by: (Optional)** box.
   c. Click **Search**. The result set is returned in the **Available items** box.
   d. Select the computers you want from the result set, and click **Add**. This adds the selected computers to the **Selected objects** box.
   e. Click **OK**.
3. Click **OK**.

See Also

Managing Run As Accounts and Profiles

How to Create a Run As Account

Distribution and Targeting for Run As Accounts and Profiles

How to Create a New Run As Account for Accessing the Operations Manager Database

How to Configure Run As Accounts and Profiles for UNIX and Linux Access

How to Create a New Run As Account for Accessing the Operations Manager Database

Use the following procedure to create a new Run As account that can access the operational database.

To create a new Run As account for accessing the Operations Manager database

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. In the **Administration** workspace, right-click **Run As Accounts**, and then click **Create Run As Account** .
4. In the **Create Run As Account Wizard**, on the **Introduction** page, click **Next**.

5. On the **General** page, do the following:
   a. Select **Windows** in the **Run As Account type** list.
   b. Type a display name in the **Display Name** text box.

      Note
      The display name you enter here becomes the Run As account you will add to a new Run As profile in the following procedure.

   c. You can also type a description in the **Description** text box.
   d. Click **Next**.
6. On the **Account** page, type a user name, password, and then select the domain for the account that you want to make a member of this Run As account, and then click **Create**.

To assign the new Run As account to the Operational Database Account Run As profile

1. In the **Administration** workspace, under **Run As Configuration**, click **Profiles**.
2. In the **Profiles** list, right-click **Operational Database Account**, and then click **Properties**.
3. On the **Introduction** and **General Properties** pages, click **Next**.
4. Under **Run As accounts**, click **Add**.
5. In the **Add a Run As Account** dialog box, click the **Run As Account** dropdown menu, click the Run As account you created in the previous procedure, and then click **OK**.
6. Click **Save**.

To grant SQL Server Login rights for the new account

1. On the Windows desktop, click **Start**, point to **Programs**, point to **Microsoft SQL Server 2008**, and then click **SQL Server Management Studio**.
2. In the **Connect to Server** dialog box, in the **Server Type** list, select **Database Engine**, in the **Server Name** list select the server and instance for your Operations Manager database (for example, computer\INSTANCE1), in **Authentication** list, select **Windows Authentication**, and then click **Connect**.
3. In the **Object Explorer** pane, expand **Security**, right-click **Logins**, and then select **New Login**.
4. In the **Login - New** dialog box, click **Windows authentication**, and then click **Search**.
5. In the **Select User or Group** dialog box, enter the user or group name that you used when you created the new Run As account, click **Check Names**, and then click **OK**.
6. In the **Login - New** dialog box, click **OK**.

To grant access to the Operations Manager database

1. On the Windows desktop, click **Start**, point to **Programs**, point to **Microsoft SQL Server 2008** , and then click **SQL Server Management Studio**.
2. In the **Connect to Server** dialog box, in the **Server Type** list, select **Database Engine**, in the **Server Name** list select the server and instance for your Operations Manager

database (for example, computer\INSTANCE1), in **Authentication** list, select **Windows Authentication**, and then click **Connect**.

3. In the **Object Explorer** pane, expand **Databases**, expand **Operations Manager**, expand **Security**, right-click **Users**, and then click **New User**.
4. In the **Database User - New** dialog box, type a name for this new user in the **User name** text box, and then click the ellipses (**…**) next to the **Login name** option.
5. In the **Select Login** dialog box, click **Browse**.
6. In the **Browse for Objects** dialog box, click the check box next to the new login, and then click **OK**.
7. In the **Database User - New** dialog box, in the **Database role membership** list, select **dbmodule_users**, and then click **OK**.

See Also

Managing Run As Accounts and Profiles

How to Create a Run As Account

Distribution and Targeting for Run As Accounts and Profiles

How to Associate a Run As Account to a Run As Profile

How to Configure Run As Accounts and Profiles for UNIX and Linux Access

How to Configure Run As Accounts and Profiles for UNIX and Linux Access

If you are the system administrator in charge of the monitoring of UNIX and Linux computers, you must create Run As accounts for agent maintenance operations, and for health and performance monitoring. These Run As accounts must then be associated with the Run As profiles defined in the UNIX and Linux management packs, so they can access the agents on UNIX and Linux computers. For an overview of the process, see Accessing UNIX and Linux Computers in Operations Manager.

Configuring Run As Accounts

The **UNIX/Linux Run As Accounts Wizard** creates Run As accounts that can be of two Run As account types:

- A monitoring account
- An agent maintenance account.

Use this wizard three or more times as needed so that you have the following Run As accounts:

- A monitoring Run As account for unprivileged monitoring.
- A monitoring Run As account for privileged monitoring.

- An agent maintenance Run As account for upgrading, uninstalling, and other agent maintenance operations.

To run this wizard, you must have the following credentials information:

- Username and password for unprivileged access to the UNIX or Linux computer.
- Secure Shell (SSH) credentials for root-level privileged access to the UNIX or Linux computer. This can be either a username and password, or a username and a key. A passphrase can be optionally provided with a key. If you prefer not to provide credentials for a privileged account, you can use unprivileged credentials and have the credentials on the UNIX or Linux computer elevated.
- Username and password for privileged access to the UNIX or Linux computer. If you prefer not to provide credentials for a privileged account, you can use unprivileged credentials and have the credentials on the UNIX or Linux computer elevated.

  You can choose between su or sudo elevation. If the account is to be elevated using 'su', you will need the 'su' password.

To create a Run As Account

1. In the Operations console, click **Administration**.
2. In **Run As Configuration**, click **UNIX/Linux Accounts**.
3. In the **Tasks** pane, click **Create Run As Account**.
4. On the **Account Type** page, choose a **Monitoring Account** or an **Agent Maintenance Account**.
5. On the **General Properties** page, provide a name and description for the account. The description is optional.
6. On the **Account Credentials** page, provide account credentials that can be used for the Run As account type that you selected.
7. On the **Distribution Security** page, select the **More Secure** or **Less Secure** option.
8. Click **Create**.

Repeat as needed until all the needed Run As accounts are created.

Configuring Run As Profiles

Now that you have created the Run As accounts, you must add each Run As account to the applicable profile. There are three profiles to configure:

- UNIX/Linux Action Account

  Add a monitoring Run As account that has unprivileged credentials, to this profile.
- UNIX/Linux Privileged Account

  Add a monitoring Run As account that has privileged credentials or credentials to be elevated, to this profile.
- UNIX/Linux Agent Maintenance Account

Add a monitoring Run As account that has privileged credentials or credentials to be elevated, to this profile.

Note
There is no need to run the **Create Run As Profile Wizard** unless you have authored a new management pack that requires it.

To add a Run As account to a profile

1. In the Operations console, click **Administration**.
2. In **Run As Configuration**, click **Profiles**.
3. In the list of profiles, right click and then select **Properties** on one of the following profiles:
   - UNIX/Linux Action Account
   - UNIX/Linux Privileged Account
   - UNIX/Linux Agent Maintenance Account
4. In the **Run As Profile** wizard, click **Next** until you get to the **Run As Accounts** page.
5. On the **Run As Accounts** page, click **Add** to add a Run As account that you created. Select the class, group, or object that will be accessed using the credentials in the Run As account.
6. Click **Save**.

Repeat as needed until all three profiles have been configured with one or more Run As accounts.

See Also

Managing Run As Accounts and Profiles

How to Create a Run As Account

Distribution and Targeting for Run As Accounts and Profiles

How to Create a New Run As Account for Accessing the Operations Manager Database

How to Associate a Run As Account to a Run As Profile

Operations Manager Monitoring Scenarios

Operations Manager Monitoring Scenarios topics

- Agentless Monitoring in Operations Manager
- Monitoring Across Untrusted Boundaries in Operations Manager
- Client Monitoring Using Agentless Exception Monitoring in Operations Manager
- Monitoring Clusters by Using Operations Manager

- Monitoring Networks by Using Operations Manager
- Monitoring Service Level Objectives by Using Operations Manager
- Monitoring .NET Applications
- Monitoring UNIX and Linux Computers by Using Operations Manager
- Collecting Security Events Using Audit Collection Services in Operations Manager
- Connecting Operations Manager With Other Management Systems
- Monitoring Operations Manager from a Second Management Group
- Integrating Active Directory and Operations Manager

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Initial Monitoring After Operations Manager Is Installed
- Managing Access in Operations Manager
- Getting Information from Operations Manager
- General Tasks in Operations Manager
- Maintenance of Operations Manager

Agentless Monitoring in Operations Manager

System Center 2012 – Operations Manager can gather performance and availability data on a computer that does not have an agent installed by using a proxy agent that is installed on another computer. Use agentless-monitoring of computers when it is not possible or desirable to install an agent on a computer.

An agentless-managed computer is a Windows-based computer that is discovered by using the Operations console. You assign an management server or agent-managed computer to provide remote (proxy) agent functionality for the computers.

Agentless-managed computers are managed as if there is an agent installed on them. Not all management packs work in agentless mode. For more information, see the documentation for the management packs you are running.

Important
Agentless management of a computer will not work if the agentless-managed computer and its proxy communicate through a firewall. A management server will not collect descriptions for events or publishers that are present on an agentless managed computer but are not present on the proxy agent.

For information about configuring an agent-managed computer as a proxy for agentless-managed computers, see How to Configure a Proxy for Agentless Monitoring.

Important

An agentless-managed computer places greater resource requirements on a management server than an agent-managed computer.

To change an agentless-managed computer to an agent-managed computer, do the following:

1. Delete the agentless-managed computer from the management group by right-clicking the computer in **Agentless Managed** in the **Administration** workspace and then clicking **Delete**.
2. Deploy the agent to the computer. For more information, see Managing Discovery and Agents.

Agentless Monitoring Compared to Agentless Exception Monitoring

Agentless monitoring provides monitoring of computers without agents by using a proxy agent and applying those management packs that support agentless monitoring. Agentless Exception Monitoring (AEM) redirects hardware, operating system, and application crash information to Operations Manager, which can aggregate, view, and report on error reports that are sent by the Windows Error Reporting service. For information on AEM, see Client Monitoring Using Agentless Exception Monitoring in Operations Manager.

You can monitor a computer without an agent by using either agentless monitoring, AEM, or both.

Agentless Monitoring in Operations Manager topics

- How to Configure a Computer for Agentless Management
- How to Configure a Proxy for Agentless Monitoring

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Initial Monitoring After Operations Manager Is Installed
- Managing Access in Operations Manager
- Getting Information from Operations Manager
- General Tasks in Operations Manager
- Maintenance of Operations Manager
- Operations Manager Report Authoring Guide
- Managing Discovery and Agents

See Also

How to Configure a Computer for Agentless Management

How to Configure a Proxy for Agentless Monitoring

How to Configure a Computer for Agentless Management

System Center 2012 – Operations Manager can gather performance and availability data on a computer that does not have an agent installed by using a proxy agent that is installed on another computer. Use agentless-monitoring of computers when it is not possible or desirable to install an agent on a computer.

An agentless-managed computer is a Windows-based computer that is discovered by using the Operations console. You assign an management server or agent-managed computer to provide remote (proxy) agent functionality for the computers.

Agentless-managed computers are managed as if there is an agent installed on them. Not all management packs work in agentless mode. For more information, see the documentation for the management packs you are running.

To configure Windows-based computers for agentless management

1. Log on to the Operations console with an account that is a member of the Operations Manager Administrators role for the management group.
2. Click **Administration**.
3. At the bottom of the navigation pane, click **Discovery Wizard**.
4. On the **Discovery Type** page, click **Windows computers**.
5. On the **Auto or Advanced?** page, do the following:
    a. Select either **Automatic computer discovery** or **Advanced discovery**. Automatic computer discovery scans for Windows-based computers in the domain. Advanced discovery allows you to specify criteria for the computers that the wizard will return, such as computer names starting with NY. If you select **Automatic computer discovery**, click **Next**, and then go to step 7. If you select **Advanced discovery**, continue with the following steps.
    b. In the **Computer and Device Classes** list, select **Servers and Clients**, **Servers Only**, or **Clients Only**.
    c. In the **Management Server** list, click the management server or gateway server to discover the computers.
    d. If you selected **Servers and Clients**, you can select the **Verify discovered computers can be contacted** check box. This is likely to increase the success rate of agent deployment, but discovery can take longer.

Note
If the Active Directory catalog does not contain the NetBIOS names for computers in a domain, select **Verify discovered computers can be contacted**. Otherwise, the **Browse, or Type In** option fails to find computers. This affects computers in the same domain as the management server, in another domain with a full trust relationship, and in untrusted domains by using a gateway server.

e. Click **Next**.

Note
The wizard can return approximately 4000 computers if **Verify discovered computers can be contacted** is selected, and it can return 10,000 computers if this option is not selected. Automatic computer discovery verifies that discovered computers can be contacted. A computer that is already managed by the management group is not returned.

6. On the **Discovery Method** page, you can locate the computers that you want to manage by either scanning or browsing Active Directory Domain Services or typing the computer names.

   If you want to scan, do the following:

   a. If it is not already selected, select **Scan Active Directory** and then click **Configure**.
   b. In the **Find Computers** dialog box, type the criteria that you want to use for discovering computers, and then click **OK**.
   c. In the **Domain** list, click the domain of the computers that you want to discover.

   If you want to browse Active Directory Domain Services or type the computer names, do the following:

   - Select **Browse for, or type-in computer names**, click **Browse**, specify the names of the computers that you want to manage, and then click **OK**.
   - In the **Browse for, or type-in computer names** box, type the computer names, separated by a semi-colon, comma, or a new line. You can use NetBIOS computer names or fully qualified domain names (FQDN).

7. Click **Next**, and on the **Administrator Account** page, do one of the following:

   - Select **Use selected Management Server Action Account** if it is not already selected.
   - Select **Other user account**, type the **User name** and **Password**, and then select the **Domain** from the list. If the user name is not a domain account, select **This is a local computer account, not a domain account**.

     Important
     The account must have administrative privileges on the targeted computers. If **This is a local computer account, not a domain account** is selected, the management server action account will be used to perform discovery.

8. Click **Discover** to display the **Discovery Progress** page. The time it takes discovery to finish depends on many factors, such as the criteria specified and the configuration of the environment.

   Note
   Computers that are already managed by the management group will not be returned by the wizard.

9. On the **Select Objects to Manage** page, do the following:
   a. Select the computers that you want to be agent-managed computers.
   b. In the **Management Mode** list, click **Agentless** and then click **Next**.
   c. Click **Change**, select the proxy agent that you want to use, click **OK**, and then click **Next**.
10. On the **Summary** page, do the following:
    a. Leave the **Agent installation directory** set to the default of **%ProgramFiles%\System Center Operations Manager** or type an installation path.

       Important
       If a different **Agent installation directory** is specified, the root of the path must exist on the targeted computer or the agent installation fails. Subdirectories, such as **\Agent**, are created if they do not exist.

    b. Leave **Agent Action Account** set to the default, **Local System**, or select **Other** and type the **User name**, **Password**, and **Domain**. The Agent Action Account is the default account that the agent will use to perform actions.
    c. Click **Finish**.
11. In the **Agent Management Task Status** dialog box, the **Status** for each selected computer changes from **Queued** to **Success**; the computers are ready to be managed.

    Note
    If the task fails for a computer, click the targeted computer. The reason for the failure is displayed in the **Task Output** text box.
12. Click **Close**. The computers will be listed in the **Administration** workspace in **Agentless Managed**.

See Also

Agentless Monitoring in Operations Manager

How to Configure a Proxy for Agentless Monitoring

How to Configure a Proxy for Agentless Monitoring

System Center 2012 – Operations Manager can monitor Microsoft Windows-based computers on which an agent is not installed by using an agent on another computer to act as a proxy. This is called agentless management.

Note

Not all management packs support agentless management, so make sure agentless management will serve your needs before using it. For example, the Active Directory and Microsoft Exchange Server 2003 management packs do not support agentless management.

When you set up agentless monitoring of a computer, you select a proxy for each agentless-managed computer. Being configured as a proxy agent allows an agent to submit data on behalf of another source. A management group can serve as a proxy, but this takes up system resources. A best practice is using an agent-managed computer as a proxy agent.

You might also configure a computer to act as a proxy to support specific features of a management pack. For example, the Active Directory Management Pack requires enabling domain controllers to act as proxy agents.

Note

If a proxy agent is removed from management, its agentless systems are no longer managed.

Both the agentless-managed system and its proxy need to have access to the managing server through any firewalls. For more information about interacting with firewalls, see (link to appropriate content in deployment).

To configure an agent-managed computer as a proxy for agentless-managed computers

1. In the **Administration** workspace, click **Agent Managed**, right-click the computer, and then click **Properties**.
2. In the **Agent Properties** dialog box, click the **Security** tab.
3. On the **Security** tab, select **Allow this agent to act as a proxy and discover managed objects on other computers**, and then click **OK**.

How to configure a management server as a proxy for agentless-managed computers

1. In the **Administration** workspace, click **Management Servers**, right-click the management server, and then click **Properties**.
2. In the **Management Server Properties** dialog box, click the **Security** tab.
3. On the **Security** tab, select **Allow this server to act as a proxy and discover managed objects on other computers,** and then click **OK**.

To change the proxy agent for agentless-managed computers

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the management group.
2. In the Operations console, click **Administration**.
3. Click **Agentless Managed**.
4. In the **Agentless Managed** pane, select the agentless-managed computers for which you want to change the proxy agent, right-click them, and then select **Change Proxy Agent**.
5. In the **Change Proxy Agent** dialog box, select the computer you want to be the new proxy agent, and then click **OK**.

See Also

Agentless Monitoring in Operations Manager

How to Configure a Computer for Agentless Management

Monitoring Across Untrusted Boundaries in Operations Manager

Monitoring Across Untrusted Boundaries topics

- About Gateway Servers in Operations Manager
- Determining the Health of Gateway Servers
- Using Multiple Gateway Servers
- How to Configure Agent Failover to Multiple Gateway Servers
- How to Configure a Gateway Server to Failover Between Multiple Management Servers
- Certificate Renewal for Gateway Servers and Management Servers

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Initial Monitoring After Operations Manager Is Installed
- Managing Access in Operations Manager
- Getting Information from Operations Manager
- General Tasks in Operations Manager
- Maintenance of Operations Manager

- Operations Manager Report Authoring Guide
- Managing Discovery and Agents

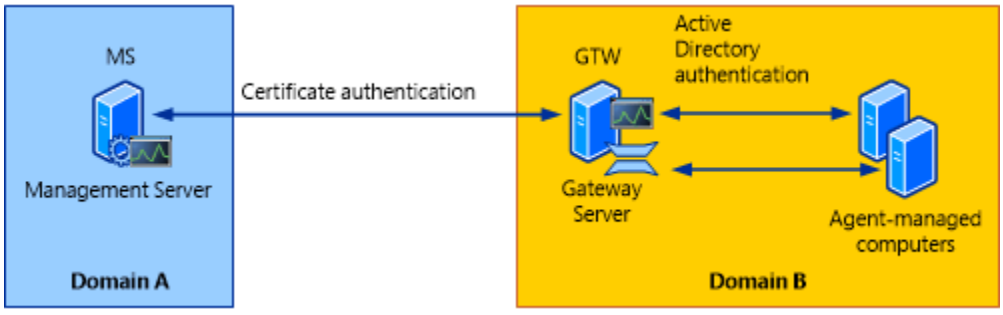
About Gateway Servers in Operations Manager

System Center 2012 – Operations Manager requires mutual authentication be performed between agents and management servers prior to the exchange of information between them. To secure the authentication process between the two, the process is encrypted. When the agent and the management server reside in the same Active Directory domain or in Active Directory domains that have established trust relationships, they make use of Kerberos V5 authentication mechanisms provided by Active Directory. When the agents and management servers do not lie within the same trust boundary, other mechanisms must be used to satisfy the secure mutual authentication requirement.

In Operations Manager, this is accomplished through the use of X.509 certificates issued for each computer. If there are many agent-monitored computers, this results in high administrative overhead for managing all those certificates. In addition, if there is a firewall between the agents and management servers, multiple authorized endpoints must be defined and maintained in the firewall rules to allow communication between them.

To reduce this administrative overhead, Operations Manager has a server role called the gateway server. Gateway servers are located within the trust boundary of the agents and can participate in the mandatory mutual authentication. Because they lie within the same trust boundary as the agents, the Kerberos V5 protocol for Active Directory is used between the agents and the gateway server. Each agent then communicates only with the gateway servers that it is aware of. The gateway servers communicate with the management servers.

To support the mandatory secure mutual authentication between the gateway servers and the management servers, certificates must be issued and installed, but only for the gateway and management servers. This reduces the number of certificates required, and in the case of an intervening firewall it also reduces the number of authorized endpoints to be defined in the firewall rules. The following illustration shows the authentication relationships in a management group using a gateway server.



For information about installing a gateway server, see Deploying a Gateway Server in the Deployment Guide.

See Also

Monitoring Across Untrusted Boundaries in Operations Manager

Determining the Health of Gateway Servers

Using Multiple Gateway Servers

How to Configure Agent Failover to Multiple Gateway Servers

How to Configure a Gateway Server to Failover Between Multiple Management Servers

Certificate Renewal for Gateway Servers and Management Servers

Determining the Health of Gateway Servers

To determine the health of a gateway server, you must examine it from two perspectives. The first, most direct method is to examine the health status in the Operations console and in Health Explorer. This examination will tell you the status of the monitored components, indicate whether or not there are any open alerts, and show you performance data. The second, indirect method is to be sure that data from the agents that are being monitored through the gateway server is being reported in a timely fashion.

Direct Method

Gateway servers are a type of management server, and therefore they are included in **Management Servers** under **Device Management** in the **Administration** workspace of the Operations console. In the details pane of this view, you can immediately see the **Health State** of any of management servers in the management group. By selecting any gateway server (or any server for that matter) and opening the context menu, you can view the properties of the server or any of the views that are available. Typically, you can directly access the **Event View**, **Alert View**, **Performance View**, **Diagram View**, and **State View** for the selected object.

For a more comprehensive understanding of the health of a gateway server, open the **Monitoring** view and navigate to the **Operations Manager**, **Management Server** folder and select the **Management Server State** view object in the navigation pane. This displays the state of all management servers in the management group, with gateway servers displayed next to the bottom by default. In the **Gateway Management Server State** pane, select the health status icon for the server you are interested in under the **Gateway** column to bring up the health state of the gateway servers component monitors in the details pane. Typically, you will get details on the **Health Service Availability**, **Audit Collection Availability**, **Configuration**, **Performance**, and **Security**.

Indirect Method

Gateway servers relay monitoring data from agents to collection management servers in the management group across trust boundaries. They also relay configuration information from the collection management server to the agents that they serve. Therefore, if agents that have a gateway server as their primary management server are reporting their data and are showing a heartbeat, you can be sure that their gateway server is performing satisfactorily.

Viewing Agents by Gateway

Use the following procedure to view the primary management server for an agent.

How to view an agent's primary management server

1. Open the Operations console, and then click **Administration**.
2. In the **Administration** workspace, click **Agent Managed**.
3. Displayed in the results pane are all the agent-managed devices grouped by their **Primary Management Server**.
4. Look for the gateway server of interest. Grouped under it are all the agents that are currently using the gateway server.

See Also

Monitoring Across Untrusted Boundaries in Operations Manager

About Gateway Servers in Operations Manager

How to Configure Agent Failover to Multiple Gateway Servers

How to Configure a Gateway Server to Failover Between Multiple Management Servers

Certificate Renewal for Gateway Servers and Management Servers

Using Multiple Gateway Servers

Multiple gateway servers can be deployed across a trust boundary to provide redundant pathways for agents that lie across that trust boundary. Just as agents can fail over between a primary management server and one or more secondary management servers, they can also fail over between gateway servers. In addition, multiple gateway servers can be used to distribute the workload of managing agentless-managed computers and managed network devices.

In addition to providing redundancy through agent-gateway failover, gateway servers can be configured to fail over between management servers in a management group if multiple management servers are available.

See Also

Monitoring Across Untrusted Boundaries in Operations Manager

About Gateway Servers in Operations Manager

Determining the Health of Gateway Servers

How to Configure Agent Failover to Multiple Gateway Servers

How to Configure a Gateway Server to Failover Between Multiple Management Servers

Certificate Renewal for Gateway Servers and Management Servers

How to Configure Agent Failover to Multiple Gateway Servers

If you have deployed multiple gateway servers in a domain that does not have a trust relationship established with the domain that the rest of the management group is in, you can configure agents to utilize those gateway servers as necessary. To do this, you must use the Operations Manager Shell to configure an agent to fail over to multiple gateway servers. The commands can be run from any command shell in the management group.

Important
When changing the primary management server of an agent, allow the agent to connect to its new primary management server before making changes to its failover server. Allowing the agent to get current topology information from the new primary management server prevents the agent from losing communication with all management servers.

To configure agent failover to multiple gateway servers

1. Log on to the computer with an account that is a member of the Administrators group.
2. Click **Start**, click **All Programs**, click **Microsoft System Center 2012**, click **Operations Manager**, and then click **Operations Manager Shell**.
3. In Operations Manager Shell, run the following command:

```
$primaryMS = Get-SCOMManagementServer –Name “<name of primary server>”
$failoverMS = Get-SCOMManagementServer –Name “<name of 1st failover>”,”<name of 2nd failover>”,…,”<name of nth failover>”
$agent = Get-SCOMAgent –Name “<name of agent>”

Set-SCOMParentManagementServer –Agent $agent –PrimaryServer $primaryMS
```

```
Set-SCOMParentManagementServer –Agent $agent –FailoverServer
$failoverMS
```

For help with the **Set-SCOMParentManagementServer** command, type the following in the command shell window:

```
Get-help Set-SCOMParentManagementServer -full
```

See Also

Monitoring Across Untrusted Boundaries in Operations Manager

About Gateway Servers in Operations Manager

Determining the Health of Gateway Servers

Using Multiple Gateway Servers

How to Configure a Gateway Server to Failover Between Multiple Management Servers

Certificate Renewal for Gateway Servers and Management Servers

How to Configure a Gateway Server to Failover Between Multiple Management Servers

Use the **Get-ManagementServer-GatewayManagementServer** cmdlet in the Operations Manager Shell as shown in the following example to configure a gateway server to fail over to multiple management servers. The commands can be run from any command shell in the management group.

To configure gateway server failover to multiple management servers

1. Log on to the gateway server with an account that is a member of the Administrators role for the management group.
2. Click **Start**, click **All Programs**, click **Microsoft System Center 2012**, click **Operations Manager**, and then click **Operations Manager Shell**.
3. In Operations Manager Shell, run the following command:

```
$primaryMS = Get-SCOMManagementServer –Name "<name of primary
server>"
$failoverMS = Get-SCOMManagementServer –Name "<name of 1st
failover>","<name of 2nd failover>",…,"<name of nth
failover>"
$gatewayMS = Get-SCOMGatewayManagementServer –Name "<name of
```

```
gateway>”

Set-SCOMParentManagementServer –Gateway $gatewayMS –
PrimaryServer $primaryMS
Set-SCOMParentManagementServer –Gateway $gatewayMS –
FailoverServer $failoverMS
```

For help with the **Set-SCOMParentManagementServer** command, type the following in the command shell window.

```
Get-help Set-SCOMParentManagementServer -full
```

See Also

Monitoring Across Untrusted Boundaries in Operations Manager

About Gateway Servers in Operations Manager

Using Multiple Gateway Servers

Determining the Health of Gateway Servers

How to Configure Agent Failover to Multiple Gateway Servers

Certificate Renewal for Gateway Servers and Management Servers

Certificate Renewal for Gateway Servers and Management Servers

Eventually, the certificates that were obtained and installed on the gateway server and collection management servers will expire and will need to be replaced with new ones. You might also need to replace an existing certificate if, for security reasons, the certificate has been revoked.

To do this, follow the procedures that were used to obtain and import the certificates in the first place. For more information, see Deploying a Gateway Server in the Deployment Guide. It is not necessary to rerun the Gateway Approval Tool.

See Also

Monitoring Across Untrusted Boundaries in Operations Manager

About Gateway Servers in Operations Manager

Determining the Health of Gateway Servers

Using Multiple Gateway Servers

How to Configure Agent Failover to Multiple Gateway Servers

[How to Configure a Gateway Server to Failover Between Multiple Management Servers]

Client Monitoring Using Agentless Exception Monitoring in Operations Manager

The Client Monitoring feature of System Center 2012 – Operations Manager enables you to monitor operating systems and applications for errors and participate in the Customer Experience Improvement Program (CEIP).

Agentless Exception Monitoring (AEM) is a component of the Client Monitoring feature in Operations Manager. AEM enables you to monitor operating systems and applications for errors within your organization. By default, when a Microsoft application encounters a severe error, it creates a report that can be sent to Microsoft to consolidate data that can lead to a reduction in errors. Using AEM, you can direct these reports to an Operations Manager management server. Operations Manager can then provide detailed views and reports on this consolidated error data. Using this data, you can determine how often an operating system or application experiences an error and the number of affected computers and users.

AEM Views

By default, the following views display AEM data in the Monitoring area of the Operations console:

Application View

A state view that lists applications that have failures.

Crash Listener View

A state view that lists the computers that are listening for failures that occur on other computers or applications.

Error Events

An event view that lists the application error reports generated by severe application or operating system failures.

Error Group View

A state view that lists application errors by error group.

System Error Group View

A state view that lists the computers that have an operating system failure.

Client Monitoring Using Agentless Exception Monitoring topics

- How to Configure a Management Server for Client Monitoring
- How to Configure Clients for Client Monitoring
- How to Customize Client Monitoring Data Collection and Solution Response URLs for Error Groups
- How to Configure Error Transmission Settings for Client Monitoring in Operations Manager
- Forwarding Client Error Reports (Client Monitoring)

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Initial Monitoring After Operations Manager Is Installed
- Managing Access in Operations Manager
- Getting Information from Operations Manager
- General Tasks in Operations Manager
- Maintenance of Operations Manager
- Operations Manager Report Authoring Guide
- Managing Discovery and Agents

How to Configure a Management Server for Client Monitoring

Use the following procedures to configure a management server for the server component of the Client Monitoring feature of System Center 2012 – Operations Manager.

Important
If you plan to configure the management server to forward error reports to Microsoft and receive links to available solutions for those errors or participate in the Customer Experience Improvement Program (CEIP), you must first configure the management server's proxy settings if it uses a proxy server to access the Internet.

The Operations Manager Client Monitoring Configuration Wizard is used to configure the server component of Client Monitoring on an Operations Manager management server. To configure the server component of Client Monitoring on multiple management servers, run the wizard once for each management server. An example of when you might configure multiple management

servers for Client Monitoring is if the connection between specific clients and management servers is less expensive.

Important
The management server and error reporting clients must be in the same or fully trusted domains.

To open the Client Monitoring Configuration Wizard

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. In the **Administration** workspace, click **Management Servers**.
4. In the **Management Servers** pane, right-click the management server on which you want to enable Client Monitoring, and then click **Configure Client Monitoring**. This will start the **Client Monitoring Configuration Wizard**. Use the same procedure to **Disable Client Monitoring** on the management server. You must also disable Client Monitoring on the clients.

   Note
   The **Configure Client Monitoring** option will be unavailable if the selected computer is a gateway server.

To configure Client Monitoring using the Client Monitoring Configuration Wizard

1. On the **Introduction** page of the **Client Monitoring Configuration Wizard**, click **Next**. The Introduction page is skipped if the wizard has run previously and the **Do not show this page again** check box was selected.
2. On the **Customer Experience Improvement Program** page, do one of the following:
   - Leave the default option of **No** if you do not want your organization to participate in the program, and then click **Next**.

   Or

   a. Select **Yes**, if you want your organization to participate in the program.
   b. Leave **Use Secure Socket Layer (SSL) protocol** selected if you have installed a certificate on your management server, leave **Use Windows Authentication** selected if you want the client computers to authenticate with the management server; otherwise, clear the options.
   c. Type the appropriate **Port**, or leave the default of 51907, and then click **Next**.
3. On the **Error Collection** page, do the following:
   a. Type the local or attached **File Share Path**, such as C:\ErrorData, for the management server that will be used to collect error reports. The file share will be created at the local path on the management server and shared with the necessary permissions.

      Important

The file share path must be on an NTFS partition and have at least 2 GB of free disk space. It is recommended that the path is no longer than 120 characters. The file share path can be a local drive path on the selected management server such as C:\ErrorData, or a UNC path to an existing network share such as \\Server\FileShare\ErrorData.

b. Select **Collect application errors from Windows Vista or later computers** if you are managing Windows Vista or later operating systems with Operations Manager. Type a **Port** number, or leave the default 51906. Leave **Use Secure Socket Layer protocol** selected if you have installed a certificate on your management server, leave **Use Windows Authentication** selected if you want the client computers to authenticate with the management server; otherwise, clear the options.

c. Type the **Organization Name**, using no more than 22 characters, and then click **Next**. The Organization Name can display on computers experiencing errors that are running Windows Server 2003 and earlier operating systems.

4. On the **Error Forwarding** page, do one of the following:

- Leave the **Automatically forward all collected errors to Microsoft** check box cleared, and then click **Next**.
- Or

a. Select **Automatically forward all collected errors to Microsoft** if the management server is connected to the Internet and you want to forward error reports to Microsoft and receive links to available solutions for those errors.

b. Select **Detailed** to help ensure Microsoft can provide a solution to the issue, or leave the default setting of **Basic**.

c. Click **Next**.

5. On the **Create File Share** page, do one of the following:

- Select an **Existing User Account** from the list, and then click **Next**.
- Select **Other user account**, type the **User name** and **Password**, select the **Domain** from the list, and then click **Next**.

Important

The account must have the permissions necessary to create a file share on the path provided in step 3a.

6. On the **Create file Share: Task Status** page, after the file share is successfully created, click **Next**.

Note

To modify the Client Monitoring settings on the management server, such as the file share, you must disable and then re-enable Client Monitoring on the management server. You must also then modify the Client Monitoring Group Policy settings on the clients.

7. On the **Client Configuration Settings** page, type or **Browse** to the location you want to save the settings from the Client Monitoring Configuration Wizard. These settings are saved in a Group Policy template file named *ServerName*.ADM. Click **Finish**.

Important
You must use the *ServerName*.ADM file to configure clients to redirect their Client Monitoring data to the management server. For more information, see How to Configure Clients for Client Monitoring.

See Also

Client Monitoring Using Agentless Exception Monitoring in Operations Manager

How to Configure Clients for Client Monitoring

How to Customize Client Monitoring Data Collection and Solution Response URLs for Error Groups

How to Configure Error Transmission Settings for Client Monitoring in Operations Manager

Forwarding Client Error Reports (Client Monitoring)

How to Configure Clients for Client Monitoring

This topic provides the procedure to configure clients for the Client Monitoring feature of System Center 2012 – Operations Manager.

Important
You must first configure a management server for the server component of Client Monitoring by running the Client Monitoring Configuration Wizard. For more information, see How to Configure a Management Server for Client Monitoring.

To configure clients for Client Monitoring in Operations Manager

1. Run the Group Policy Object Editor (gpedit.msc) for the domain or local computer.

   Note
   For information about Group Policy, see http://go.microsoft.com/fwlink/?LinkId=156845.

2. If needed, disable the **Turn off Windows Error Reporting** policy. This policy can be found in Computer Configuration/Administrative Templates/System/Internet Communication Management/Internet Communication settings.
3. Add the Agentless Exception Monitoring (AEM) Group Policy administrative template (*ServerName*.ADM) to the domain or local computer policy. The ADM file is created when the Client Monitoring Configuration Wizard is run.

   Note
   Use the same procedure to **Disable** the Group Policy settings, thereby disabling

Client Monitoring on the clients.

See Also

Client Monitoring Using Agentless Exception Monitoring in Operations Manager

How to Configure a Management Server for Client Monitoring

How to Customize Client Monitoring Data Collection and Solution Response URLs for Error Groups

How to Configure Error Transmission Settings for Client Monitoring in Operations Manager

Forwarding Client Error Reports (Client Monitoring)

How to Customize Client Monitoring Data Collection and Solution Response URLs for Error Groups

You can help decrease the time it takes to diagnose and resolve operating system and application errors in your organization by customizing the data that is collected in error reports by computers experiencing errors and the solution response URL for an error group. The solution response URL can point to an appropriate location in a knowledge base.

To customize client monitoring data collection and the solution response URL for an error group

1. Log on to the computer with an account that is a member of the Operations Manager Administrator role.
2. In the Operations console, click **Monitoring**.
3. In the **Monitoring** workspace, expand **Agentless Exception Monitoring**, and then click **Error Group View**.
4. In the **Error Group View**, select an entry.
5. In the **Tasks** pane, click **Show or Edit Error Group Properties**.
6. In the **Error Group Responses** dialog box, select **Custom Collection**, and then click **Edit**.
7. In the **Diagnostic Data Collection Configuration** dialog box, specify the **Files**, **WMI Queries**, and **Registry Keys** you want to collect from the computers experiencing the error, and then click **OK**. A computer will send the specified data in an error report to the management server on the next occurrence of an error in the error group.

   Note
   You can use variables, such as **%ProgramFiles%**, for file paths. For information about WMI, see http://go.microsoft.com/fwlink/?LinkId=71799.

8. In the **Error Group Responses** dialog box, select **Custom error information**, type the URL for the custom error information, such as **http://server/errors/100.htm**, click **Test Link**, and then click **OK**.

See Also

Client Monitoring Using Agentless Exception Monitoring in Operations Manager

How to Configure Clients for Client Monitoring

How to Configure a Management Server for Client Monitoring

How to Configure Error Transmission Settings for Client Monitoring in Operations Manager

Forwarding Client Error Reports (Client Monitoring)

How to Configure Error Transmission Settings for Client Monitoring in Operations Manager

When you enable Client Monitoring for a management group, you can configure it to forward error reports for Microsoft products to Microsoft. Error Transmission settings allow you to specify which error reports are sent to Microsoft and the additional diagnostic data that is included with the error reports.

Note
For information about enabling the Client Monitoring feature of System Center 2012 – Operations Manager, see How to Configure a Management Server for Client Monitoring.

To find the Error Transmission tab of the Global Management Server Settings - Privacy dialog box

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. In the **Administration** workspace, click **Settings**.
4. In the **Settings** pane, expand **Type: General**, right-click **Privacy**, and then click **Properties**.
5. In the **Global Management Server Group Settings - Privacy** dialog box, click the **Error Transmission** tab.

   Note
   Click **Read the privacy statement** to view the privacy statement.

To filter errors that are sent to Microsoft

1. On the **Error Transmission** tab of the **Global Management Server Group Settings - Privacy** dialog box, click **Filter**.
2. In the **Error Forwarding Filters** dialog box, select one or more of the options for sources of errors that you do not want forwarded to Microsoft, such as **that come from specific computers**.
3. In the **Criteria description** text box, click **specific**, and provide the values for the criteria of errors that you do not want forwarded to Microsoft, such as **contoso.com**.
4. Click **OK** twice.

To configure diagnostic data sent to Microsoft with error reports

1. On the **Error Transmission** tab of the **Global Management Server Settings - Privacy** dialog box, do one or more of the following:
   a. Select **Upload diagnostic data collection request,** select the additional diagnostic data that you want to send with error reports from computers reporting errors to the management servers, and then forward from the management server to Microsoft with the error reports.
   b. Set **Maximum number of CAB files to send to Microsoft per error group** to help Microsoft diagnose the error. Ten is the recommended number.
   c. Select **Display links to solutions from Microsoft on error reporting computers**. A link to available solutions will display to end users after the error is first encountered and the link to the solution is downloaded to the management server.
   d. Select **Display links to surveys from Microsoft on error reporting computers**.
   e. Specify the **Default solution link when no Microsoft solution is available**. This could be an internal Web page for technical support, for example.
2. Click **OK**.

See Also

Client Monitoring Using Agentless Exception Monitoring in Operations Manager

How to Configure Clients for Client Monitoring

How to Customize Client Monitoring Data Collection and Solution Response URLs for Error Groups

How to Configure a Management Server for Client Monitoring

Forwarding Client Error Reports (Client Monitoring)

Forwarding Client Error Reports (Client Monitoring)

The Microsoft Customer Experience Improvement Program (CEIP) collects information about how you use Microsoft programs and about some of the issues you might encounter. Microsoft uses this information to improve the products and features you use most often and to help solve issues. Participation in the program is strictly voluntary.

When you choose to participate in the CEIP, you configure clients with Group Policy to redirect CEIP reports to a System Center 2012 – Operations Manager management server, instead of reporting directly to Microsoft. The management servers are configured to forward these reports to Microsoft.

Important
The CEIP reports do not contain contact information about you or your organization, such as names or an address.

The CEIP reports forwarded from your organization to Microsoft are combined with CEIP reports from other organizations and individual customers to help Microsoft solve issues and improve the Microsoft products and features that customers use most often. For more information about the CEIP, see the CEIP page.

Use the following procedure to configure CEIP settings. The management server must have access to the Internet to participate in the program.

Important
CEIP is a component of the Client Monitoring feature of Operations Manager. Client Monitoring must be enabled on at least one management server and managed computers to participate in the CEIP. For information about enabling the Client Monitoring feature of Operations Manager, see Client Monitoring Using Agentless Exception Monitoring. After a management server has been configured for client monitoring, all agents that are participating in CEIP should be configured via Group Policy to send their CEIP data to that management server.

To configure the CEIP settings for Operations Manager

1. Log on to a management server with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click **Administration**.
3. In the **Administration** workspace, expand **Administration**, and then click **Settings**.
4. In **Settings**, expand **Type: General**, right-click **Privacy**, and then click **Properties**.
5. In the **Global Management Server Group Settings - Privacy** dialog box, on the **CEIP** tab, click **Join the Customer Experience Improvement Program (recommended)** to join the CEIP program or click **I don't want to join the program at this time** to decline participation. Then click **OK**.

Note
You can click **Tell me more about the program** to view information about the CEIP program, including the privacy statement.

See Also

Client Monitoring Using Agentless Exception Monitoring in Operations Manager

How to Configure Clients for Client Monitoring

How to Customize Client Monitoring Data Collection and Solution Response URLs for Error Groups

How to Configure Error Transmission Settings for Client Monitoring in Operations Manager

How to Configure a Management Server for Client Monitoring

Monitoring Clusters by Using Operations Manager

The purpose of this topic is to explain how to use System Center 2012 – Operations Manager to monitor computers that are in clustered configurations. For information on monitoring clustering services, see the guide for the management pack you are using, such as Windows Server 2003 Cluster Management Pack Guide or Windows Server Failover Cluster Management Pack Guide.

To begin monitoring computers in a cluster, perform the following steps:

1. Install an agent on all cluster nodes (computers).
2. Enable agent proxy on all cluster nodes. For more information, see How to Configure a Proxy for Agentless Monitoring.

In the **Administration** workspace, cluster nodes will be displayed in **Agent Managed**, and the cluster will be displayed in **Agentless Managed**. The cluster will show as “not monitored” unless a management pack contains monitors that specifically target the cluster object. The agent on the active cluster node will perform all monitoring. If the node fails, the agent on the cluster node that clustering fails over to will begin monitoring, but the agent on the failover node will have no awareness of anything the agent on other node had monitored previously, such as alerts, state changes, and so forth. The agents are independent.

When you are monitoring virtual servers on a cluster, you must deploy agents to the cluster nodes, configure them to be managed as a proxy, and then monitor the virtual servers as you would monitor an agentless-managed computer.

The Windows Server Operating System Management Pack provides discovery and monitoring of cluster shared volumes.

Note

You might see alerts from **Cluster discovery connect functionality monitor** and **Cluster state connect functionality monitor** when the Action Account uses low privilege credentials. To resolve this problem, assign higher privilege credentials to the Windows Cluster Action Account. For instructions, see the procedure “To modify Run As account properties” in How to Create a Run As Account.

See Also

Operations Manager Monitoring Scenarios

Integrating Active Directory and Operations Manager

Connecting Operations Manager With Other Management Systems

Collecting Security Events Using Audit Collection Services in Operations Manager

Monitoring UNIX and Linux Computers by Using Operations Manager

Monitoring .NET Applications

Monitoring Service Level Objectives by Using Operations Manager

Monitoring Networks by Using Operations Manager

Monitoring Operations Manager from a Second Management Group

Client Monitoring Using Agentless Exception Monitoring in Operations Manager

Monitoring Across Untrusted Boundaries in Operations Manager

Agentless Monitoring in Operations Manager

Monitoring Networks by Using Operations Manager

System Center 2012 – Operations Manager can monitor physical network routers and switches, including the interfaces and ports on those devices, and the virtual local area networks (VLANs) and Hot Standby Router Protocol (HSRP) groups that they participate in, as well as firewalls and load balancers. Increased visibility into your network infrastructure can help you identify failures in critical services and applications that were caused by the network. For example, you observe an alert informing you that a critical server is unavailable. If you have configured network monitoring, you would also observe an alert informing you that a port is offline. When you view the computer vicinity diagram for the server, you see that the unavailable computer is connected to the offline port. Thus, you can focus on troubleshooting the root cause for the unavailable computers.

Operations Manager can show you how your network is connected to the computers you are monitoring through the **Network Vicinity View** dashboard. Using Network Vicinity View, you can see how your topology is laid out, as well as the health of each network device, computer, and the connection between each.

Operations Manager can discover and monitor network devices that use the Simple Network Management Protocol (SNMP) v1, v2c, and v3. For a complete list of supported devices, see Network Devices Supported for Discovery by Operations Manager.

Network Device Monitoring Capabilities and Scope

Operations Manager provides the following monitoring for discovered network devices:

- Connection health - Based on looking at both ends of a connection
- VLAN health - Based on health state of switches in VLAN
- HSRP group health - Based on health state of individual HSRP end points
- Port/Interface
  - Up/down (operational & administrative status)
  - Volumes of inbound/outbound traffic (includes abort, broadcast, carrier sense, collision, CRC rates, discard, error, FCS error, frame, giants, runts, ignored, MAC transmit/receive error, queue rates)
  - % Utilization
  - Drop and broadcast rates

  Note
  Ports that are connected to a computer are not monitored; only ports that connect to other network devices are monitored. You can monitor a port that is connected to a computer that is not agent-managed in the same management group by adding the port to the Critical Network Adapters Group.
- Processor - % Utilization (for some certified devices)
- Memory - including high utilization, high buffer utilization, excessive fragmentation, and buffer allocation failures (for some certified devices)
  - In-depth memory counters (Cisco devices only)
  - Free memory

Note
Some of the monitoring capabilities are disabled by default. For more information, see Tuning Network Monitoring.

Operations Manager supports monitoring of the following number of network devices:

- 2000 network devices (approximately 25,000 monitored ports) managed by two resource pools
- 1000 network devices (approximately 12,500 monitored ports) managed by a resource pool that has three or more management servers
- 500 network devices (approximately 6,250 monitored ports) managed by a resource pool that has two or more gateway servers

Required Management Packs

Network discovery and monitoring requires the following management packs, which are installed with Operations Manager:

- Microsoft.Windows.Server.NetworkDiscovery
- Microsoft.Windows.Client.NetworkDiscovery

There are additional management packs that are required to relate network devices to each other and to the agent computers they are connected to. Network monitoring requires discovery of the network adapter for each agent computer, which is performed by the management pack for the agent computer's operating system. Verify that the management packs from the following list are installed for each of the operating systems in your environment.

- Windows Server 2003 Operating System
- Windows Server 2008 Operating System
- Windows 7 Client Operating Systems
- Windows Vista Client Operating Systems

How Network Device Discovery Works

Network device discovery is performed by discovery rules that you create. For instructions on creating a discovery rule, see How to Discover Network Devices in Operations Manager and Network Device Discovery Settings.

When you create a discovery rule, you designate a management server or gateway server to run the rule. Each management server or gateway server can run only one discovery rule. You may need to strategically place management servers on different network segments so that they can access the network devices that they are discovering.

Discovery rules run on a schedule that you can specify, and you can also run a rule on demand. Each time the discovery rule runs, it attempts to find new devices within its definition or changes to devices that were previously discovered. A discovery rule can perform *explicit discovery* or *recursive discovery*.

- *Explicit discovery* – An explicit discovery rule will only attempt to discover those devices that you explicitly specify in the wizard by IP address or FQDN. It will only monitor those devices that it can successfully access. The rule will attempt to access the device by using ICMP, SNMP, or both depending on the configuration of the rule.
- *Recursive discovery* – A recursive discovery rule will attempt to discover those devices that you explicitly specify in the wizard by IP address, as well as other network devices that are connected to the specified SNMP v1 or v2 device and that the specified SNMP v1 or v2 device knows about through the device's Address Routing Protocol (ARP) table, its IP address table, or the topology Management Information Block (MIB).

  If you use recursive discovery, you can elect to discover all the other network devices that the specified SNMP v1 or v2 device knows about or only network devices that are connected to the specified SNMP v1 or v2 device that are in a specified IP address range. You can also

filter recursive discovery by using such properties as the device type, name, and object identifier (OID).

Note
Operations Manager can identify connected devices in a recursive discovery that use an IPv6 address; however, the initial device that is discovered must use an IPv4 address.

A discovery rule can perform only explicit or recursive discovery, but cannot perform a combination of discovery types. You can change the discovery type of a rule after the rule is created. If you know all of the network devices that you want discovered, you should use explicit discovery. Recursive discovery can discover devices that you have no business need to monitor and as a result, can increase the administrative workload of monitoring your network.

A discovery rule can discover any combination of SNMP v1, v2, and v3 devices. SNMP v3 devices can only be discovered by explicit discovery or by being specified in a recursive discovery rule. If you specify an SNMP v3 device in a recursive discovery rule, the SNMP v3 device will be discovered but devices connected to it will not be discovered. If you specify an SNMP v1 or v2 device in a recursive discovery rule, only SNMP v1 and v2 devices connected to it will be included in the recursive discovery.

Note
Windows computers running SNMP are filtered out of discovery results if:

- The device type is “Host” and the vendor is “Microsoft”
- The sysDescription field contains “Microsoft”
- The sysOid starts with .1.3.6.1.4.1.311.1.1.3.1
- The sysOid contains 1.3.6.1.4.1.199.1.1.3.11

In the discovery rule configuration, you specify whether Operations Manager will use ICMP, SNMP, or both to communicate with the network device. The network device must support the protocol that you specify. When the discovery rule runs, Operations Manager attempts to contact the network devices that you specify, using the protocol or protocols that you specified. If you specify that a device uses both ICMP and SNMP, Operations Manager must be able to contact the device by using both methods or discovery will fail. If you specify ICMP as the only protocol to use, discovery is limited to the specified device and monitoring is limited to whether the device is online or offline.

Credentials are also needed to communicate with the device. You associate each discovery rule with Run As accounts that supply the community string (for SNMP v1 and v2 devices) or access credentials (SNMP v3) to Operations Manager. For more information, see Run As Accounts for Network Monitoring in Operations Manager.

After Operations Manager successfully accesses a specified network device, if you selected recursive discovery, it attempts to discover other network devices that the specified device knows about through the device’s ARP table, its IP address table, or the topology MIB files.

Network device discovery consists of the following phases, which are displayed in the status of the discovery task:

1. **Probing**

   During the probing phase, Operations Manager attempts to contact device using the specified protocol, as follows:

   - ICMP only: ping the device
   - ICMP and SNMP: contact the device using both protocols
   - SNMP only: uses the SNMP GET message

2. **Processing**

   After probing is complete, Operations Manager processes all of the components of the device, such as ports and interfaces, memory, processors, VLAN membership, and HSRP groups.

3. **Post Processing**

   Operations Manager correlates network device ports to the servers that the ports are connected to, inserts items into the operational database, and associates Run As accounts.

After discovery is complete, the management server resource pool that you specify in the discovery rule begins monitoring the discovered network devices. For more information on monitoring network devices, see Viewing Network Devices and Data in Operations Manager and Reports for Network Monitoring in Operations Manager.

See Also

How to Discover Network Devices in Operations Manager

Network Device Discovery Settings

Run As Accounts for Network Monitoring in Operations Manager

How to Delete or Restore a Network Device in Operations Manager

Viewing Network Devices and Data in Operations Manager

Security for Servers Performing Network Discovery

Network Devices Supported for Discovery by Operations Manager

Reports for Network Monitoring in Operations Manager

Tuning Network Monitoring

How to Discover Network Devices in Operations Manager

System Center 2012 – Operations Manager performs network discovery by running discovery rules that you create. Each time the rule runs, it will attempt to find new devices within its definition or changes to devices that were previously discovered.

Note

Discovery of a large number of devices can take several hours to complete.

Each management server or gateway server can run only one discovery rule. You specify a single management server or gateway server to run the discovery rule and a management server resource pool to perform the actual monitoring of the network devices. If you plan to monitor more than 1000 network devices, you should use two resource pools and split the number of devices evenly between the pools.

Note

If you create discovery rules on multiple management servers, you should create a management pool for each and make sure that each discovery defines a different set of devices. If a single device is managed in different pools, it will not be able to be deleted.

For more information on how network device discovery works, see How Network Device Discovery Works.

Prerequisites

To create a network devices discovery rule, you need the following information:

- The IP address or FQDN of each device that you want to discover and monitor.

  Note

  Operations Manager can identify connected devices in a recursive discovery that use an IPv6 address; however, the initial device that is discovered must use an IPv4 address.
- The version of SNMP that each devices uses. This can be SNMP v1, v2, or v3.
- The SNMP community string of each SNMP v1 or v2 device that you want to discover and monitor.
- The user name, context, authentication protocol, authentication key, privacy protocol, and privacy key for each SNMP v3 device that you want to discover and monitor.
- If you are using recursive discovery and you only want to discover network devices that have interfaces whose addresses fall within a specified IP address range, you must have the IP address range.
- The name of the management server resource pool that will monitor the discovered devices.

Note

When Network Load Balancing (NLB) is used, the destination MAC address for the network adapter (cluster adapter) uses the format of 02-BF-1-2-3-4 and the cluster hosts use a format of 02-h-1-2-3-4, where h is the host's priority within the cluster (set in the Network Load Balancing Properties dialog box). Operations Manager will create a network connection between the devices using 02-h-1-2-3-4 to the destination MAC address of 02-BF-1-2-3-4.

You must ensure the following firewall configuration before creating the network devices discovery rule:

- All firewalls between the management server and the network devices need to allow SNMP (UDP) and ICMP bi-directionally, and ports 161 and 162 need to be open bi-directionally. This includes Windows Firewall on the management server itself.
- If your network devices are using a port other than 161 and 162, you need to open bi-directional UDP traffic on these ports.

To create a network devices discovery rule

1. Open the Operations console with an account that is a member of Operations Manager Administrators.
2. In the **Administration** workspace, right-click **Administration**, and then click **Discovery Wizard**.
3. On the **What would you like to manage?** page, select **Network devices**, and then click **Next**.
4. On the **General Properties** page, do the following:
   a. In the Name box, type a name, such as **My Network Devices**.
   b. In the **Available servers** drop-down list, select a management server that has access to the devices you are discovering to run the discovery rule. Servers that already run a network devices discovery rule will not be listed.
   c. Click **Create Resource Pool** to create a management server resource pool for monitoring the devices, or in the **Select a resource pool** drop-down list, click a resource pool, and then click **Next**.
5. On the **Discovery Method** page, select **Explicit discovery** or **Recursive discovery**, and then click **Next**.

   Note
   If you know all of the network devices that you want discovered, you should use explicit discovery. Recursive discovery can discover devices that you have no business need to monitor and as a result, can increase the administrative workload of monitoring your network
6. On the **Default Accounts** page, if you are discovering only SNMP v3 devices, click **Next**. If you are discovering any SNMP v1 or v2 devices, do the following:
   a. If you previously created Run As accounts for SNMP v1 or v2 devices, the Run As accounts will be listed and you can select a listed account for this discovery rule. If no accounts are listed or the listed accounts are not appropriate for this discovery rule, continue to the next step.

      Note
      If you are creating a recursive discovery rule, you must create a default account, which will be used to connect to and discover devices connected to the device that you specify on the **Devices** page. If you do not create and select an account on the **Default Accounts** page, the recursive discovery will discover the device that you specify but will not discover devices connected to it.

b. Click **Create Account**.

c. In the **Create Run As Account Wizard**, on the **Introduction** page, click **Next**.

d. In the **Display Name** text box, type a name such as **Router Credentials**.

e. Optionally, type a description in the **Description** box. Click **Next**.

f. On the **Credentials** page, type the SNMP community string for your network devices, and then click **Create**.

Note

If the rule will discover devices that use more than one SNMP community string, you must create one Run As account for each SNMP community string.

g. On the **Default Accounts** page, you will see that the Run As account that you just created is listed in the **SNMPv1/v2 Run As accounts** box and is selected. Click **Next**

7. If you are adding an SNMP v1 or v2 device, on the **Devices** page, do the following:

Note

This procedure describes how to add devices one at a time. You can also add multiple devices by clicking the **Import** button to import a text file with a list of IPv4 addresses. This file should have a single IP address on each line. After import, the IP addresses are part of the discovery rule and the text file is no longer needed.

a. Click **Add** to open the **Add Device** page.

b. On the **Add Device** page, type the IPv4 address or FQDN of the device that you want to discover and monitor. If you are creating a recursive discovery, the discovery will access this device to locate other devices on your network.

c. In **Access Mode**, select **ICMP**, **SNMP**, or **ICMP and SNMP**. This specifies how the device will be discovered and how it will be monitored after discovery.

Note

If you select **ICMP and SNMP**, the device must be accessible by both protocols or it will not be discovered. If you select **ICMP**, discovery will be limited to the specified device, and monitoring will be limited to whether the device is online or offline.

d. In **Port number**, retain the default port (161) or select another port number for the device.

e. Select **v1 or v2** from the **SNMP version** drop-down box.

f. In **SNMP V1 or V2 Run As account**, select **Use selected default account**. If you specify an account in this window, then only the specified account will be used for discovery.

Note

If you are discovering devices that use more than one SNMP community string and therefore have multiple Run As accounts, you can retain the

default value of **Use selected default accounts** in the **SNMP V1 or V2 Run As account** field. When you do this, the Network Devices Discovery Wizard will attempt to use the community string for every Run As account that you selected on the **Default Accounts** page against every device that you add to the discovery list until a community string succeeds.

g. Click **OK**. This returns you to the **Devices** page and you should see the device that you just added listed.

Note

The **Advanced Discovery Settings** button on the **Devices** page opens a dialog box that contains a number of settings that you can use to configure discovery of network devices, such as number of retry attempts. If you know you are going to discover more than 1500 devices, you must change the **Maximum number of devices to discover** in **Advanced Discovery Settings**. For more information on the available settings, see Network Device Discovery Settings.

h. Add other SNMP v1 or v2 devices and Run As accounts as necessary, and then click **Next**.

Note

If you add multiple devices to the rule, you can set a common Run As Account for all of them by selecting all of the devices and then clicking **Edit**.

8. If you are adding an SNMP v3 device, on the **Devices** page, do the following:

Note

This procedure describes how to add devices one at a time. You can also add multiple devices by clicking the **Import** button to import a text file with a list of IPv4 addresses. This file should have a single IP address on each line. After import, the IP addresses are part of the discovery rule and the text file is no longer needed. Each device requires an SNMP v3 credential. After you import the addresses, you can edit each device to add the credential or you can select multiple devices and provide the same credential for all selected devices.

a. Click **Add**. This opens the **Add Device** page.

b. On the **Add a Device** page, type the IPv4 address or FQDN of the SNMP v3 device that you want to discovery and monitor.

c. In **Access Mode**, select **ICMP**, **SNMP**, or **ICMP and SNMP**. This specifies how the device will be discovered and how it will be monitored after discovery.

Note

If you select **ICMP and SNMP**, the device must be accessible by both protocols or it will not be discovered. If you select **ICMP**, discovery will be limited to the specified device, and monitoring will be limited to whether the device is online or offline.

d. In **Port number**, retain the default port (161) or select another port number for the

device.

e. Select **v3** from the **SNMP version** drop-down box.

f. Click **Add SNMP V3 Run As Account**.

Note
Each SNMP v3 device requires its own Run As account.

g. In the **Create Run As Account Wizard**, on the **Introduction** page, click **Next**.

h. Type a value in the **Display name** box, optionally type a description, and then click **Next**.

i. On the **Credentials** page, enter the values for **User name**, **Context**, **Authentication protocol**, **Authentication key**, **Privacy protocol** and **Privacy key** for the SNMP v3 device. Click **Create**.

j. Click **OK**. This returns you to the **Devices** page.

Note
The **Advanced Discovery Settings** button on the **Devices** page opens a dialog box that contains a number of settings that you can use to configure discovery of network devices, such as number of retry attempts. If you know you are going to discover more than 1500 devices, you must change the **Maximum number of devices to discover** in **Advanced Discovery Settings**. For more information on the available settings, see "Network Device Discovery Settings" in the Operations Manager 2012 Operations Guide.

k. Add other SNMP v3 devices and Run As accounts as necessary, and then click **Next**.

9. If you are creating an explicit discovery rule, go to the next step. If you are creating a recursive discovery rule, do the following:

a. On the **Include Filters** page, leave the default setting to discover all devices. If you want to filter for only a particular set of devices, select **Discover only network devices within the specific IP address ranges**, and then click **Add** to configure a filter. Click **Next** when complete.

In the **IP address range** field, you can enter addresses such as the following:

- **10.193.220.25** (a single IP address to include one specific device)
- **172.23.136<1-100>** (include any IP address from 1 to 100 in 172.23.136/255.255.255.0)
- **172.23.135.*** (include any IP address in 172.23.135/255.255.255.0)

Note
For more information on formatting an IP address range, see "Network Device Discovery Settings" in the Operations Manager 2012 Operations Guide.

b. On the **Exclude Filters** page, leave the default setting to not exclude any of the discovered devices. If you want to filter an IP address from being discovered, click

Add and specify an IP address. Click **Next** when complete.

Note
Although the dialog box states that an IP address or host name can be entered for an exclude filter, only an IP address is valid. A host name cannot be specified here.

10. On the **Schedule Discovery** page, either accept the default value of Saturday at 2 AM or specify an alternate schedule, and then click **Next**.

    Note
    We recommend that you do not run network discovery more frequently than twice per week because network discovery can take hours to complete and may place an excessive load on the management server or gateway server during discovery.

11. Review your settings on the **Summary** page, and then click **Finish** when you are ready to proceed.
12. You will see a Warning popup that reads "The following accounts need to be distributed to the health service *management server name* in order for the discovery to work: *DiscoveryName**Run As Account*. Would you like Operations Manager to distribute the accounts? Yes: Distribute the accounts and create the discovery. No: Do not distribute the accounts and do not create the discovery." Click **Yes**.
13. The wizard completes and you see the message **The network discovery rule was successfully created**. Ensure **Run the network discovery rule after the wizard is closed** is selected if you want the rule to run immediately, and then click **Close**. The network devices discovery rule is created. If you did not select **Run the network discovery rule after the wizard is closed**, the discovery rule will run on the scheduled day and time.

    Note
    It can take several minutes for the network discovery rule to appear in the Operations console and begin discovery if you select **Run the network discovery rule after the wizard is closed**.

14. To monitor the progress of network device discovery, watch the **status** column of the discovery rule. It will provide the following statuses while it is running, along with the number of devices that it has located:
    a. **Probing**

       During the probing phase, Operations Manager attempts to contact device using the specified protocol, as follows:

       - ICMP only: ping the device
       - ICMP and SNMP: contact the device using both protocols
       - SNMP only: uses the SNMP GET message

    b. **Processing**

       After probing is complete, Operations Manager processes all of the components of

the device, such as ports and interfaces, memory, processors, VLAN membership, and HSRP groups.

c. **Post Processing**

Operations Manager correlates network device ports to the servers that the ports are connected to, inserts items into the operational database, and associates Run As accounts.

15. To confirm the successful discovery and management of the devices, select **Device Management**, and then select **Network Devices**. You should see your discovered devices listed in the results pane.

If a network device discovery rule fails, the device or devices will be listed in **Network Devices Pending Management**. This can be a subset of the devices specified in the discovery rule. Use one of the following methods to retry the discovery:

- To attempt to discover that specific device only, right-click the device in **Network Devices Pending Management** and then click **Submit rediscovery**.
- To retry a recursive discovery that begins with that device, click **Discovery Rules**, right-click the respective rule, and then click **Run**.

To change the discovery type of a network devices discovery rule

1. In the Operations console, in the **Administration** workspace, click **Discovery Rules**.
2. In the results pane, right-click the discovery rule that you want to change and click **Properties**.
3. On the **General Properties** page, click **Next**.
4. On the **Discovery Method** page, click the type of discovery you want the rule to use.
5. Follow the instructions for creating a discovery rule to complete the remaining wizard pages, and then click **Save**.

See Also

Monitoring Networks by Using Operations Manager

Tuning Network Monitoring

Network Device Discovery Settings

Run As Accounts for Network Monitoring in Operations Manager

How to Delete or Restore a Network Device in Operations Manager

Viewing Network Devices and Data in Operations Manager

Security for Servers Performing Network Discovery

Network Devices Supported for Discovery by Operations Manager

Reports for Network Monitoring in Operations Manager

Network Device Discovery Settings

System Center 2012 – Operations Manager offers a number of settings that you can use to configure discovery of network devices. The following table explains the available settings and how to configure them in the Network Devices Discovery Wizard.

Setting	Location	Notes
Name or IP address	**Devices** page, **Add** button	Enter either a fully qualified domain name (FQDN) or an IPv4 address. Operations Manager can identify connected devices in a recursive discovery that use an IPv6 address; however, the initial device that is discovered must use an IPv4 address.
Access mode	**Devices** page, **Add** button	Select either **ICMP and SNMP**, **ICMP**, or **SNMP**. This specifies the protocol that will be used for both discovery and monitoring. If you select **ICMP and SNMP**, the device must be accessible by both protocols, or discovery will fail.
SNMP version	**Devices** page, **Add** button	Select either **v1 or v2** or **v3**. SNMP v1 and v2 devices can use the same Run As account. SNMP v3 devices require a different format Run As account.
Port number	**Devices** page, **Add** button	The default port is 161. You can change this value if you are discovering a network device that uses another port.
Run As account	**Devices** page, **Add** button	The available accounts in the menu are populated based on your selection in the **SNMP version** box. You can create the appropriate Run As account by clicking **Add SNMP** *version*

Setting	Location	Notes
		Run As Account.
Number of retry attempts	**Devices** page, **Advanced Discovery Settings** button	This setting specifies how many times the management server should attempt to contact the network device before reporting that discovery failed.
ICMP time-out (in milliseconds)	**Devices** page, **Advanced Discovery Settings** button	If you specify **ICMP and SNMP** or **ICMP** for **Access mode**, the management server attempts to contact the network device by using **ping**. The default setting is 1500 milliseconds (1.5 seconds).
SNMP time-out (in milliseconds)	**Devices** page, **Advanced Discovery Settings** button	If you specify **ICMP and SNMP** or **SNMP** for **Access mode**, the management server attempts to contact the network device by using SNMP. The default setting is 1500 milliseconds (1.5 seconds).
Maximum number of devices to discover	**Devices** page, **Advanced Discovery Settings** button	This setting applies during recursive discovery and sets a limit on the number of devices to discover. The default is 1500. If you know you are going to discovery more than 1500 devices, you must change this setting.
IP address range	**Include Filters** page, **Add** button, when configuring a recursive discovery rule	Use this field to limit the recursive discovery to IP addresses that meet the specified criteria. This field uses a wildcard format. For example, if you enter **192.168.1.***, the discovery rule discovers devices that use any IP address between 192.168.1.1 and 192.168.1.255.

Setting	Location	Notes
		If you enter **192.168.1.<1-140>**, the discovery rule discovers devices that use any IP address between 192.168.1 and 192.168.140. For more options, see **IP Address Range for Network Device Filtering**.
Included device types	**Include Filters** page, **Add** button, when configuring a recursive discovery rule	Any devices that you select are included in the recursive discovery. Clear the selection for any type of device that you do not want discovered.
Include only network devices with the following system attributes (OIDs) - Name	**Include Filters** page, **Add** button, when configuring a recursive discovery rule	If you enter a value here, only devices with a matching name are discovered. This field allows a wildcard format. For more options, see **IP Address Range for Network Device Filtering**.
Include only network devices with the following system attributes (OIDs) – Object ID (OID)	**Include Filters** page, **Add** button, when configuring a recursive discovery rule	If you enter a value here, only devices with a matching OID are discovered. This field allows a wildcard format. For more options, see **IP Address Range for Network Device Filtering**.
Include only network devices with the following system attributes (OIDs) – Description	**Include Filters** page, **Add** button, when configuring a recursive discovery rule	If you enter a value here, only devices with a matching description are discovered. This field allows a wildcard format. For more options, see **IP Address Range for Network Device Filtering**.
IP Address or Host Name	**Exclude Filters** page, **Add** button, when configuring a recursive discovery rule	Enter either a fully qualified domain name (FQDN), an IPv4 address, or an IPv6 address to exclude from discovery. You can add multiple IP address

Setting	Location	Notes
		individually.

Wildcard Matching for IP Address Range

Wildcard pattern matching is done from left to right, one character or basic wildcard pattern at a time. The pattern and the incoming string must match exactly, so for example, the pattern *abc* does not match the string *abcd*. Compound patterns consist of basic patterns separated by an ampersand (&) or a tilde (~). If the first character of a compound pattern is an ampersand or tilde, it is interpreted as if there were an asterisk at the beginning. For example, the pattern ~*[0-9] matches any string that does not contain a digit. A trailing ampersand can only match an empty string, and a trailing tilde indicates “except for an empty string.”

Spaces are significant characters, and are subject to matching.

The wildcard patterns consist of the following.

Character	Description	Example
?	Matches any single character	Example?.com matches Example1.com andExample2.com, but not Example01.com
*	Matches zero or more characters	Example*.com matches example.com, example1.com, and examplereallylong.com
[set]	Matches any single character in set, or if the first character ^, it matches any character not in set. A hyphen indicates a range. A caret (^) not in the first position, and a hyphen in the first or last position has no special meaning.	Ex[abc]mple matches Example, Exbmple, and Excmple. Ex[^abc]mple does not match Example, Exbmple, and Excmple, but does match ExZmple Ex[0-9] matches Ex followed by a single digit.
<n1-n2>	Matches any integer greater than or equal to the non-negative n1 and less than or equal to the non-negative n2. Omitting n1 or n2 indicates no bound	10.193.220.<1-25> matches all IP addresses between 10.193.220.1 and 10.193.220.25 inclusive. <10-> matches any string of digits greater than or equal to 10.

Character	Description	Example
		<1-10>* Matches any number between 1 and 10 with an option following character such as 1, 20x, 5z, but it does not match 11 since that is not a number between 1 and 10.
|	Alternative matches	AB|DC matches either AB or DC ABC| matches either ABC or an empty string
\	Escape character	
\\	Escape character for (,), [,], <, and >	\\(A\\) matches (A)
&	And also	*NY*ROUTER matches all strings containing NY and ROUTER <1-100>&*[02468] matches all even numbers between 1 and 100. *A*|*B*&*C* matches strings that contain either an A or a B, and also a C.
~	Except	10.20.30.*~10.20.30.50 matches all hosts on 10.20.30 except for 10.20.30.50. *Router*~*Cisco*&*10.20.30.<5-10> matches routers except Cisco routers with the addresses between 10.20.30.5 and 10.20.30.10.

Configuring a VLAN Tag

To differentiate between VLANs, you can configure a tag for a virtual local area network (VLAN) by editing the vlan-tag-settings.conf file on each management server that runs a network discovery rule. Vlan-tag-settings.conf is located in the Operations Manager installation directory in **\Server\NetworkMonitoring\conf\discovery**.

To configure a VLAN tag

1. On each management server that runs a network discovery rule, open vlan-tag-settings.conf in a text editor.
2. Add the following text to the file. You can use wildcard matching.

```
config name
match Type type
match Description text to match
settings VLAN_Provisioning_Setting
param Tag tag name
```

3. Save vlan-tag-settings.conf.

The following is an example of the configuration of a VLAN tag “LDSwitch” to be used for all switches that have a description that starts with “Cisco”:

```
config LanceSwitch
match Type SWITCH
match Description Cisco*
settings VLAN_Provisioning_Setting
param Tag LDSwitch
```

See Also

Monitoring Networks by Using Operations Manager

How to Discover Network Devices in Operations Manager

Tuning Network Monitoring

Run As Accounts for Network Monitoring in Operations Manager

How to Delete or Restore a Network Device in Operations Manager

Viewing Network Devices and Data in Operations Manager

Security for Servers Performing Network Discovery

Network Devices Supported for Discovery by Operations Manager

Reports for Network Monitoring in Operations Manager

Run As Accounts for Network Monitoring in Operations Manager

System Center 2012 – Operations Manager uses Run As accounts to discover and monitor network devices. The credentials in the Run As account enable management servers to communicate with the network devices. You can monitor devices that use SNMP v1, v2, and v3.

Network devices that use SNMP v1 or v2 require a Run As account that specifies a community string, which acts like a password to provide read-only access to the device.

Each network device that uses SNMP v3 requires a unique Run As account that provides the following credentials:

- User name: Obtained from device configuration.
- Context: Name that together with the user name determines the access permissions of a request sent to the SNMPv3 agent.
- Authentication protocol: MD5 for Message Digest 5, SHA for Secure Hash Algorithm, or NONE
- Authentication key: String consisting of 1 to 64 characters; required if the authentication protocol is MD5 or SHA
- Privacy protocol: DES for Data Encryption Standard, AES for Advanced Encryption Standard, or NONE
- Privacy key: String consisting of 1 to 64 characters; required if the privacy protocol is DES or AES

Note

The authentication key and privacy key are masked as you enter them.

You can create the required Run As accounts when you create a network devices discovery rule, or you can create the Run As accounts beforehand and then select the appropriate account when you create the discovery rule.

Two Run As profiles are created when you install Operations Manager: SNMP Monitoring Account and SNMPv3 Monitoring Account. When you create a discovery rule, the Run As accounts you create for network device discovery are automatically associated with the appropriate Run As profile.

See Also

Monitoring Networks by Using Operations Manager

How to Discover Network Devices in Operations Manager

Network Device Discovery Settings

Tuning Network Monitoring

How to Delete or Restore a Network Device in Operations Manager

Viewing Network Devices and Data in Operations Manager

Security for Servers Performing Network Discovery

Network Devices Supported for Discovery by Operations Manager

Reports for Network Monitoring in Operations Manager

How to Delete or Restore a Network Device in Operations Manager

After System Center 2012 – Operations Manager has discovered and is monitoring a network device, you might want to stop monitoring the device because it is being replaced or because there is no business value in monitoring that particular device or for any other reason. To stop monitoring a device, you can use maintenance mode or you can delete the network device from the discovery rule. You can also restore a deleted device that was discovered by a recursive discovery rule.

To delete a device that is the starting point for recursive discovery, you must first delete the discovery rule or remove the device from the discovery rule.

Note
You can identify the discovery rule associated with a discovered network device by right-clicking the device in **Network Devices** or **Network Devices Pending Management** and then clicking **Discovery Rule Properties**.

If you delete a device that was discovered by a recursive discovery rule, it will be added to the exclude list of the rule. If you want to have that device discovered and monitored again, you must remove the device from the **Exclude Filters** page of the rule's properties and run the discovery again.

To delete a network device discovered by explicit discovery

1. In the Operations console, select the **Administration** workspace.
2. Click **Network Devices**, right-click the device that you want to delete, and then click **Delete**.

   Note
   You can select multiple devices to delete.

To delete a network device specified in a recursive discovery rule

1. In the Operations console, select the **Administration** workspace.
2. Open **Properties** for the discovery rule and remove the device on the **Devices** page.

To delete a network device discovered by recursive discovery

1. In the Operations console, select the **Administration** workspace.
2. Click **Network Devices** in **Network Management**.
3. In the **Network Devices** pane, right-click a device that was discovered by recursive discovery, and then select **Delete**.
4. You will be prompted with a message asking you to confirm that you want to stop

monitoring the selected network device. Click **Yes**.

5. Click **Discovery Rules**.
6. Right-click the recursive discovery rule, and then select **Properties**.
7. Click **Exclude Filters**.
8. Verify that an exclude filter has been created for the deleted device. This may take a few minutes to occur.

To restore a network device that was deleted from recursive discovery

1. In the Operations console, select the **Administration** workspace.
2. Click **Discovery Rules**.
3. Right-click the recursive discovery rule, and then select **Properties**.
4. Click **Exclude Filters**.
5. Click the network device and then click **Remove**.
6. Click **Summary**, and then click **Save** to save and close the discovery rule.
7. With the discovery rule selected, click **Run** in the **Actions** pane to rerun the discovery rule.

   Note the status of the rule as it runs and wait until it shows a blank status.
8. Verify that the device is rediscovered. This may take a few minutes to a few hours depending on the number of devices in the environment. You can view the status of the discovery rule to determine when it has completed.

See Also

Monitoring Networks by Using Operations Manager

How to Discover Network Devices in Operations Manager

Network Device Discovery Settings

Run As Accounts for Network Monitoring in Operations Manager

Tuning Network Monitoring

Viewing Network Devices and Data in Operations Manager

Security for Servers Performing Network Discovery

Network Devices Supported for Discovery by Operations Manager

Reports for Network Monitoring in Operations Manager

Tuning Network Monitoring

System Center 2012 – Operations Manager includes the following management packs specific to network device discovery and monitoring:

- Network Management - Core Monitoring

This management pack contains monitoring logic for network devices.

- Windows Client Network Discovery

  This management pack contains discovery rules to set the properties of discovered network adapters connected to computers running client operating systems.
- Windows Server Network Discovery

  This management pack contains discovery rules to set the properties of discovered network adapters connected to computers running server operating systems.
- Network Discovery Internal

  This management pack contains definitions and rules for discovering network devices.
- Network Management Library

  This management pack contains definitions for core network device management.
- Network Management Reports

  This management pack contains reports for network management.
- Network Management Templates

  This management pack contains templates for authoring network management workflows.

Tuning Network Rules

The following rules are disabled by default. Using overrides, enable these rules only for the specific device types in your environment. To view these rules grouped by type, in the **Administration** workspace, scope **Management Pack Objects** to the network monitoring management packs listed in the previous section, and then click **Rules**.

Rule	Description	Types
Internal Network Management Discovery Trap Rediscovery	Internal rule to initiate rediscovery via trap requests	• Bridge • Call Server • Card (Multilayer Switch Feature) • Firewall • Host • Hub • Load Balancer • Media Gateway • Network Device • Node • Probe • Relay Device • Route Switch Feature Card

Rule	Description	Types
		• Route Switch Module • Router • Switch • Terminal Server
Output Packet Error Percentage	Collects the percentage of output packet errors	• Interface (if-mib dot3) • Interface (if-mib ethernet) • Interface (if-mib netcor) • Interface (if-mib router) • Interface (netcor cisco ethernet) • Interface (netcor if-mib cisco ethernet) • Interface (netcor if-mib cisco) • Interface (netcor if-mib MIB2) • Interface (netcor MIB2) • Interface (netcor router) • Network adapter (dot3) • Network adapter (if-mib cisco) • Network adapter (if-mib performance) • Network adapter (if-mib) • Network adapter (MIB2) • Network adapter (netcor cisco) • Network adapter (netcor ethernet) • Network adapter

Rule	Description	Types
		(netcor if-mib) • Network adapter (netcor performance) • Network adapter (netcor) • Port (MIB2 Dot3 ethernet) • Port (netcor if-mib dot3)
Input Broadcast Packets Percentage	Collects the percentage of input broadcast packets.	• Interface (if-mib dot3) • Interface (if-mib ethernet) • Interface (if-mib netcor) • Interface (if-mib router) • Interface (netcor cisco ethernet) • Interface (netcor if-mib cisco ethernet) • Interface (netcor if-mib cisco) • Interface (netcor if-mib MIB2) • Interface (netcor MIB2) • Interface (netcor router) • Network adapter (if-mib cisco) • Network adapter (if-mib performance) • Network adapter (if-mib) • Network adapter (netcor if-mib) • Network adapter (netcor

Rule	Description	Types
		performance) • Port (MIB2 Dot3 ethernet) • Port (netcor if-mib dot3)
Input Packet Error Percentage	Collects the percentage of input packet errors	• Interface (if-mib dot3) • Interface (if-mib ethernet) • Interface (if-mib netcor) • Interface (if-mib router) • Interface (netcor cisco ethernet) • Interface (netcor if-mib cisco ethernet) • Interface (netcor if-mib cisco) • Interface (netcor if-mib MIB2) • Interface (netcor MIB2) • Interface (netcor router) • Network adapter (dot3) • Network adapter (if-mib cisco) • Network adapter (if-mib performance) • Network adapter (if-mib) • Network adapter (MIB2) • Network adapter (netcor cisco) • Network adapter (netcor ethernet) • Network adapter

Rule	Description	Types
		(netcor if-mib) • Network adapter (netcor performance) • Network adapter (netcor) • Port (MIB2 Dot3 ethernet) • Port (netcor if-mib dot3)
Collision Percentage	Collects the rate of Ethernet packet collisions	• Interface (if-mib dot3) • Interface (if-mib ethernet) • Interface (netcor cisco ethernet) • Interface (netcor if-mib cisco ethernet) • Interface (netcor if-mib cisco ethernet) • Network adapter (dot3) • Network adapter (netcor ethernet) • Port (MIB2 Dot3 ethernet) • Port (netcor if-mib dot3)
Outbound Multicast Packets per Second	Collects outbound multicast packets per second	• Interface (if-mib dot3) • Interface (if-mib ethernet) • Interface (if-mib netcor) • Interface (if-mib router) • Network adapter (if-mib base) • Network adapter (if-mib cisco)

Rule	Description	Types
		• Network adapter (if-mib performance) • Network adapter (if-mib)
Inbound Unicast Packets per Second	Collects inbound unicast packets per second	• Interface (if-mib dot3) • Interface (if-mib ethernet) • Interface (if-mib netcor) • Interface (if-mib router) • Interface (netcor cisco ethernet) • Interface (netcor if-mib cisco ethernet) • Interface (netcor if-mib cisco) • Interface (netcor if-mib MIB2) • Interface (netcor MIB2) • Interface (netcor router) • Network adapter (dot3) • Network adapter (if-mib base) • Network adapter (if-mib cisco) • Network adapter (if-mib performance) • Network adapter (if-mib) • Network adapter (MIB2) • Network adapter (netcor base) • Network adapter (netcor cisco)

Rule	Description	Types
		• Network adapter (netcor ethernet) • Network adapter (netcor if-mib) • Network adapter (netcor performance) • Network adapter (netcor) • Port (MIB2 Dot3 ethernet) • Port (netcor if-mib dot3)
Outbound Broadcast Packets per Second	Collects outbound broadcast packets per second	• Interface (if-mib dot3) • Interface (if-mib ethernet) • Interface (if-mib netcor) • Interface (if-mib router) • Network adapter (if-mib base) • Network adapter (if-mib cisco) • Network adapter (if-mib performance) • Network adapter (if-mib)
Outbound Unicast Packets per Second	Collects outbound unicast packets per second	• Interface (if-mib dot3) • Interface (if-mib ethernet) • Interface (if-mib netcor) • Interface (if-mib router) • Interface (netcor cisco ethernet) • Interface (netcor if-

Rule	Description	Types
		mib cisco ethernet) • Interface (netcor if-mib cisco) • Interface (netcor if-mib MIB2) • Interface (netcor MIB2) • Interface (netcor router) • Network adapter (dot3) • Network adapter (if-mib base) • Network adapter (if-mib cisco) • Network adapter (if-mib performance) • Network adapter (if-mib) • Network adapter (MIB2) • Network adapter (netcor base) • Network adapter (netcor cisco) • Network adapter (netcor ethernet) • Network adapter (netcor if-mib) • Network adapter (netcor performance) • Network adapter (netcor) • Port (MIB2 Dot3 ethernet) • Port (netcor if-mib dot3)
Input Packet Discard Rate	Collects the percentage of discarded input packets	• Interface (if-mib dot3)

Rule	Description	Types
		• Interface (if-mib ethernet) • Interface (if-mib netcor) • Interface (if-mib router) • Interface (netcor cisco ethernet) • Interface (netcor if-mib cisco ethernet) • Interface (netcor if-mib cisco) • Interface (netcor if-mib MIB2) • Interface (netcor MIB2) • Interface (netcor router) • Network adapter (dot3) • Network adapter (if-mib base) • Network adapter (if-mib cisco) • Network adapter (if-mib performance) • Network adapter (if-mib) • Network adapter (MIB2) • Network adapter (netcor base) • Network adapter (netcor cisco) • Network adapter (netcor ethernet) • Network adapter (netcor if-mib) • Network adapter (netcor

Rule	Description	Types
		performance) • Network adapter (netcor) • Port (MIB2 Dot3 ethernet) • Port (netcor if-mib dot3)
Outbound Bits per Second	Collects outbound bits per second	• Interface (if-mib dot3) • Interface (if-mib ethernet) • Interface (if-mib netcor) • Interface (if-mib router) • Interface (netcor cisco ethernet) • Interface (netcor if-mib cisco ethernet) • Interface (netcor if-mib cisco) • Interface (netcor if-mib MIB2) • Interface (netcor MIB2) • Interface (netcor router) • Network adapter (dot3) • Network adapter (if-mib base) • Network adapter (if-mib cisco) • Network adapter (if-mib performance) • Network adapter (if-mib) • Network adapter (MIB2) • Network adapter

Rule	Description	Types
		(netcor base) • Network adapter (netcor cisco) • Network adapter (netcor ethernet) • Network adapter (netcor if-mib) • Network adapter (netcor performance) • Network adapter (netcor) • Port (MIB2 Dot3 ethernet) • Port (netcor if-mib dot3)
Inbound Broadcast Packets per Second	Collects inbound broadcast packets per second	• Interface (if-mib dot3) • Interface (if-mib ethernet) • Interface (if-mib netcor) • Interface (if-mib router) • Network adapter (if-mib base) • Network adapter (if-mib cisco) • Network adapter (if-mib performance) • Network adapter (if-mib)
Inbound Bits per Second	Collects inbound bits per second	• Interface (if-mib dot3) • Interface (if-mib ethernet) • Interface (netcor cisco ethernet) • Interface (netcor if-mib cisco ethernet)

Rule	Description	Types
		• Interface (if-mib netcor) • Interface (if-mib router) • Interface (netcor if-mib cisco) • Interface (netcor if-mib MIB2) • Interface (netcor MIB2) • Interface (netcor router) • Network adapter (dot3) • Network adapter (if-mib base) • Network adapter (if-mib cisco) • Network adapter (if-mib performance) • Network adapter (if-mib) • Network adapter (MIB2) • Network adapter (netcor base) • Network adapter (netcor cisco) • Network adapter (netcor ethernet) • Network adapter (netcor if-mib) • Network adapter (netcor performance) • Network adapter (netcor) • Port (MIB2 Dot3 ethernet) • Port (netcor if-mib

Rule	Description	Types
		dot3)
Inbound Multicast Packets per Second	Collects inbound multicast packets per second	• Interface (if-mib dot3) • Interface (if-mib ethernet) • Interface (if-mib netcor) • Interface (if-mib router) • Network adapter (if-mib base) • Network adapter (if-mib cisco) • Network adapter (if-mib performance) • Network adapter (if-mib)
Interface Utilization	Collects the utilization of the interface	• Interface (if-mib dot3) • Interface (if-mib ethernet) • Interface (if-mib netcor) • Interface (if-mib router) • Interface (netcor cisco ethernet) • Interface (netcor if-mib cisco ethernet) • Interface (netcor if-mib cisco) • Interface (netcor if-mib MIB2) • Interface (netcor MIB2) • Interface (netcor router) • Network adapter (dot3) • Network adapter (if-

Rule	Description	Types
		mib base) • Network adapter (if-mib cisco) • Network adapter (if-mib performance) • Network adapter (if-mib) • Network adapter (MIB2) • Network adapter (netcor base) • Network adapter (netcor cisco) • Network adapter (netcor ethernet) • Network adapter (netcor if-mib) • Network adapter (netcor performance) • Network adapter (netcor) • Port (MIB2 Dot3 ethernet) • Port (netcor if-mib dot3)
Output Packet Discard Rate	Collects the percentage of discarded output packets	• Interface (if-mib dot3) • Interface (if-mib ethernet) • Interface (if-mib netcor) • Interface (if-mib router) • Interface (netcor cisco ethernet) • Interface (netcor if-mib cisco ethernet) • Interface (netcor if-mib cisco)

Rule	Description	Types
		• Interface (netcor if-mib MIB2) • Interface (netcor MIB2) • Interface (netcor router) • Network adapter (dot3) • Network adapter (if-mib base) • Network adapter (if-mib cisco) • Network adapter (if-mib performance) • Network adapter (if-mib) • Network adapter (MIB2) • Network adapter (netcor base) • Network adapter (netcor cisco) • Network adapter (netcor ethernet) • Network adapter (netcor if-mib) • Network adapter (netcor performance) • Network adapter (netcor) • Port (MIB2 Dot3 ethernet) • Port (netcor if-mib dot3)
Inbound Queue Packets Dropped Per Second	Collects the number of packets dropped per second due to the input queue being full.	Interface (Cisco Router)
Inbound Giant Packets	Collects giant inbound packets per second.	Interface (Cisco Router)

Rule	Description	Types
per Second		
Inbound Packets with CRC Error per Second	Collects the number of inbound packets per second with CRC errors.	Interface (Cisco Router)
Inbound Packets Aborted per Second	Collects the number of inbound packets aborted per second.	Interface (Cisco Router)
Inbound Misaligned Packets per Second	Collects the number of inbound misaligned packets per second.	Interface (Cisco Router)
Output Queue Packets Dropped per Second	Collects the number of packets dropped per second due to the output queue being full.	Interface (Cisco Router)
Inbound Runts per Second	Collects the number of inbound packets smaller than permitted by the physical media.	Interface (Cisco Router)
Inbound Packets Ignored per Second	Collects inbound packets ignored per second.	Interface (Cisco Router)
Output Packet Queue Drop Percentage	Collects the number of output packets discarded because of output queue overflow.	• Interface (if-mib ethernet) • Interface (if-mib router) • Interface (netcor cisco ethernet) • Interface (netcor if-mib cisco ethernet) • Interface (netcor if-mib cisco) • Interface (netcor router) • Network adapter (if-mib cisco) • Network adapter (netcor cisco) • Network adapter (netcor ethernet)
Input Packet Queue Drop Percentage	Collects the number of input packets discarded because of input queue overflow.	• Interface (if-mib ethernet) • Interface (if-mib router)

Rule	Description	Types
		• Interface (netcor cisco ethernet) • Interface (netcor if-mib cisco ethernet) • Interface (netcor if-mib cisco) • Interface (netcor router) • Network adapter (if-mib cisco) • Network adapter (netcor cisco) • Network adapter (netcor ethernet)
Outbound Non-Unicast Packets per Second	Collects outbound non-unicast packets per second.	• Interface (netcor cisco ethernet) • Interface (netcor if-mib cisco ethernet) • Interface (netcor if-mib cisco) • Interface (netcor if-mib MIB2) • Interface (netcor MIB2) • Interface (netcor router) • Network adapter (dot3) • Network adapter (MIB2) • Network adapter (netcor base) • Network adapter (netcor cisco) • Network adapter (netcor ethernet) • Network adapter (netcor if-mib) • Network adapter (netcor

Rule	Description	Types
		performance) • Network adapter (netcor) • Port (MIB2 Dot3 ethernet) • Port (netcor if-mib dot3)
Inbound Non-Unicast Packets per Second	Collects inbound non-unicast packets per second.	• Interface (netcor cisco ethernet) • Interface (netcor if-mib cisco ethernet) • Interface (netcor if-mib cisco) • Interface (netcor if-mib MIB2) • Interface (netcor MIB2) • Interface (netcor router) • Network adapter (dot3) • Network adapter (MIB2) • Network adapter (netcor base) • Network adapter (netcor cisco) • Network adapter (netcor ethernet) • Network adapter (netcor if-mib) • Network adapter (netcor performance) • Network adapter (netcor) • Port (MIB2 Dot3 ethernet) • Port (netcor if-mib dot3)

Rule	Description	Types
Port Alignment Errors Rate	Determines the change in the SNMP dot3StatsAlignmentErrorsRate value for the dot3_Ethernet_Performance_Port since the last polling.	Port (Dot3 ethernet)
Port Carrier Sense Errors Rate	Determines the change in the SNMP dot3StatsCarrierSenseErrorsRate value for the dot3_Ethernet_Performance_Port since the last polling.	Port (Dot3 ethernet)
Port FCS Errors Rate	Determines the change in the SNMP dot3StatsFCSErrorsRate value for the dot3_Ethernet_Performance_Port since the last polling.	Port (Dot3 ethernet)
Port Frame Too Longs Rate	Determines the change in the SNMP dot3StatsFrameTooLongsRate value for the dot3_Ethernet_Performance_Port since the last polling.	Port (Dot3 ethernet)
Port Internal Mac Receive Errors Rate	Determines the change in the SNMP dot3StatsInternalMacReceiveErrorsRate value for the dot3_Ethernet_Performance_Port since the last polling.	Port (Dot3 ethernet)
Port Internal Mac Transmit Errors Rate	Determines the change in the SNMP dot3StatsInternalMacTransmitErrorsRate value for the dot3_Ethernet_Performance_Port since the last polling.	Port (Dot3 ethernet)

Tuning Alerts for Network Monitoring

The following monitors that generate alerts are disabled by default. Using overrides, enable these monitors if you want to receive alerts for the issue.

Monitor	Description	Targets
Interface Is Flapping	Monitors whether the interface link is switching frequently between up and down based on SNMP traps received.	• BPX Port (Cisco) • Interface • Network Adapter • Port

Monitor	Description	Targets
		• Token Ring Port • VR Interface
Interface Status	Aggregate monitor that rolls up interface health states for Operational Status and Administrative Status monitors.	• BPX Port (Cisco) • Interface • Network Adapter • Port • Token Ring Port • VR Interface
High Discard Percentage	Aggregate monitor that rolls up discard percentage health monitors.	• BPX Port (Cisco) • Interface • Network Adapter • Port • Token Ring Port • VR Interface
High Error Percentage	Aggregate monitor that rolls up error percentage health monitors.	• BPX Port (Cisco) • Interface • Network Adapter • Port • Token Ring Port • VR Interface
High Queue Drop Percentage	Aggregate monitor that rolls up queue drop percentage health monitors	• BPX Port (Cisco) • Interface • Network Adapter • Port • Token Ring Port • VR Interface
ICMP (Ping) Monitor	Monitors the response of network devices to ping.	ICMP IP
ICMPv6 (Ping) Monitor	Monitors the response of network devices to an IPv6 ping.	ICMPv6 IPv6
Collision Rate (Dot3 Ethernet)	Monitors the packet collision rate on this device	• Interface • Network Adapter
High Input Broadcast Rate (if MIB Dot3 Ethernet Port)	Monitors the level of input broadcast packets on this	• Interface • Network Adapter

Monitor	Description	Targets
	device	

See Also

Monitoring Networks by Using Operations Manager

How to Discover Network Devices in Operations Manager

Network Device Discovery Settings

Run As Accounts for Network Monitoring in Operations Manager

How to Delete or Restore a Network Device in Operations Manager

Viewing Network Devices and Data in Operations Manager

Security for Servers Performing Network Discovery

Network Devices Supported for Discovery by Operations Manager

Reports for Network Monitoring in Operations Manager

Viewing Network Devices and Data in Operations Manager

After System Center 2012 – Operations Manager discovers your network devices, you can view information about the devices using the following procedures.

Important
You must open the Operations console as an Operations Manager administrator to view the dashboard views.

This topic describes the following views:

- Network Summary Dashboard View
- Network Node Dashboard View
- Network Interface Dashboard View
- Network Vicinity Dashboard

Network Summary Dashboard View

The Network Summary Dashboard view provides a view of important data for the nodes and interfaces of the network. A node can be any device connected to a network. Nodes can be switches, routers, firewalls, load balancers, or any other networked device. An interface is a physical entity with which network connections are made, such as a port.

Use the Network Summary Dashboard view to view the following information:

- Nodes with Slowest Response (ICMP ping)
- Nodes with Highest CPU Usage
- Interfaces with Highest Utilization
- Interfaces with Most Send Errors
- Interfaces with Most Receive Errors
- Nodes with the Most Alerts
- Interfaces with the Most Alerts

You can select a particular node or interface name in the Network Summary Dashboard view and then select related tasks in the **Tasks** pane, such as starting the Network Node Dashboard view and the Network Interface Dashboard view.

To open the Network Summary Dashboard view

1. Open the Operations console, and then select the **Monitoring** workspace.
2. Expand **Network Monitoring**.
3. Click **Network Summary Dashboard**.

Network Node Dashboard View

A node can be any device connected to a network. Nodes can be switches, routers, firewalls, load balancers, or any other networked device. Use the Network Node Dashboard view to view the following information:

- Vicinity view of the node
- Availability statistics of the node over the last 24 hours, last 48 hours, past 7 days, or past 30 days

  Note
  Periods of time that were not monitored are counted as available in the availability statistics.
- Node properties
- Average response time of the node
- Processor usage of the node over the last 24 hours
- Current health of interfaces on the node
- Alerts generated by this node
- Alert details

To open the Network Node Dashboard view

1. Open the Operations console, and then select the **Monitoring** workspace.
2. Expand **Network Monitoring**.
3. Click the view for the desired node, such as **Switches**.

4. Select a node.
5. In the **Tasks** pane, select **Network Node Dashboard**.

Network Interface Dashboard View

An interface is a physical entity with which network connections are made, such as a port. By default, Operations Manager will only monitor ports that are connected to another device that is being monitored. Ports that are not connected will not be monitored. Use the Network Interface Dashboard view to view the following information:

- Bytes sent and received over the past 24 hours
- Packets sent and received over the past 24 hours
- Interface properties
- Send and receive errors and discards over the past 24 hours
- Network interface usage percentage
- Alerts generated by this interface
- Alert details

To open the Network Interface Dashboard view

1. Open the Operations console, and then select the **Monitoring** workspace.
2. Expand **Network Monitoring**.
3. Click the view for the desired node, such as **Switches**.
4. Select a node.
5. In the **Tasks** pane, select **Network Node Dashboard**.
6. In the **Health of Interfaces on this Node** section, click an interface, and then in the **Tasks** pane, select **Network Interface Dashboard**.

Network Vicinity Dashboard

Use the Network Vicinity Dashboard to view a diagram of a node and all nodes and agent computers that are connected to that node. The Network Vicinity Dashboard view displays one “hop”, or level of connection. However, you can configure the view to display up to five levels of connection. The diagram displays the health of the nodes and the health of the connections between nodes.

The vicinity view shows the relation between network devices and the Windows computers and other network devices that are connected to them. This logic is performed by relating the network adapter on the agent computer with the network device that it is connected to. Because of this, the network adapter must be discovered before this association can occur. You can view the discovered network adapters by either creating a new view or using the **Discovered Inventory** view to list instances of the **Computer Network Adapter** class.

Note

Because devices that use OSI layer 1, such as hubs, do not have MAC addresses, layer 1 devices will not be connected to computers in the Network Vicinity Dashboard. The vicinity view will only show connections between layer 1 devices and layer 2 or 3 devices.

Note
Network adapters using NIC teaming will not be identified as “teamed” in the Network Vicinity Dashboard.

Note
Virtual machines are associated with the same network device as their host. This version of Operations Manager does not show a relationship between the two computers.

Note
Operations Manager does not display UNIX- and Linux-based devices in the Network Vicinity Dashboard.

To open Network Vicinity View

1. Open Operations console, and then select the **Monitoring** workspace.
2. Expand **Network Monitoring**.
3. Click a node state view, such as **Network Devices**.
4. In the **Tasks** pane, click **Vicinity Dashboard**.

Things to try in the vicinity view:

- Select a node or connection to view details for that node or connection in the **Details** view.
- Change the levels of connection to be displayed in the diagram by selecting a new value for **Hops** in the toolbar.
- To include agent computers in the view in addition to network devices, select the **Show Computers** check box.
- Select a node in the vicinity view. In the **Tasks** pane, click the option to launch the Network Node dashboard.
- To change the central device of the view, select a device, and then click **Vicinity View**.

See Also

Monitoring Networks by Using Operations Manager

How to Discover Network Devices in Operations Manager

Network Device Discovery Settings

Run As Accounts for Network Monitoring in Operations Manager

How to Delete or Restore a Network Device in Operations Manager

Tuning Network Monitoring

Security for Servers Performing Network Discovery

Network Devices Supported for Discovery by Operations Manager

Security for Servers Performing Network Discovery

You must ensure the following firewall configuration for network monitoring:

- All firewalls between the management servers in the resource pool and the network devices need to allow SNMP (UDP) and ICMP bi-directionally, and ports 161 and 162 need to be open bi-directionally. This includes Windows Firewall on the management server itself.
- If your network devices are using a port other than 161 and 162, you need to open bi-directional UDP traffic on these ports as well.

Important
Note for customers who used EMC Solutions for Microsoft System Center Operations Manager: EMC Smarts included tools to create an isolation layer to prevent denial of service attacks. In System Center 2012 – Operations Manager, you need to protect your network against packet storms by using external tools.

See Also

Monitoring Networks by Using Operations Manager

How to Discover Network Devices in Operations Manager

Network Device Discovery Settings

Run As Accounts for Network Monitoring in Operations Manager

How to Delete or Restore a Network Device in Operations Manager

Viewing Network Devices and Data in Operations Manager

Tuning Network Monitoring

Network Devices Supported for Discovery by Operations Manager

Reports for Network Monitoring in Operations Manager

Network Devices Supported for Discovery by Operations Manager

System Center 2012 – Operations Manager can monitor physical network routers and switches, including the interfaces and ports on those devices, and the virtual local area networks (VLANs) and Hot Standby Router Protocol (HSRP) groups that they participate in, as well as firewalls and load balancers. Operations Manager can monitor network devices that support SNMP, and can

provide port monitoring for devices that implement interface MIB (RFC 2863) and MIB-II (RFC 1213) standards.

Operations Manager provides more detailed processor or memory monitoring for some network devices, which are listed in the Network Devices with Extended Monitoring Capability spreadsheet. The devices worksheet includes processor and memory columns for each device to indicate whether Operations Manager can provide extended monitoring for either or both aspects for each device.

See Also

Monitoring Networks by Using Operations Manager

How to Discover Network Devices in Operations Manager

Network Device Discovery Settings

Run As Accounts for Network Monitoring in Operations Manager

How to Delete or Restore a Network Device in Operations Manager

Tuning Network Monitoring

Viewing Network Devices and Data in Operations Manager

Security for Servers Performing Network Discovery

Reports for Network Monitoring in Operations Manager

Reports for Network Monitoring in Operations Manager

Processor Utilization Report

This report displays the processor utilization of a particular network device over a period of time.

Memory Utilization Report

This report displays the percentage of free memory on a particular network device over a period of time.

Interface Traffic Volume Report

This report displays the rate of inbound and outbound traffic that goes through the selected port or interface over time.

Interface Error Packet Analysis Report

This report displays the percentage of error packets or discarded packets, both inbound and outbound, for the selected port or interface.

Interface Packet Analysis Report

This report display the types of packets (unicast or nonunicast) that traverse the selected port or interface.

Custom Performance Report

This report displays performance counter values.

Port Traffic Volume

This report display the rate of inbound and outbound traffic that goes through the selected port or interface over time.

Port Packet Analysis

This report display the types of packets (unicast or nonunicast) that traverse the selected port or interface.

Port Error Packet Analysis

This report display the types of error packets that traverse the selected port or interface.

Processor Utilization

This report displays the process utilization of a particular network device over a period of time.

Memory Utilization

This report displays the percentage of free memory on a particular network device over a period of time.

See Also

Monitoring Networks by Using Operations Manager

How to Discover Network Devices in Operations Manager

Network Device Discovery Settings

Run As Accounts for Network Monitoring in Operations Manager

How to Delete or Restore a Network Device in Operations Manager

Viewing Network Devices and Data in Operations Manager

Security for Servers Performing Network Discovery

Network Devices Supported for Discovery by Operations Manager

Tuning Network Monitoring

Monitoring Service Level Objectives by Using Operations Manager

To ensure that resources, such as applications and systems, are available and performing at acceptable levels, companies set goals for their service availability and response times. System Center 2012 – Operations Manager provides the capability to monitor these service goals by tracking service level objectives.

Service level objectives are measurements to ensure that you are meeting defined service level commitments. In Operations Manager, you define a service level objective – the set of monitors that you need to track (such as performance or availability) – and then run reports against that service level objective to ensure that you are meeting your goals.

Using the information from these reports, you can identify any shortfalls between your service level objectives and your actual performance. This means that you are not only aware of problems, but also can track the relative business effect of these problems.

For example, if you have a group of servers running instances of Microsoft Exchange Server, which are critical to your internal e-mail network, you can define a service level objective that states that 95% of the servers must be available at all times. Then, you can generate a report that compares the actual availability of those servers against the service level objective.

You can also create dashboard views to track service level objectives.

Monitoring Service Level Objectives topics

- Defining a Service Level Objective Against an Application
- Defining a Service Level Objective Against a Group
- Running a Service Level Tracking Report
- Creating a Service Level Dashboard

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Initial Monitoring After Operations Manager Is Installed
- Managing Access in Operations Manager
- Getting Information from Operations Manager

- General Tasks in Operations Manager
- Maintenance of Operations Manager
- Operations Manager Report Authoring Guide
- Managing Discovery and Agents

Defining a Service Level Objective Against an Application

You can define a service level objective (SLO) to establish the availability and performance goals for an application. In the following procedure, you create a service level objective against a distributed application, define a monitor SLO that is based on availability (99.9% up-time), and define a collection rule SLO that is based on a performance rule (80% average processor time).

To define a service level objective for an application

1. Open the Operations console with an account that is a member of the Operations Manager Administrators user role.
2. Click **Authoring**.
3. In the navigation pane, expand **Management Pack Objects**, and then click **Service Level Tracking**.
4. In the **Tasks** pane, click **Create**.
5. In the **Service Level Tracking** dialog box, type a name for the service level that you are defining. For example, type **LOB Application 1**. Optionally, you can provide a description. Click **Next**.
6. On the **Objects to Track** page, under **Targeted class**, click **Select**.
7. In the **Select a Target Class** dialog box, select a class for the service level, such as **Distributed Application**, from the list in the text box. You can search for a class by typing its name into the **Look For** text box. Click **OK** to close the **Select a Target** dialog box.
8. You can use the **Scope** option to specify the scope for the service level. The default selection is to use all objects of the targeted class.
9. Select the management pack that this service level will be saved in. You can use an existing management pack or create a new one.
10. Click **Next**.
11. On the **Service Level Objectives** page, click **Add**, and then click **Monitor state SLO** to create a new monitor. This monitor will track the availability of the application.
12. Define the state monitor as follows:
    a. In the **Service level objective name** text box, type a name for the service level objective. For this scenario, type **Availability**.
    b. From the **Monitor** drop-down list, choose the specific monitor that you want to use to

measure the objective. For this scenario, choose **Availability**.

c. Using the **Service level objective goal (%)** spin box, provide the numerical measure for your objective. For example, select **99.990** to indicate that your goal is 99.99% availability.

d. You can refine what the monitor tracks to determine availability by selecting or clearing any of the following state criteria:

- **Unplanned maintenance**
- **Unmonitored**
- **Monitoring unavailable**
- **Monitor disabled**
- **Planned maintenance**
- **Warning**

13. Click **OK**.
14. On the **Service Level Objectives** page, click **Add**, and then click **Collection rule SLO** to create a new collection rule. This rule will track the performance of the application
15. Define the performance collection rule as follows:

a. In the **Service level objective name:** text box, type a name for the service level objective. For this scenario, type **Performance**.

b. Under **Targeted class**, click **Select** to open the **Select a Target Class** dialog box. Specify the target class for the rule from the list of targets in the text box. Note that this class must be contained in the distributed application. For this scenario, select the specific class the rule is targeted to, such as Windows Server 2008 Operating System.

c. Under **Performance collection rule**, click **Select** to open the **Select a Rule** dialog box. Specify the performance collection rule to use. For this scenario, choose **Collect Processor\ % Processor Time performance counter**, and then click **OK**.

d. Using one of the **Aggregation method** options, choose one of the following:

- Average
- Min
- Max

e. Use the **Service level objective goal** drop-down list to specify either **Less than** or **More than**, and enter a value in the adjacent text box. For this scenario, choose **Less Than** and **80**. This indicates that the performance goal is to never exceed 80% processor time.

f. Click **OK**.

16. On the **Service Level Objectives** page, click **Next**.
17. On the **Summary** page, review the settings, and then click **Finish**.
18. When the **Completion** page appears, click **Close**.

After you create a service level objective, you can monitor it by using a Service Level Tracking dashboard view and the Service Level Tracking Report.

See Also

Running a Service Level Tracking Report

Defining a Service Level Objective Against a Group

Creating a Service Level Dashboard

Monitoring Service Level Objectives by Using Operations Manager

Defining a Service Level Objective Against a Group

You can configure a service level objective (SLO) against a group of computers to ensure their availability. In the following scenario, you create a service level that consists of a group of servers (Exchange Servers) and then define a service level objective of 99.99% availability.

To define a service level objective against a group

1. Open the Operations console with an account that is a member of the Operations Manager Administrators user role.
2. Click **Authoring**.
3. In the navigation pane, expand **Management Pack Objects**, and then click **Service Level Tracking**.
4. In the **Tasks** pane, click **Create**.
5. In the **Service Level Tracking** dialog box, type a name for the service level that you are defining. For example, type **Exchange Servers**. Optionally, you can provide a description. Click **Next**.
6. On the **Objects to Track** page, under **Targeted class**, click **Select**.
7. In the **Select a Target Class** dialog box, select a class for the service level, such as **Operations Management Group**, from the list in the text box. You can search for a class by typing its name into the **Look for** text box. Click **OK** to close the **Select a Target** dialog box.
8. You can use the **Scope** options to specify the scope of the service level. The default selection is to use all objects of the targeted class.
9. Select the management pack that this service level will be saved in. You can use an existing management pack or create a new one.
10. Click **Next**.
11. On the **Service Level Objectives** page, click **Add**, and then click **Monitor state SLO** to create a new monitor. This monitor will track the availability of the application.
12. Define the state monitor as follows:
    a. In the **Service level objective name** text box, type a name for the service level objective. For this scenario, type **Availability**.
    b. From the **Monitor** drop-down list, choose the specific monitor that you want to use to

measure the objective. For this scenario, choose **Availability**.

c. For the **Service level objective goal**, provide the numerical measure for your objective. For example, select **99.990** to indicate that your goal is 99.99% availability.

d. You can refine what the monitor tracks to determine availability by selecting or clearing any of the following state criteria:

- **Unplanned maintenance**
- **Unmonitored**
- **Monitoring unavailable**
- **Monitor disabled**
- **Planned maintenance**
- **Warning**

e. Click **OK** to close the **Service Level Tracking** dialog box.

13. On the **Service Level Objectives** page, click **Next**.
14. On the **Summary** page, review the settings, and then click **Finish**.
15. When the **Completion** page appears, click **Close**.

After you create a service level objective, you can monitor it by using a Service Level Tracking dashboard view and the Service Level Tracking Report.

See Also

Running a Service Level Tracking Report

Defining a Service Level Objective Against an Application

Creating a Service Level Dashboard

Monitoring Service Level Objectives by Using Operations Manager

Running a Service Level Tracking Report

You can create a report that shows how your application or group is performing in relation to the defined service level objectives. The report that is generated provides both high-level information to give you a picture of the overall status at a glance, and detailed low-level information to provide specific information on availability and performance metrics.

The Service Level Tracking Summary report shows the results for one or more service levels in comparison to the defined target objectives. From this report, you can examine a more detailed report, the State view, or the Service Level Agreement view.

Use the following steps to generate a Service Level Tracking Summary report.

To generate a Service Level Tracking Summary report

1. Open the Operations console with an account that is a member of the Operations

Manager Administrators user role.

2. In the Reporting workspace, click **Microsoft Service Level Report Library**.
3. In the results pane, right-click **Service Level Tracking Summary Report**, and then click **Open**.
4. Click **Add SLA**.
5. In **SLA Name**, type the name of the defined service level and then click **Search**.
6. Select the service level, and then click **Add**.
7. Click **OK** to close the **Add SLA** window.
8. Define the data period for the report. You can select the following options:
   - **Data aggregation**
   - **Day range**
   - **Time range**
9. Under **Report Fields**, select the fields that you want to include in the report. The fields that are available depend on the day and time range selection. For example, if you have specified a day range of Thursday to Wednesday, you do not have the option to include the **Last 30 Days** field.
10. Click **Run** to generate the report.

See Also

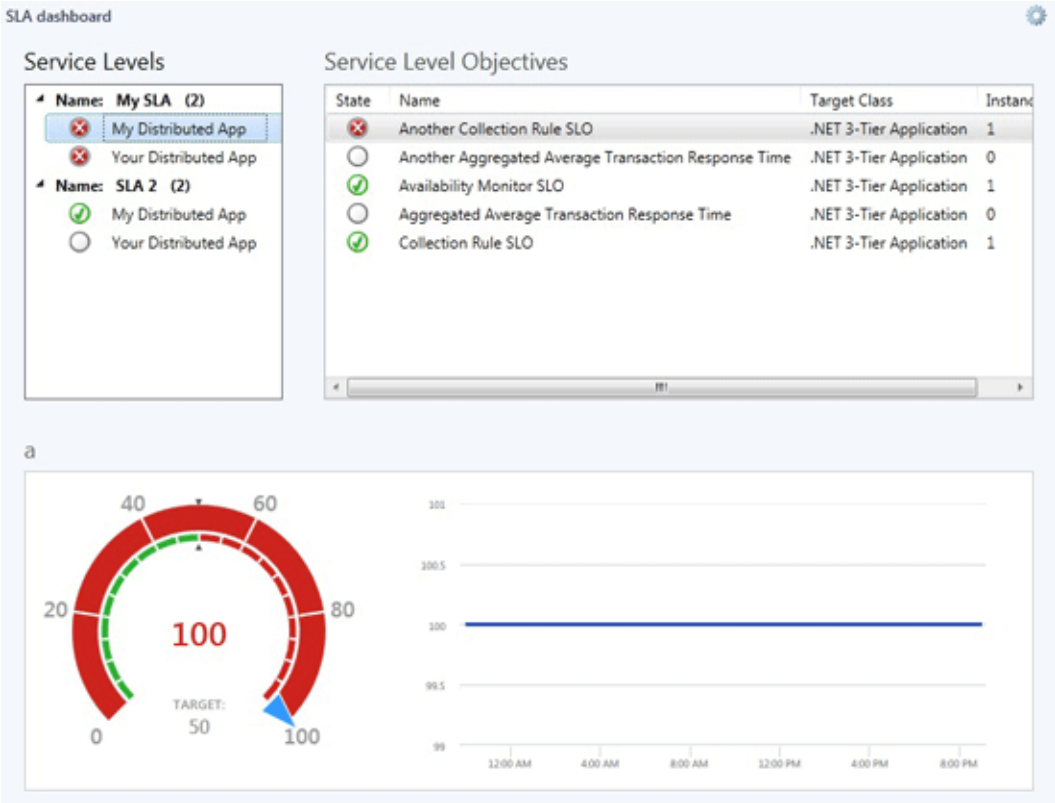
Defining a Service Level Objective Against a Group

Defining a Service Level Objective Against an Application

Monitoring Service Level Objectives by Using Operations Manager

Creating a Service Level Dashboard

After you configure a service level objective, you can create a service level dashboard view to monitor the service level objective. The service level dashboard view displays a grid of service levels and a grid of service level objectives grid which lists the various objectives which have a goal or target value and whether success is either above or below that target value for the currently selected SLA/instance. When you select an objective in the **Service Level Objectives** grid, a gauge and chart is displayed, as shown in the following image.



The gauge will show the average actual value, along with the target value and a indication as to whether the value and goal relationship corresponds to success (green) or failure (red). The chart will show a time history of the actual values, which will be a function of the aggregation of the values in the data warehouse, which will depend on the timeframe of the configured dashboard, as to whether the values come from the Hourly or Daily aggregation table.

To create a service level dashboard view

1. In the Operations console, click **My Workspace**.
2. Right-click the folder where you want to store the view, point to **New**, and click **Dashboard View**.
3. In the New Instance Wizard, on the **Template** page, click either **Flow Layout** or **Grid Layout**, and then click **Next**.
4. On the **General Properties** page, enter a name for the dashboard view. The description is optional. Click **Next**.
5. On the **Specify the Scope** page, click **Add**.
6. In the **Add SLA** window, select the service level objective that you created, click **Add**, and then click **OK**. You can add multiple service level objectives.
7. On the **Specify the Scope** page, in the **Last** section, set the period of time that you want to display in the dashboard view, and then click **Next**.
8. Review the settings on the **Summary** page, and then click **Create**.

9. Click **Close**.

See Also

Monitoring Service Level Objectives by Using Operations Manager

Defining a Service Level Objective Against an Application

Defining a Service Level Objective Against a Group

Monitoring .NET Applications

In System Center 2012 – Operations Manager, you can monitor web applications from server- and client-side perspectives to get details about application performance and reliability that can help you pinpoint the root causes of incidents. When you specify settings, the types of events to collect, the performance goals to measure, and servers to monitor, Operations Manager application monitoring reveals how web-based applications are running. You can see how frequently a problem is occurring, how a server was performing when a problem occurred, and the chain of events related to the slow request or method that is unreliable. This information is required to partner with software developers and database administrators to help ensure that applications perform correctly and reliably at optimal levels.

A New 2-Step Application Monitoring Strategy

Application monitoring in Operations Manager has two new monitoring features that allow you to prioritize alerts and then investigate and troubleshoot individual issues:

- **Step 1: Identify problem areas** Use Application Advisor to help you prioritize and manage which performance and exception events to address. Application Advisor identifies and lists which applications are causing the most problems within an environment. These are the applications you should address first because they are causing most SLA violations. If you are responsible for applications, Application Advisor provides a helpful view into your application's overall health.
- **Step 2: Diagnose problems** Use Application Diagnostics to help you investigate and troubleshoot specific events. You can view event properties, performance counters, distributed chains, similar and related events to narrow the cause of the issue and help identify who should correct the problem. Application Diagnostics is available as a standalone web console or through links in the Alert descriptions in the Operations Manager consoles.

Monitoring .NET Applications Topics

- Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)
- Working with the Application Diagnostics Console
- Working with Events by Using Application Diagnostics
- Prioritizing Alerts by Using Application Advisor

- User Roles for Application Performance Monitoring
- Working with Sensitive Data for .NET Applications
- Notes for AVIcode 5.7 Customers

See Also

Prioritizing Alerts by Using Application Advisor

Working with Events by Using Application Diagnostics

User Roles for Application Performance Monitoring

Notes for AVIcode 5.7 Customers

.NET Application Performance Monitoring Template

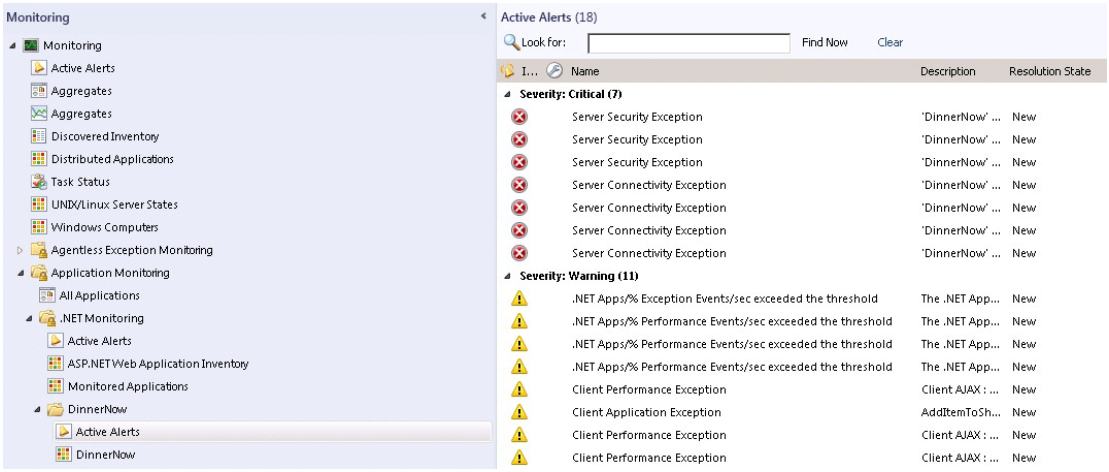
Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

After you have configured .NET applications to be monitored, you can view alerts and begin investigating the issues.

To view and investigate alerts for .NET applications (server-side example)

1. To view active alerts by application group, in the System Center 2012 – Operations Manager console, in the navigation pane, click the **Monitoring** button, expand **Application Monitoring**, expand **.NET Monitoring**, expand the folder with the name of the application group you configured for monitoring, and then click **Active Alerts**.

   View alerts by application group

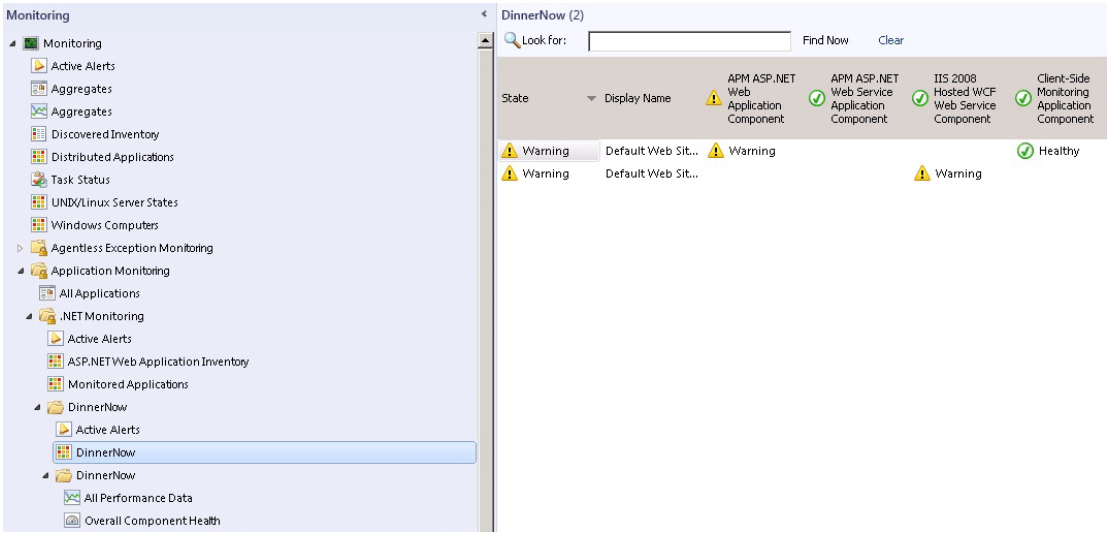


   Additional views:

   - To see why a monitoring aspect is unhealthy, use the application group state view

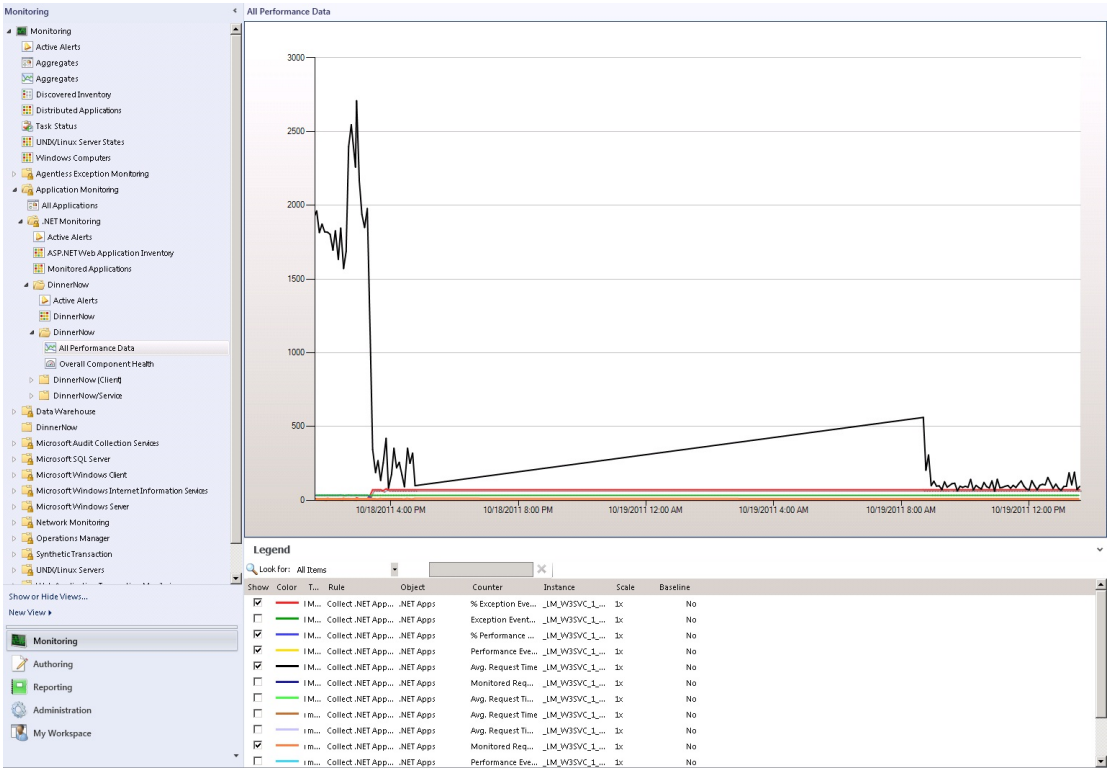
and click the state view cell related to it. The Details View will show you the instance and the state of the Availability, Configuration, Performance, and Security monitors. You can also start the Health Explorer in context of the application instance to see which monitors have gone into a critical or warning state.

Application group state view



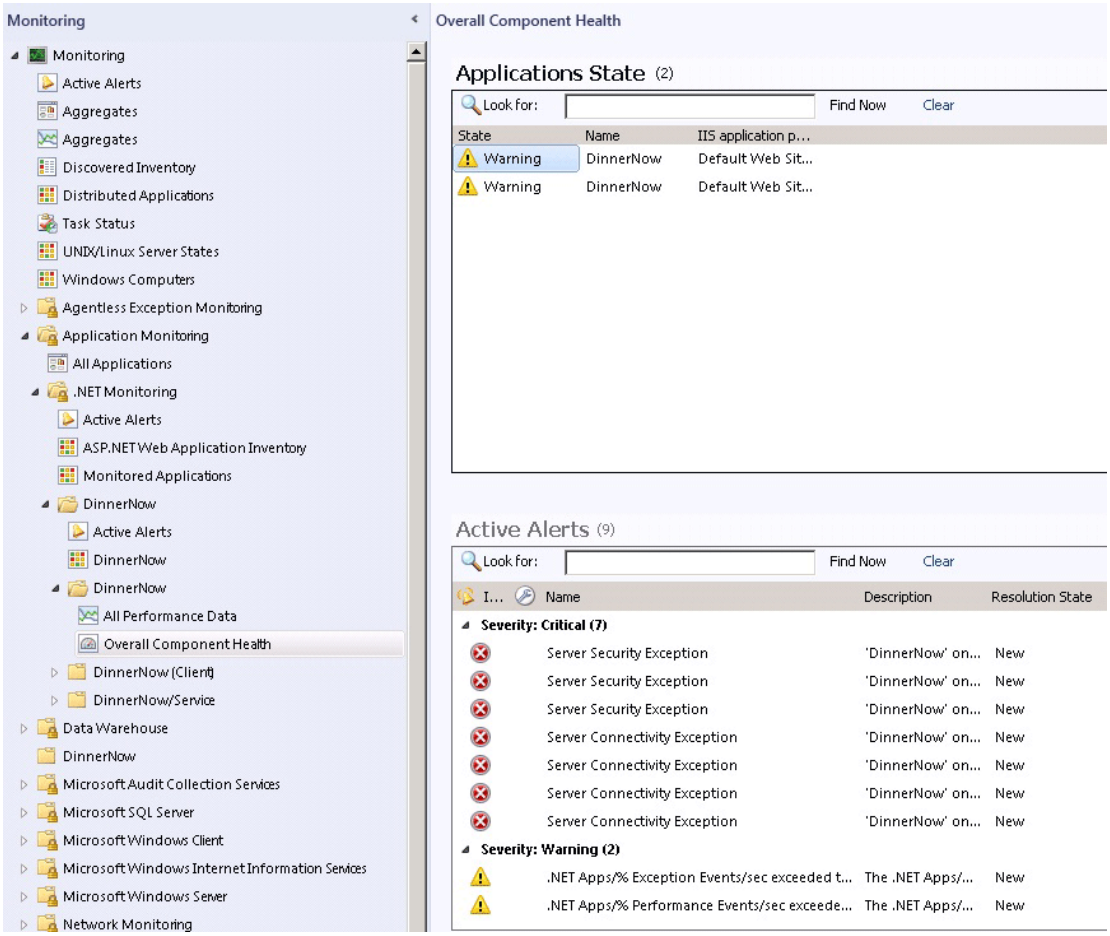
- To see application performance, in the application component folder, click **All Performance Data**. This gives you the base information about each component, shown by instance.

  All performance data



- To see the overall health dashboard view of the components you selected for the application you are monitoring, in the application component folder, click **Overall Component Health**. You will see the application state, active alerts, and a detail view.

  Overall component health



To work with data collected by client-side monitoring, in the Operations Manager console, in the navigation pane, click the **Monitoring** button, expand **Application Monitoring**, expand **.NET Monitoring**, and then application name (client) folder. The client-side monitoring process is very similar to server-side monitoring, except that you click **All Performance Data** and **Overall Component Health** in the application name (client) folder to view alerts pertaining to the client-side monitoring for the application group.

To make sure client-side application monitoring is working, go to the application group state view and the **CSM Application Component** will have application monitoring status filled in.

Note

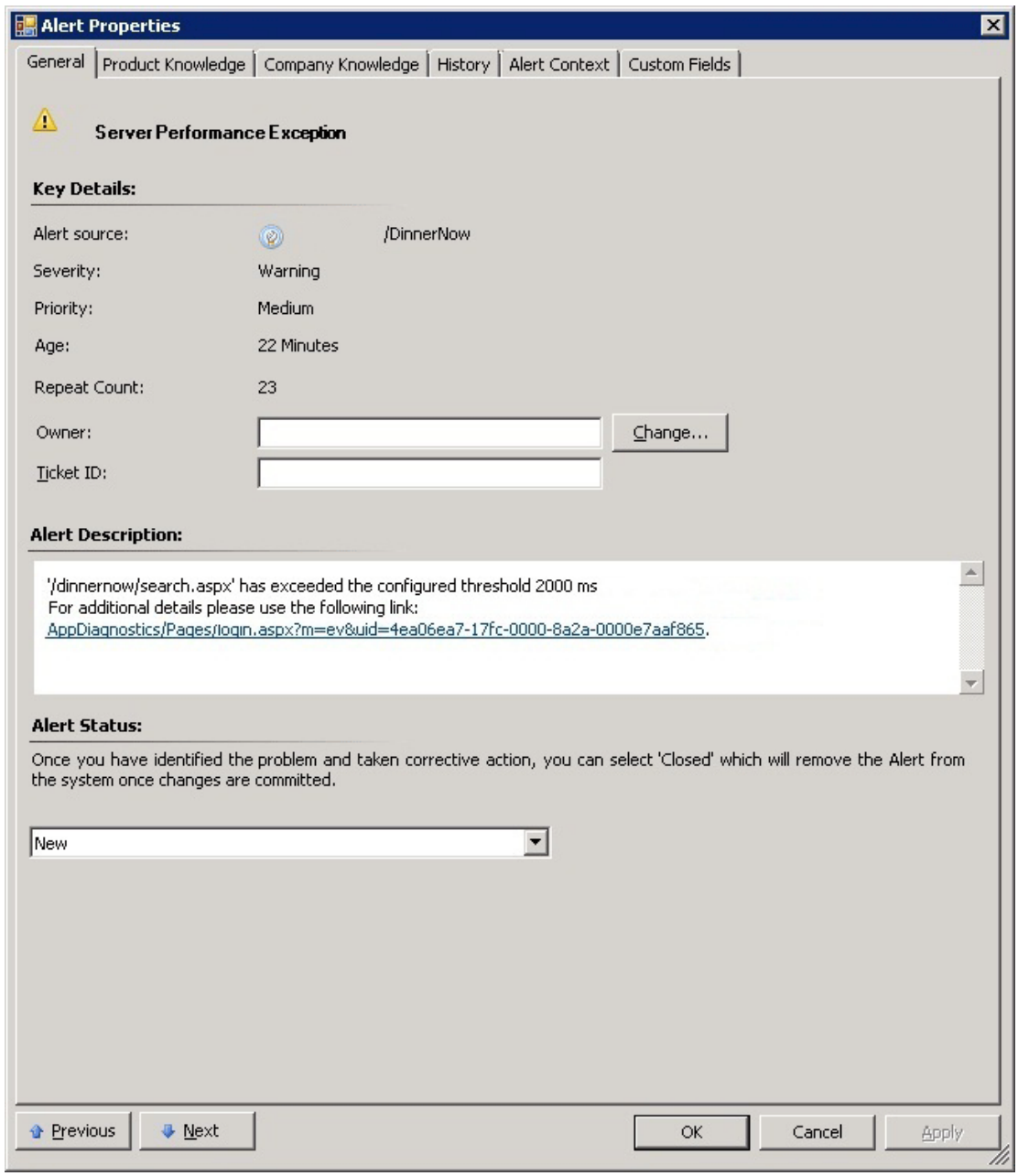
Client-side monitoring is an extension of server-side monitoring that is not enabled by default. You set it up through the same template as server-side monitoring. It might take a few minutes to discover the objects after you set up client-side monitoring.

2. To see general details about an alert, click an alert. The **Alert Details** pane describes the alert, including information about its source, rule, creation date, and the monitoring

setting that caused the alert to be raised.

3. To begin investigating an alert and view the alert description, double-click an alert. The **Alert Properties** page will open.

Begin investigating alerts on the Alert Properties page



Note

To see details about an alert in any of these views, click the alert you want to investigate and look in the **Alert Details** pane for the **Knowledge** section. You

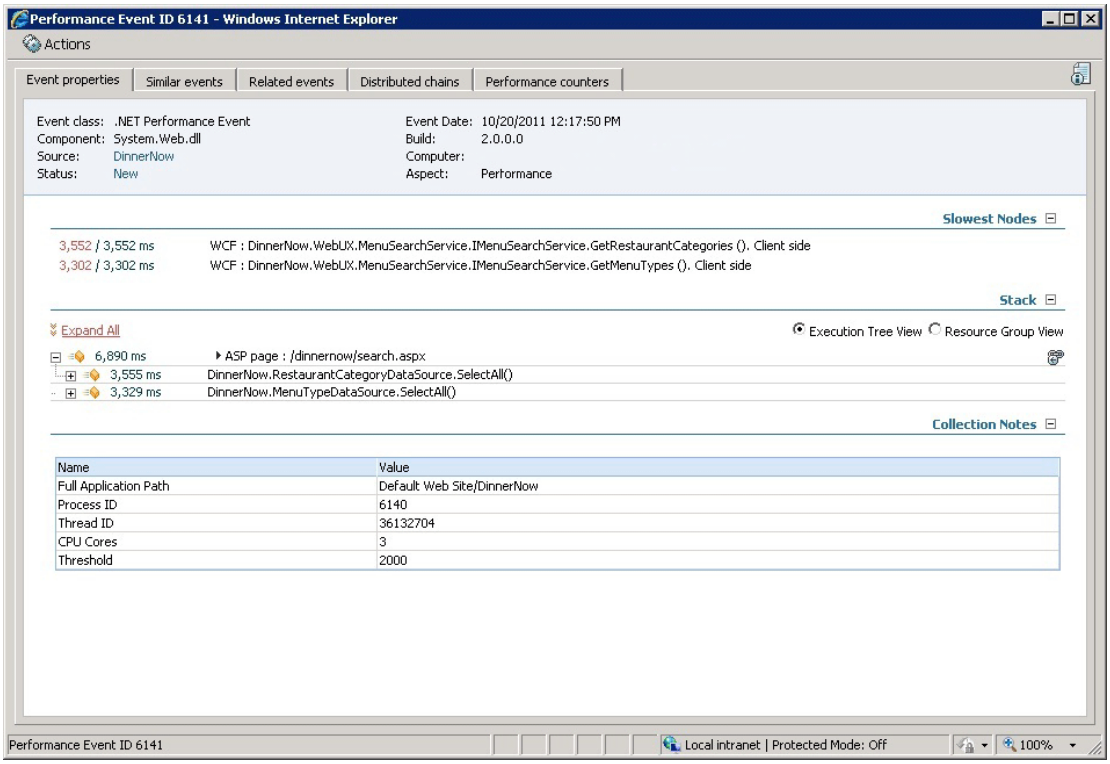
can also open the Alert Properties page, which shows the details of an alert and you can enter alert status. To open the Alert Properties page, double-click an alert or in the **Tasks** pane, in the **Tasks** section, click **Alert Properties**.

4. On the **Alert Properties** page, click the link in the **Alert Description** pane. This opens Application Diagnostics, a new monitoring feature in Operations Manager in a web browser. Here on the **Event properties** tab you can see information, such as the performance metrics, the call stack, and collection notes. For more information on the Event properties tab, see Performance Event Details. Click **Yes** to close the main window once the event information has loaded.

   Note

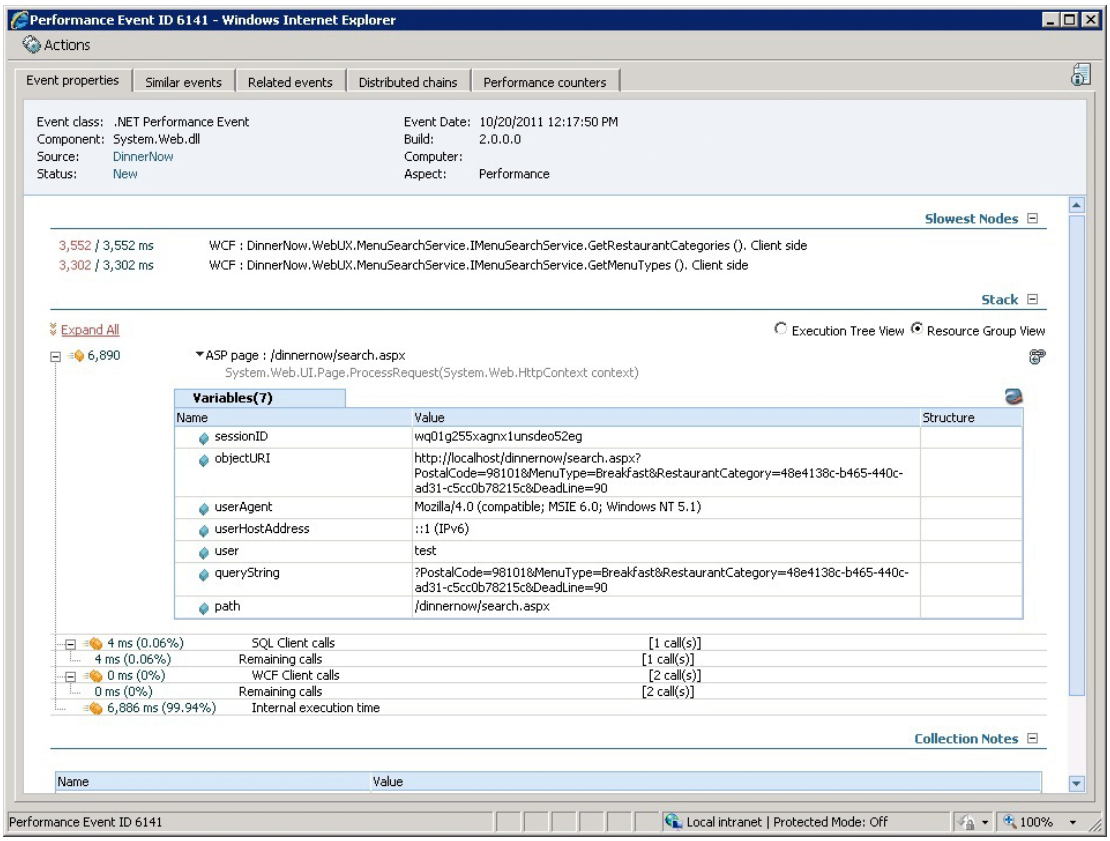
   This link to Application Diagnostics is also on the **Alert Context** tab.

5. **Application Diagnostics Event properties**



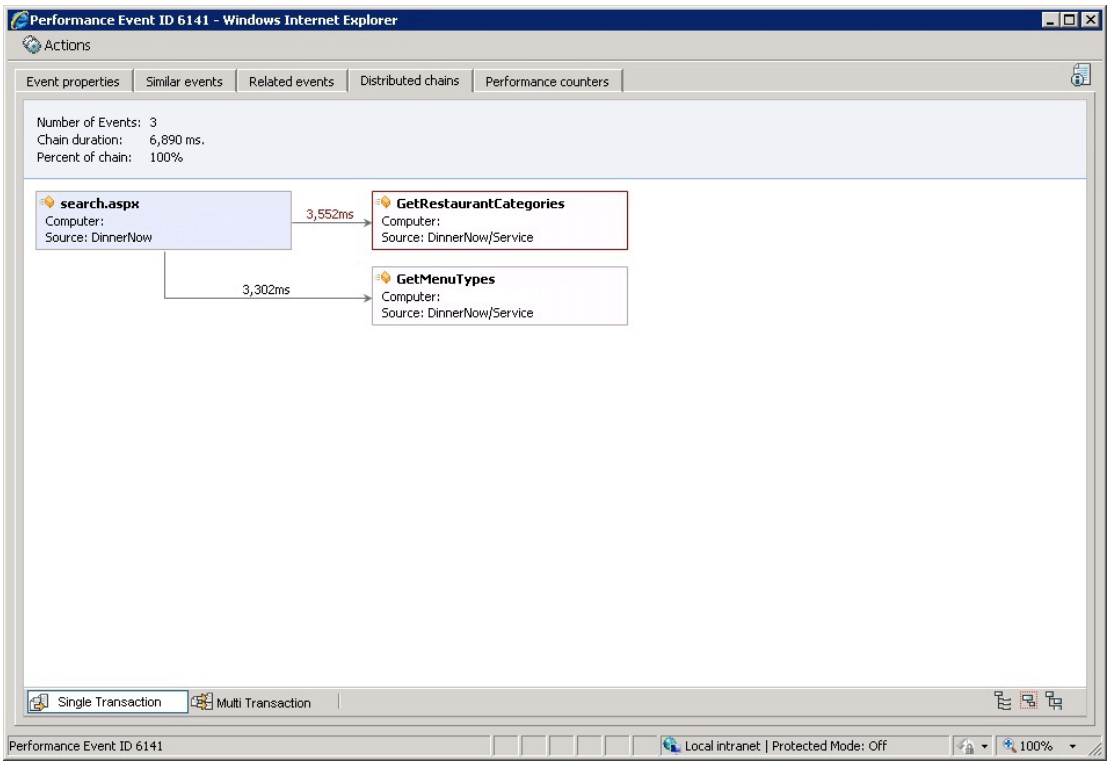
6. On the **Event Properties** tab, expand the **Stack** section. The stack is the order in which events happened. The **Resource Group View** and **Execution Tree View** allow you to expand nodes to investigate the various calls. This view helps answer which tier the problem is in, or where is it occurring.

   Application Diagnostics tree views lets you see exactly what went wrong where and when.



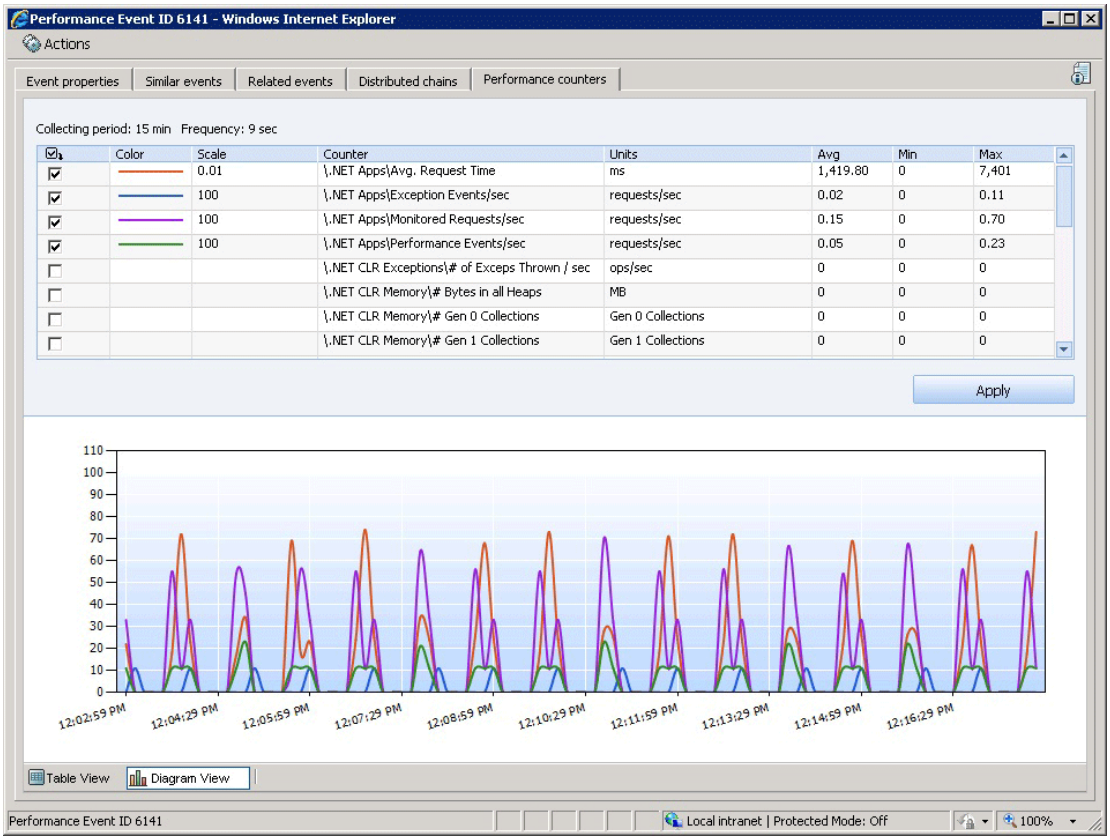
7. To see how this event relates to other events in the chain of events, on the Application Diagnostics page, click the **Distributed chains** tab. This view shows all of the components that are involved in the request.

   Application Diagnostics Distributed chains show how events relate to each other.



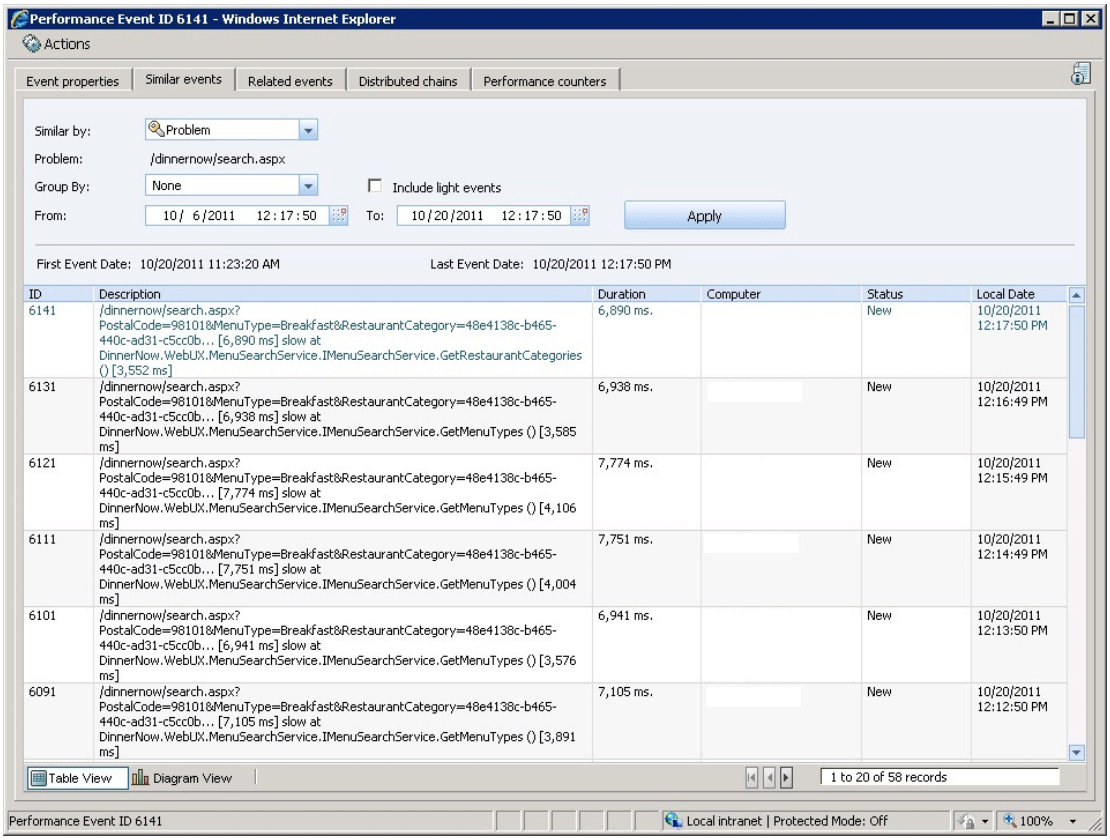
8. To pinpoint the root cause of the problem or incident, click the last event in the chain. This is the latest event that broke the performance threshold. The **Event Properties** tab for that event will open.
9. On the **Application Diagnostics** page, click the **Performance counters** tab. Performance counters show the system 15 minutes before the event happened. This gives a baseline measure before the event, which allows you to see your system state before the event so that you know if the system was impacting the performance of the application.

   Application Diagnostics Performance counters allow you to compare system performance before, during, and after an event.



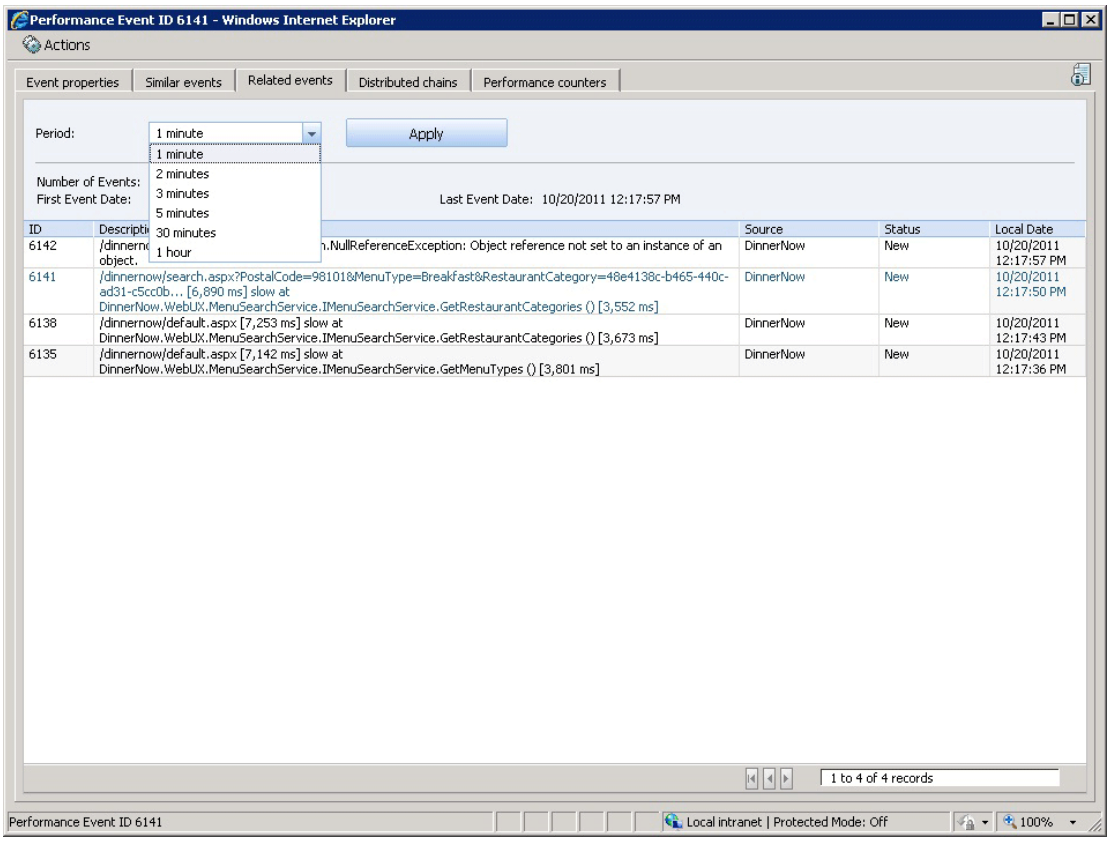
10. On the **Application Diagnostics** page, click the **Similar events** tab. Similar events are the other events that are in the same problem group. On this page you can filter similar events by **Problem** and **Heaviest Resource** to help you identify trends.

    Application Diagnostics Similar events allow you to compare similar events to identify trends.



11. On the **Application Diagnostics** page, click the **Related events** tab. Related events are events that occurred around the same time as the event you are investigating. Related events tell you what else is going on about the same time as the event you are investigating. You can increase or decrease the range of time in which other related events occurred relative to the event you are investigating. In general, specifying a greater time range shows you more related events.

    Application Diagnostics Related events allows you to see what other events are occurring about the same time as the event you are investigating.



Working with the Application Diagnostics Console

The Application Diagnostics console is an event management system for .NET Application Performance Monitoring in System Center 2012 – Operations Manager. You can use Application Diagnostics console to monitor deployed .NET applications for slowdowns, faults, and failures, and immediately pinpoint the source of the problem.

The Application Diagnostics Console

The Application Diagnostics console is the place to look at the individual performance and reliability events that are being raised within your environment. You can look at all of the events, or group them into “problem groups” in which events coming from the same sources are grouped together to highlight the problems with the monitored applications. Use Application Diagnostics to look at events and the transaction chains related to those events to understand how the performance and reliability issues are impacting your applications. The Application Advisor

console provides analytics and telemetry of the data presented in Application Diagnostics. Through the Application Advisor console you gain insights into which events are causing the most problems. For more information about Application Advisor, see Prioritizing Alerts by Using Application Advisor

To open the Application Diagnostics console

1. Application Diagnostics and Application Advisor are installed along with the Operations Manager web console. To find the web address of the Operations Manager web console, open the Operations console. In the navigation pane, click the **Administration** button, click **Settings**, and then double-click **Web Addresses**. The Operations Manager web console URL will be specified as: http(s)://<web host>/OperationsManager. Using this URL format and the same web host, here are the links to Application Advisor and Application Diagnostics:
   - The Application Diagnostics console address is: http(s)://<web host>/AppDiagnostics
   - The Application Advisor console address is: http(s)://<web host>/AppAdvisor

   To make access to the consoles easy, add all three console URLs to your web browser's favorites list.

   To open Application Diagnostics, paste the Application Diagnostics URL into your browser. Application Diagnostics opens in the web browser window.

   Note
   If you are running Operations Manager on a server rather than a client computer, you can access Application Diagnostics and Application Advisor from the **Start** menu in **All Programs**.

   Access to Application Diagnostics is controlled through the Application Monitoring Operator and Administrator roles. You must be a member of one of these roles to have rights to the console. For more information, see User Roles for Application Performance Monitoring

Viewing Events by Areas of Interest

In Application Diagnostics, there are two major types of events, those related to application performance and those related to application failures and errors. The failures and errors can be divided further into connectivity, security, and failure issues. Failure issues are typically related to a problem with the application code. In Application Diagnostics, you can view events grouped in these ways:

- All (displays all events)
- Application Errors (displays exception events)
- Performance (displays performance events)

To select the type of events to view

1. Open Application Diagnostics and select **Events** from the Navigation pane.
2. In the Navigation pane, use the **Search for** menu to select the category of events you want to view.

Grouping Events within Areas of Interest

Grouping application events by similarity provides the best method for determining if the same issue has occurred before and ensuring that resources responsible for the issue resolution are allocated in the most efficient way.

To group events into areas of interest

1. Open Application Diagnostics and select **Events** from the Navigation pane.
2. In the Navigation pane, use the **Search for** menu to select the category of events you want to view.
3. In the **Group By** menu, select the way you want to group the events.

Your first selection (**Application Errors** and **Performance**) affects the grouping options you see for your second selection.

Grouping Application Errors

- **Problem** What it displays: All events in this grouping are coming from the same entry point into the application (for example, a method or a web page) and have the same call stack. Value: Consolidating events by problem allows you to prioritize your efforts to correct an issue based on the number of events in the group.
- **Action** What it displays: Action-based consolidation categorizes events based on entry points, such as page calls, button clicks, web service calls, or some other action representing a particular process. Value: This grouping is valuable for determine under what circumstances a failure occurs.
- **Exception Class** What it displays: The bottom level exception thrown by each event is the same. Value: Consolidating by exception class is a good way to find the most typical coding mistakes and promotes improved coding practices.
- **Failed Function** What it displays: The exception occurred in the same function for each event. Value: This grouping is valuable for two reasons: First, it allows you to identify cases where a shared function is used incorrectly. Second, it allows you to identify how many applications are impacted by an error in a shared function.
- **None** This option does not group the events.

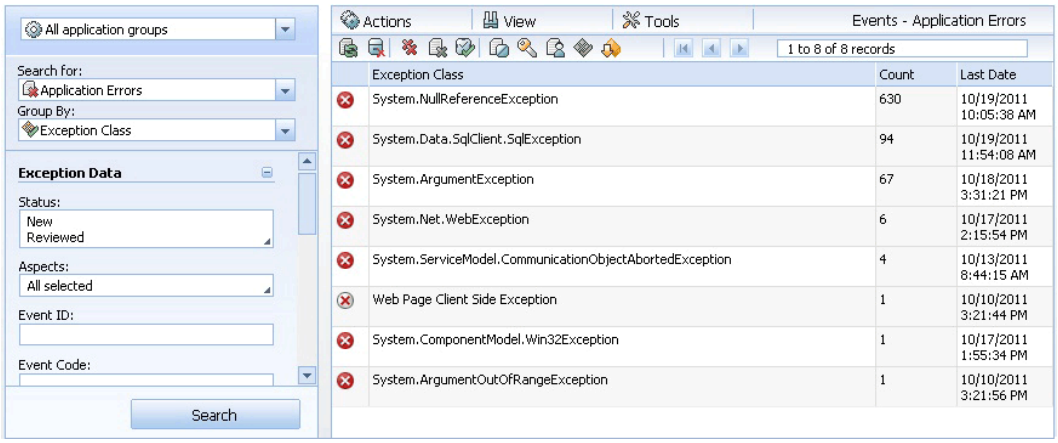
Grouping Performance Events

- **Problem** What it displays: All events in this grouping have the identical call stack. Value: Consolidating events by problem allows you to prioritize your efforts to correct an issue based on the number of events in the group.

- **Heaviest Resource** What it displays: All events triggered by the same resource call. This grouping is valuable for determine which events exceeded their thresholds more than other resources.
- **None** This option does not group the events.

Example: Grouping Application Errors by Exception Class

Filtering by application errors and exception class quickly shows you which kinds, or classes, of exception events you are receiving most often.

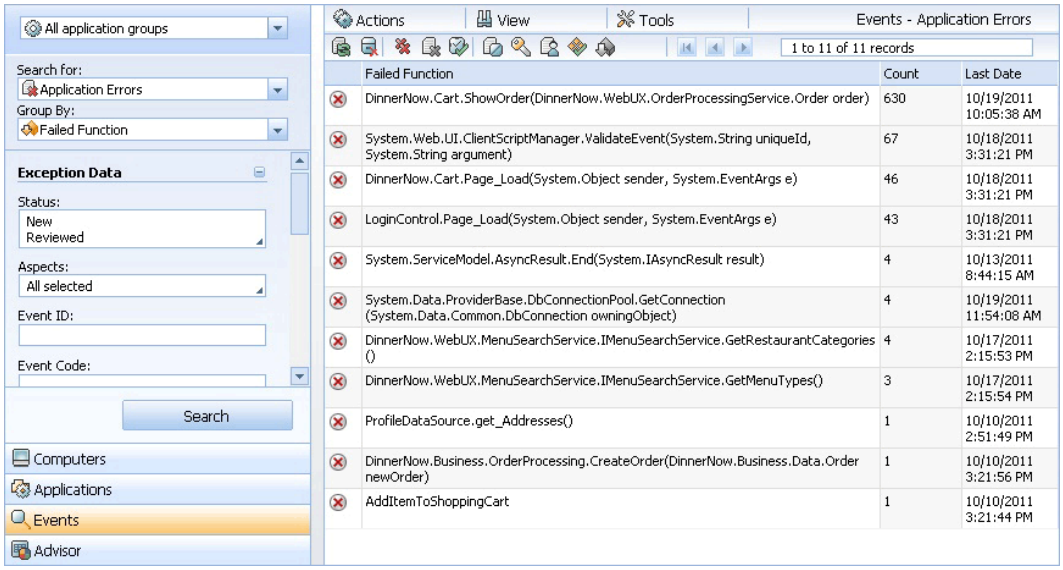


To group application errors by exception class

1. Open Application Diagnostics and select **Events** from the Navigation pane.
2. In the Navigation pane, in the **Search for** menu, select **Application Errors**.
3. In the **Group By** menu, select **Exception Class**.
4. To sort by count, at the top of the Count column, click **Count**. The exception classes that have occurred most often are ranked from highest to lowest.
5. To begin investigating the issue and open Event properties, click an **Exception Class** entry. For information about working with events, see Working with Events by Using Application Diagnostics

Example: Grouping Application Errors by Failed Function

Filtering by application errors and failed function quickly shows you which functions are failing most often. The functions that are failing the most are the ones you should investigate first to have the highest impact on your application's reliability.

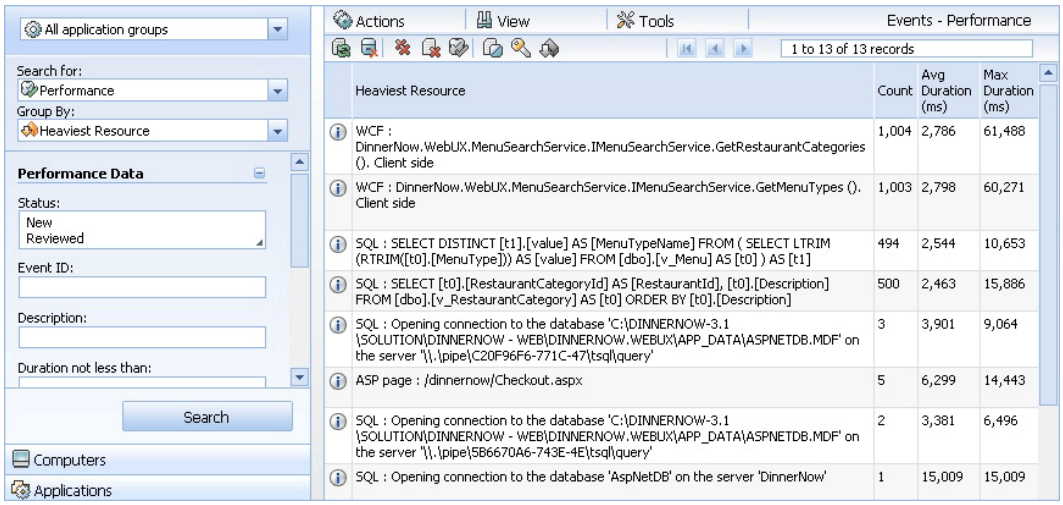


To group application errors by failed function

1. In the navigation pane, in the **Search for** menu, select **Application Errors**.
2. In the **Group By** menu, select **Failed Function**.
3. To sort by count, at the top of the Count column, click **Count**. The functions that have failed most often are ranked from highest to lowest.
4. To begin investigating the issue and open Event properties, click a **Failed Function** entry. For information about working with events, see Working with Events by Using Application Diagnostics

Example: Grouping Performance Events by Heaviest Resource

Filtering by application errors and exception class quickly shows you which performance events are triggered by the same resource call. The performance events that are most often triggered by the same resource call are the ones you should investigate first to have the highest impact on you application's performance.



To group performance events by heaviest resource

1. In the navigation pane on the left, in the **Search for** menu, select **Performance**.
2. In the **Group By** menu, select **Heaviest Resource**.
3. To sort by count, at the top of the Count column, click **Count**. The exception classes that have occurred most often are ranked from highest to lowest. You can also sort by average duration and maximum duration to see if some events that are occurring less often are still causing long delays and therefore should receive your attention.
4. To begin investigating the issue and open Event properties, click a **Heaviest Resource** entry. For information about working with events, see Working with Events by Using Application Diagnostics

See Also

Prioritizing Alerts by Using Application Advisor

Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

Working with Events by Using Application Diagnostics

Working with alerts is a standard part of working with System Center 2012 – Operations Manager. Alerts for .NET application monitoring show you the information you will recognize from other alerts, such as the general information and product knowledge. However, a .NET application alert also provides a link in the alert description. This link opens the event that raised the alert in Application Diagnostics. Here you can see far more information that will help you troubleshoot and identify your problem and solution.

Note

Deep troubleshooting of alerts from Application Performance Monitoring often requires access to the application source code and might require input from developers. You can install the Team Foundation Server Work Item Synchronization Management Pack and forward alerts to Team Foundation Server used by the development team. The Team Foundation Server Work Item Synchronization Management Pack tracks and synchronizes changes made to Team Foundation Server work items and changes made to associated Operations Manager alerts.

Investigating .NET Application Alerts

Decreasing the time it takes to determine, assign, and resolve issues is the central goal of application monitoring in Operations Manager. When you receive an alert, you need to know what caused it—the system hosting the application or the code, be able to show the data to back up that conclusion, and clearly see who should fix the problem. To know if it is a system issue, you need to know the state of your system at the time of the event. To know where the root problem occurred, you need to know the chain of calls that occurred. To further investigate you need to compare similar events and related events that happened at the same time. Together, the event details, performance counters, and distributed chains will help you triage who should look at this problem first. If it is a system error you can adjust the available resources or configuration of the host system and address the issue at the host level. If it is an application failure, the problem will need to go to the application team along with the line of code where the failure occurred. Here are some strategies for using the views, filters, and settings in Application Diagnostics to help you get to the root cause, find a resolution, and better know who needs to be involved to fix the problem.

To open Application Diagnostics from an alert

1. Since you are responding to alerts related to specific application groups that you configured, it is helpful to scope active alerts and view them by application group. In the Operations Manager console, in the navigation pane, click the **Monitoring** button, expand **Application Monitoring**, expand **.NET Monitoring**, click the folder with the name of the application group you configured for monitoring whose alerts you want to investigate, and then click **Active Alerts**.
2. Double-click the alert you want to open.
3. On the **Alert Properties** page, click the link in the **Alert Description** pane. This opens Application Diagnostics, a new monitoring feature in Operations Manager in a web browser. Here on the **Event properties** tab you can see information, such as the performance metrics, the call stack, and collection notes about the alert. Using the tabs, you can see similar events, related events, event chains, and performance counters. This is detailed information about the performance or exception event that was raised for the application that will help you diagnose whether the issue is coming from the application itself, a call to a web service, or a call to a database. For more information on the Event properties tab, see Performance Event Details. Click **Yes** to close the main window once the event information has loaded.

Note

This link to Application Diagnostics is also on the on the **Alert Context** tab.

Use the following procedures to investigate your alert. IT Pros will most likely want to use information on the Event properties, Performance counters, and Distributed chains tabs to find out what happened, understand if a system issue caused the problem, and investigate where the root cause occurred. Developers will most likely need to use the information on the Distributed chains, Similar events, and Related events tabs to understand the specific context around a code problem.

To troubleshoot by using Exception Event properties in Application Diagnostics

1. In the Application Diagnostics window for the exception alert you are investigating, click the **Event properties** tab to view key details about the alert. This is the first place to check to see if the alert problem is apparent. Some of the key categories of information you will see on the Event properties page are as follows:
   - **Source** To display the application load and response times, click the **Source** link in the upper-left corner. This information shows the load the system was under in the context of the exception event failure. To view performance counters and further assess system state, on the Source page, click the **Trend reports** tab. To see which computers this application is working on and see if there might be a load balancing problem across computers, click the **Computers** tab. To see a breakdown of related calls, or where the events are happening based on chains, click the **Topology** tab.
   - **Exception Chain** This displays for exception events. Expand Exception Chain to view the actual exception that occurred.
   - **Exception Data** This displays for exception events and shows parameters and variables set for the class through the exception.
   - **Stack** This is the call stack, or order in which things happened. The Execution Tree View allows you to expand nodes to investigate the calls. Click the **Resource Group View** radio button to display an overview of where time was spent. This answers which tier the problem is in, or where is it occurring.
   - **Modules List** This displays for exception events and shows modules loaded at time of exception.
   - **Collection Notes** This displays any notes about the event.

   Tip

   Use the same troubleshooting steps for Performance events, Similar events, Related events, Distributed chains, and Performance counters as you did for Exception events.

To troubleshoot by using Performance Event properties in Application Diagnostics

1. In the Application Diagnostics window for the performance alert you are investigating, click the **Event properties** tab to view key details about the alert. This is the first place to check to see if the alert problem is apparent. Some of the key categories of information

you will see on the Performance properties page are as follows:

- **Source** To display the application load and response times, click the **Source** link in the upper-left corner. This information shows the load the system was under in the context of the exception event failure. To view performance counters and further assess system state, on the Source page, click the **Trend reports** tab. To see which computers this application is working on and see if there might be a load balancing problem across computers, click the **Computers** tab. To see a breakdown of related calls, or where the events are happening based on chains, click the **Topology** tab.
- **Slowest Nodes** This is a list of the slowest nodes in the Execution Tree View and the most likely cause of the performance issues in the application.
- **Stack** This is the call stack, or order in which things happened. The Execution Tree View allows you to expand nodes to investigate the calls. Click the **Resource Group View** radio button to display an overview of where time was spent. This answers which tier the problem is in—where is it occurring?
- **Collection Notes** This displays any notes about the event.

To troubleshoot the state of the system by using Performance counters

1. To view a table or diagram of key performance counters, click the **Performance counters** tab.

   Note
   Fifteen minutes of performance data is collected and cached on the monitored system. When a performance or exception is raised, the performance data is sent back to Operations Manager along with the event.

2. Select the performance counter checkboxes for the performance counters you want to include in your information, and then click **Apply**.
3. Use the information in this display to assess the system performance state around the event you are investigating. For example, if the performance is uniformly slow at the time of the event, then your alert is likely due to a system performance problem.

To find the root problem by using Distributed chains

1. Click the **Distributed chains** tab to view the order of calls—the chain of events of which the event is part. This helps you understand how the event you are investigating was impacted by other events from the application or related applications.
2. In the Distributed chains view, click one of the calls, or links, in the chain. If there are multiple events for the same object, the Chaining Wizard will open. This wizard allows you to select possible events to correlate into a chain of events. To begin the Wizard, click **Next**.

   Note
   Get the time stamp from the call you select as you will pair this with an event on the next page.

3. The **Select Possible Chain Event** page, select the event that you want to examine.

Ideally it will be the event with the time stamp that is closest to call you selected in the Distributed Chains view.

4. What you see next depends on the kind of problem you are investigating. For example, if you select a transaction where a server is not found, you might go to the event properties page for that event. This will let you pair the server error with the event you were initially investigating. Since it is a server error, you know that the problem is not on the client side, but server side. You might see a graph of the event you selected and be able to breakdown a performance event in terms of the page load time.
5. From event properties, click the server-side call, and click the **Performance Counters** tab for more details.

To troubleshoot by viewing similar events

1. Click the **Similar events** tab to see if similar alerts have been thrown more times, which could mean that there is a problem with the application.
2. There are several ways to filter similar events. Click the **Similar by** dropdown menu to select how you want to group the similar events: by problem, action, exception class, or failed function. In the **From** and **To** text boxes, you can set the range of dates from which you want to view the similar events. Use the **Similar events** tab to view if similar alerts has been thrown more times, which could mean that there is a problem with the application.
   - **Filtering by Problem** shows you similar events that are of the same type. For example you can see all similar events where the object reference is not set to an instance of an object. Click the **Diagram View** button and you can see the ratio of total number of events for the current problem and the total number of events from other problems. This information gives you a quick view into the magnitude of the problem that this particular event has. If many of the current total similar events have the same problem, it might be a higher priority problem to resolve since it will have high impact in reducing the number of alerts you receive.
   - **Filtering by Action** groups the similar events by aspect: security, performance, connectivity, and application failure. Click the **Diagram View** button and you can see the number of similar events by these aspect categories and more easily see which ones the problem might be related to.
   - **Filtering by Exception class** groups the similar events according to how you named them during configuration. Presumably, these would be names that would help you identify the kind of exceptions they are, such as **System.NullReferenceException** class.
   - **Filtering by Failed function** groups the similar events by the same function is throwing the exception. This could mean that there is a problem with the entry point.

   Keep in mind that these are all similar events—related by definition—and these filters give you a better idea of exactly how they are related. So, using the Similar Events filters, you might find that most of your total events have the same problem as the event you are viewing, that it is a performance problem, that they belong to an exception class you configured, and that half of the similar events had the same failed function. Action: The

function goes to the developer who needs to update the function code.

To troubleshoot by viewing related events

1. Click the **Related events** tab to view events that are related by time. These are exceptions correlated with other events that might give you an insight to the problem.
2. To view the event details of an event in the list, click the link in the **Description** column.

   In the related events you might notice that response time is very slow for all events during a certain time. This could indicate a problem with the system, not the code, and so might go to the IT pro for a solution.

Prioritizing Alerts by Using Application Advisor

Application Advisor works with .NET Application Performance Monitoring in System Center 2012 – Operations Manager and helps you prioritize and manage which alerts to address. It identifies which applications are causing the most alerts within an environment. These are the applications you should investigate first because they are causing the most service level agreement (SLA) violations. Use Application Advisor as a first step in alert management and as a view into the overall health of an application. Essentially, Application Advisor helps you “follow the noise” and find out where the most events are occurring. Application failure and analysis reports let you view those individual applications in fine detail. Summary reports give you key information at a glance, such as the top-five alerts to resolve.

To scope and run an Application Advisor report

1. Application Advisor and Application Diagnostics are installed along with the Operations Manager web console. To find the web address of the Operations Manager web console, open the Operations console. In the navigation pane, click the **Administration** button, click **Settings**, and then double-click **Web Addresses**. The Operations Manager web console URL will be specified as: http(s)://<web host>/OperationsManager. Using this URL format and the same web host, here are the links to Application Advisor and Application Diagnostics:
   - The Application Advisor console address is: http(s)://<web host>/AppAdvisor
   - The Application Diagnostics console address is: http(s)://<web host>/AppDiagnostics

   To make access easy, add all three console URLs to your web browser’s favorites list.

   To open Application Advisor, paste the Application Advisor URL into your browser. Application Advisor opens in the web browser window. Different application monitoring reports display in the context of the application features and services you configured when you created application groups to monitor.

Access to Application Advisor is controlled through the Application Monitoring Operator, Report Operator and Administrator roles. You must be a member of Application Monitoring Operator and Report Operator roles or the Administrator role. For more information, see User Roles for Application Performance Monitoring

Access to Application Diagnostics is controlled through the Application Monitoring Operator and Administrator roles. You must be a member of one of these roles to have rights to the console.

Note
Application Advisor requires SQL Server Report Services (SSRS). You must have Operations Manager reporting installed before using Application Advisor.

2. In the **Navigation** pane, in the **All application groups** dropdown menu, select whether you want reports to include information for all application groups or a subset of application groups.

   Note
   Application groups are created in the Application Diagnostics console. Use them to create a group of applications to which you would like to scope your reports. Using many application groups can have a performance impact.

3. In the **Select report** menu, select how you want to scope the reports, and then click the report you want to run. You can scope reports by Client-Side Monitoring, Problem Analysis Reports, Resource Utilization analysis, or choose just one of the individual reports to view.

   You can also select a report by clicking on one of the report graphics.

4. Use the **Start Date** and **End Date** fields to select the time or date range for the alerts you want included in the reports.
5. Click the **Status** text box to filter alerts by those that are New, Reviewed, Deleted, or By Design.

   Tip
   Viewing alerts categorized as By Design can show you if the way an application is designed is actually causing issues.

6. Click **Source** dropdown menu to select the application component you want to include in the report.

   Note
   Only applications that are part of the application group you initially selected are available to be used as a source.

7. Click the **Computer** dropdown menu to select which computer or computers you want reported on.
8. In the **Problem** dropdown menu, you can filter by all problems detected or only critical problems.
9. Click **Apply** to save this report configuration and run the report.

To add an Application Advisor report to Favorites

1. If you want to save a report with certain scoped information that you can easily view later, add it to your Favorites list. In the **Select report** menu or by clicking the report graphic, select the report you want to run.

   Note
   You can scope the information you want included in the report before making it a favorite or create the scoping information in the Favorite Management Wizard.
2. In the **Results** pane, to open the Favorite Management Wizard, click the Favorites icon.
3. In the Favorite Management Wizard, you can either keep the settings you used to scope the information to be included in your report, reset them, or set them for the first time.
4. As you make or confirm your scoping settings, click **Next** to proceed through the wizard settings pages, and then click **Finish**.
5. In the Favorites namespace, click **Favorites** and you will be able to view the report you just configured.
6. To view a report in your Favorites, just click the report you want to view.

Example: To Prioritize Alerts by Using the Problems Distribution Analysis Report

A first step in working with application monitoring alerts is to try to see which ones you should address first to have the greatest impact on the applications in your environment. This is the role of Application Advisor—to identify the applications causing the most alerts and to see the types of alerts being raised. This introduces a proactive approach to managing application health because you are smartly addressing the most problematic areas of your applications and not merely reacting to alerts as they arrive.

To show how Application Advisor prioritizes alerts, this walkthrough uses a report that is helpful when first investigating application issues: the Problems Distribution Analysis report. This report shows the distribution of application failure, performance, connectivity, and security problems across all monitored applications—and highlights the applications that are the most problematic. For the applications that contributed to the majority of problems, this report provides more details by showing application components and external dependencies that are the root cause of those problems.

To interpret key elements of the Problems Distribution Analysis Report

1. Following the procedure to scope and run an Application Advisor report, choose the information you want to include in the report, and then click **Apply** to run the report.
2. Here there are three views that will show top issues:
   - To view only performance problems and top performance events for the applications, click **Summary Performance Analysis**.

- To view only exceptions and top exception events for the applications, click the **Summary Failure Analysis** link.
- You can view all problem types and top problems for the individual application, in the **Overall Source Statistics** section. This section shows you what percentage of performance and exception events are being raised by the application resources, such as function calls or database queries.

3. Click the first link in whichever view you want to investigate. This first link shows the highest cause of alerts and launches a list of all problems related to that application or source.

   Important
   This is the stage where you shift from a prioritized list to investigating individual alerts related to the most important issue. None of the events in this list is more important than another, but each can help highlight the route cause.

4. Click a link in **Event Description** and the Application Diagnostics Event Properties page opens. Here you are viewing data about the event itself. And this is the place to start troubleshooting. See Working with Events by Using Application Diagnostics for more information.

   Beginning with Event properties tab, use this and other tabs to discover more about what happened, whether it was likely a system issue as shown by performance data, and what application tier the problem occurred in, using distributed chains. Following this information should reveal if it was a system problem or an application code problem, and thus who should resolve the issue.

See Also

Working with the Application Diagnostics Console

Working with Events by Using Application Diagnostics

User Roles for Application Performance Monitoring

.NET Application Performance Monitoring Tasks and User Roles

This table shows the System Center 2012 – Operations Manager .NET Application Performance Monitoring tasks and the user roles with their permissions.

Legend:

- Yes = Can always use the feature

- No = Cannot use the feature unless the user also belongs to a group that grants access to functionality.

	Administrator	Author	Advanced Operator	Application Monitoring Operator	Operator	Read-Only Operator	Report Operator	Report Security Administrator
Run APM Wizard or change APM settings	Yes	No	No	No	No	No	No	No
Access Application Diagnostics	Yes	No	No	Yes	No	No	No	No
Access Application Advisor	Yes	No	No	Yes*	No	No	Yes*	Yes

Note
* The Application Monitoring Operator role and Report Operator role are both required to access Application Advisor.

How to Configure Grooming Settings for .NET Application Performance Monitoring Events

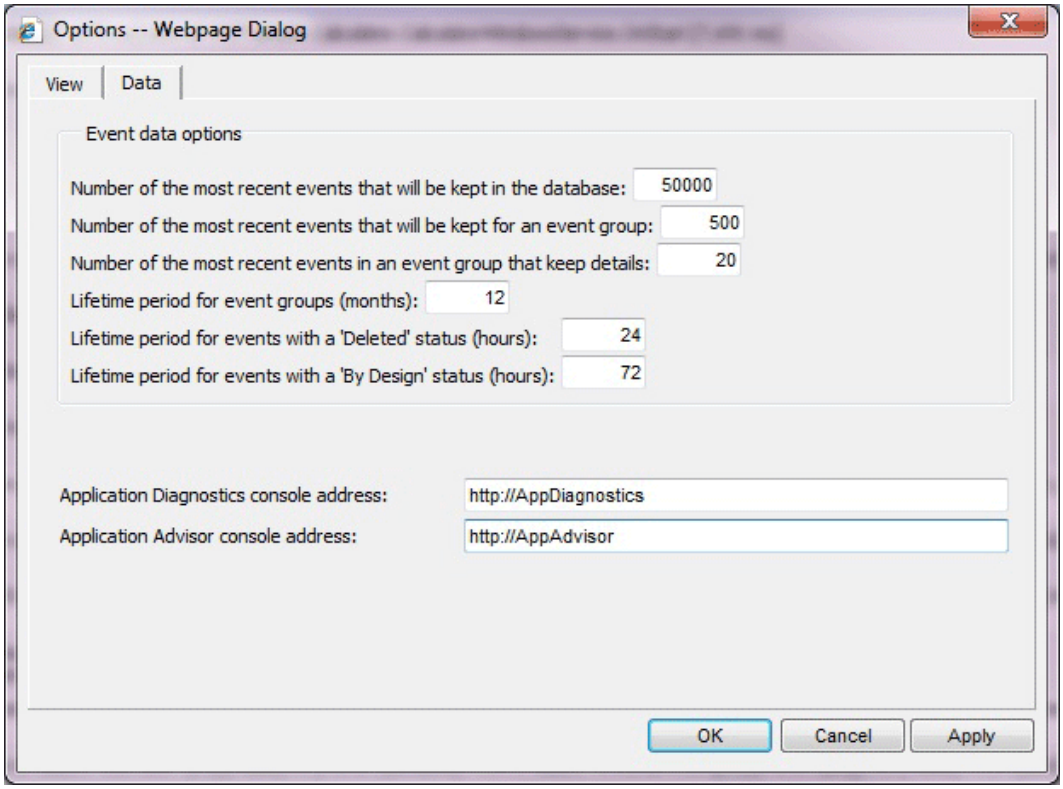
When you have been monitoring applications using .NET Application Performance Monitoring (APM), a new data type, APM events, will begin to take up space. Eventually, you will want to groom your database for APM events. Changing the grooming settings for your database for APM events requires the following procedures. You can groom APM events in three locations:

- In Application Diagnostics you can configure grooming settings for APM events in the Operations Manager Database
- In Application Advisor you can configure grooming settings for APM events in the Data Warehouse

- Using the Data Transfer rule, you can override parameters related to time-based APM event grooming in the Data Warehouse

Using Application Diagnostics to configure grooming settings for APM events in the Operations database

In Application Diagnostics you can select how many APM events you want in the Operations database and how long you want to keep them.



To use Application Diagnostics to configure grooming settings for APM events in the Operations database

1. Application Diagnostics is installed along with the Operations Manager web console. To find the web address of the Operations Manager web console, open the Operations console. In the navigation pane, click the **Administration** button, click **Settings**, and then double-click **Web Addresses**. The Operations Manager web console URL will be specified as: http(s)://<web host>/OperationsManager. Using this URL format and the same web host, the Application Diagnostics console address is: http(s)://<web host>/AppDiagnostics

   To open Application Diagnostics, paste the Application Diagnostics URL into your

browser. Application Diagnostics opens in the web browser window.

Note

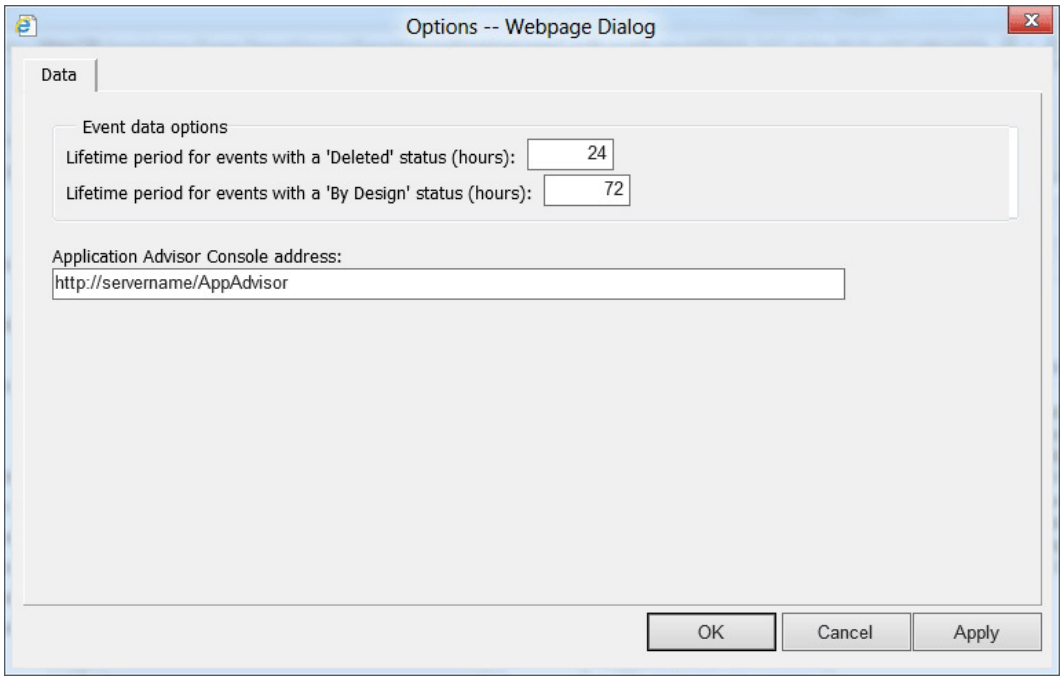
If you are running Operations Manager on a server rather than a client computer, you can access Application Diagnostics from the **Start** menu in **All Programs**.

Access to Application Diagnostics is controlled through the Application Monitoring Operator and Administrator roles. You must be a member of one of these roles to have rights to the console. For more information, see User Roles for Application Performance Monitoring

2. In Application Diagnostics, click **Tools**, select **Options**, and then click the **Data** tab.
3. Change the **Event data options** to define how you want to groom the database, and then click **OK**.

Using Application Advisor to configure grooming settings for “Deleted” or “By Design” APM events in Data Warehouse

In Application Advisor you can choose the how long you want to keep APM events that have a Deleted or By Design status in Data Warehouse.



To use Application Advisor to configure grooming settings for APM events in Data Warehouse

1. Application Advisor is installed along with the Operations Manager web console. To find

the web address of the Operations Manager web console, open the Operations console. In the navigation pane, click the **Administration** button, click **Settings**, and then double-click **Web Addresses**. The Operations Manager web console URL will be specified as: http(s)://<web host>/OperationsManager. Using this URL format and the same web host, the Application Advisor console address is: http(s)://<web host>/AppAdvisor

To open Application Advisor, paste the Application Advisor URL into your browser. Application Advisor opens in the web browser window. Different application monitoring reports display in the context of the application features and services you configured when you created application groups to monitor.

Access to Application Advisor is controlled through the Application Monitoring Operator, Report Operator and Administrator roles. You must be a member of Application Monitoring Operator and Report Operator roles or the Administrator role. For more information, see User Roles for Application Performance Monitoring

Note
Application Advisor requires SQL Server Report Services (SSRS). You must have Operations Manager reporting installed before using Application Advisor.

2. In Application Advisor, click **Tools**, select **Options**, and then click the **Data** tab.
3. Change the **Event data options** to define how you want to groom the database, and then click **OK**.

Using the Data Transfer rule to configure grooming settings for APM events and performance data from the Data Warehouse

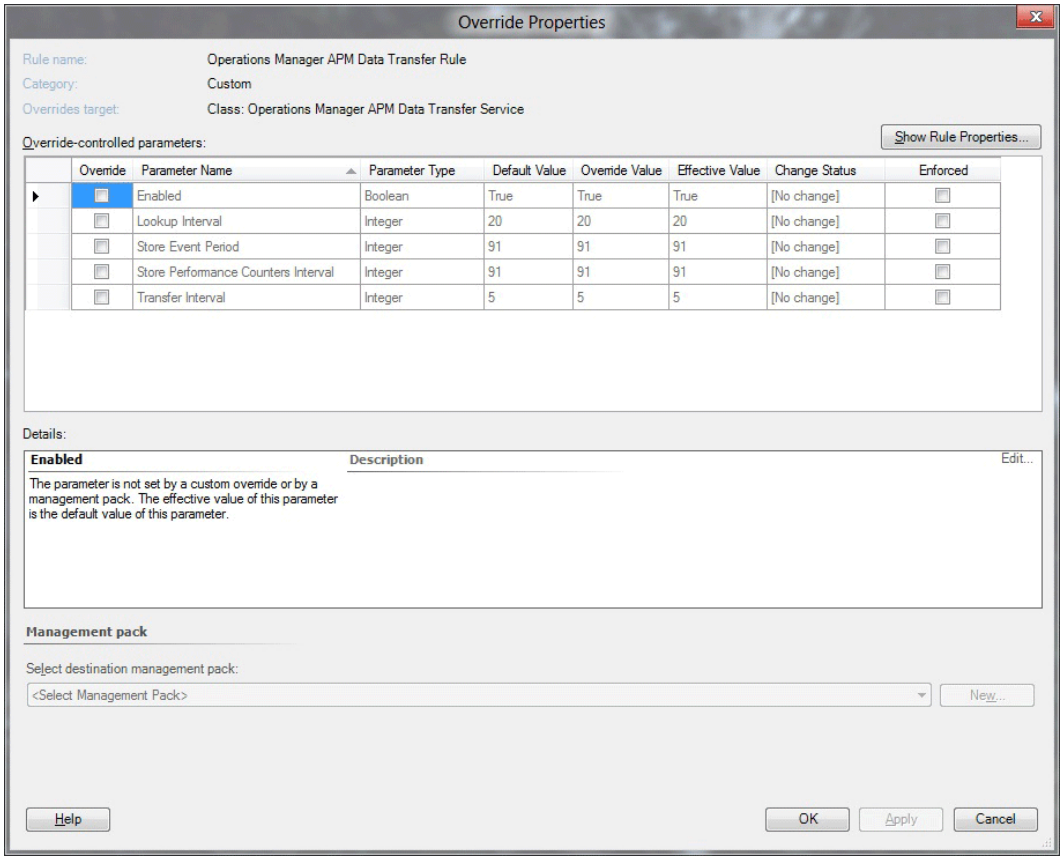
The Data Transfer rule lets you override time-based grooming for the Data Warehouse. This rule triggers the Data Transfer, Aggregation, and Grooming activities related to APM events on the Operations or Data Warehouse databases. It provides overrides control to the retention settings for APM events in the Data Warehouse database.

Warning
Disabling this rule or overriding any other setting will have an adverse negative impact on the overall health, functionality, and consistency of the APM feature, the Data Warehouse, and Application Advisor reports, among other things.

The Operations Manager APM Data Transfer Rule is targeted to the Operations Manager APM Data Transfer Service object and has two overrides for those settings: for events and for counters. The setting for Events applies to events that had not been previously marked as “Deleted” or “By Design”, for which grooming is controlled by Advisor, as described in the previous paragraph. If events have been left in status “New”, then they will be retained in the Data Warehouse for as many days as this setting indicates.

The Performance Counter setting is intended for hourly performance aggregations, which potentially can take a lot of space. There is no configurable setting for daily performance

aggregations. The default for this is 182. Typically, daily aggregations consume a lot less disk space.



To use the Data Transfer Rule to configure grooming settings for APM events in the Data Warehouse

1. In the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Objects**.
2. Click **Rules**, click **Change Scope**, click **View All Targets**, search for **Operations Manager APM Data Transfer Service**, and then click **OK**.
3. Right-click and select **Overrides**, select **Override the Rule**, and then select **For all objects of class**. You see the **Override Properties** page.
4. On the **Override Properties** page, make your changes to **Store Event Period** and **Store Performance Counters Interval**, and then click **OK**.

   Store Event Period lets you determine how many days you want to keep APM events. Store Performance Counters Interval lets you determine how many days of performance counters you want to keep in Data Warehouse.

See Also

How to Configure Grooming Settings for the Operations Manager Database

How to Configure Grooming Settings for the Reporting Data Warehouse Database

Working with Sensitive Data for .NET Applications

Here are some ways to work with sensitive data and .NET Application Performance Monitoring in System Center 2012 – Operations Manager.

Masking Sensitive Data for .NET Applications

Masking sensitive data allows you to use a regular expression to filter out common parameters and insert ***** or some other character in place of the real value. This is used for functions and exceptions where you might capture sensitive information, such as credit card information, passwords, and other personally identifiable information.

To mask sensitive data for .NET applications

1. To open the .NET Application Performance Monitoring template, in the Operations Manager console, in the navigation pane, click the **Authoring** button, expand **Management Pack Objects**, click **Rules**, and then click **change scope** in the right-hand side of the information bar to see the current scoping.
2. In the **Scope Management Packs objects** page, select **.NET Application Monitoring Agent** to the current scope, and click **OK**.
3. To override the **Sensitive Data Rules** property of the **Apply APM Agent Configuration** rule, right-click **Apply APM Agent configuration**, select **Overrides**, select **Override the Rule**, and then select **For all objects of class: .NET Application Monitoring Agent**.
4. On the **Override Properties** page, in the **Override-controlled parameters** section, select **Sensitive data rules**.
5. In the **Sensitive data rules** row, in the **Override Value** column, enter the formula for the mask you want to apply, using the syntax `<Hidden><Expression>((pwd|password)=?)[^;]*</Expression><CompareExpression>((pwd|password)=?)[^;]*</CompareExpression><Replacement>$1*****</Replacement><Type>all</Type></Hidden>`, where the <Expression> and <CompareExpression> use regular expression syntax and <Replacement> defines the characters to use when masking out the actual value of the parameter.
6. In the **Management Pack** section, select an existing management pack or create a new one where the override will be stored.
7. Click **OK**.

Avoid Collecting Sensitive Data

If you do not want to get this sensitive information at all, here is how to avoid it. Some applications will pass sensitive information embedded in the exceptions raised or parameters collected. To avoid the sensitive information, you can disable monitoring for specific methods and restrict collection of specific exceptions. To do this, you disable parameter collection of a method or you disable collection of exceptions thrown from specific namespaces or classes.

To disable parameter collection of a method

1. To open the .NET Application Performance Monitoring template, in the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Templates**, click **.NET Application Performance Monitoring**, right-click the application group you want to modify, and then click **Properties**.
2. On the **What to Monitor** tab, select the application component you want to change and click **Customize**.

   Note
   Methods can also be defined at the application group level and be applied to all application components. To do this, follow the same steps after clicking the **Advanced Settings** button on the **Server-Side Defaults** tab.
3. On the **Modifying Settings** page, click **Set Methods**. Specify the method name for the function where you want to disable parameter collection, and then clear the **Collect function parameters** checkbox.

   Additionally, if you do not want to continue monitoring this method, clear the **Enable monitoring** checkbox.
4. Click **OK**.

To disable collection of exceptions

1. To open the .NET Application Performance Monitoring template, in the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Templates**, click **.NET Application Performance Monitoring**, right-click the application group you want to modify, and then click **Properties**.
2. On the **Server-Side Defaults** tab, click **Advanced Settings**.
3. On the **Advanced settings** page, click **Exception Tracking**.
4. On the **Exception tracking list** page, click **Add**, enter the namespace or class where you want to stop collecting exceptions, and then clear the **Enable monitoring** checkbox.
5. Click **OK**.

See Also

Operations Manager Privacy Statement

Notes for AVIcode 5.7 Customers

System Center 2012 – Operations Manager includes application monitoring. The major difference is that AVIcode 5.7 required you to deploy a separate infrastructure alongside Operations Manager. Now these infrastructures have been combined, so you don't need to install anything.

Note

Now that System Center 2012 is generally available as of April 17, 2012, AVIcode 5.7 will no longer be available as a standalone product from the Microsoft AVIcode subsidiary. AVIcode 5.7 support will continue for 12 months following general availability of System Center 2012. If certain customers already have existing support agreements with other support terms, those agreements will be honored until they expire. When the support for AVIcode 5.7 ends, the Microsoft AVIcode subsidiary will no longer provide new updates or hotfixes for AVIcode 5.7 and we will encourage customers to move to System Center 2012, which will be supported as described in the Microsoft Support Lifecycle Policy FAQ

If you are running AVIcode 5.7 to monitor applications and install Operations Manager, servers that have AVIcode 5.7 agents installed will continue to work in the same way they were doing before since only Operations Manager has been upgraded. NET Application Performance Monitoring configuration will not affect the AVIcode 5.7 agents because they will not receive it. If you have legacy applications monitored by AVIcode 5.7 (IIS6, .NET services, SharePoint 2007, for example), you can continue to monitor them with AVIcode 5.7. You can begin using .NET Application Performance Monitoring on new servers where AVIcode 5.7 has not been installed or was removed.

Converting AVIcode 5.7 Monitoring to .NET Application Performance Monitoring

As a legacy product, AVIcode 5.7 will receive very limited updates. Future technologies will only be added to .NET Application Performance Monitoring in Operations Manager.

When you are ready to move from using AVIcode 5.7 to .NET Application Performance Monitoring to monitor applications (for example, when AVIcode 5.7 is monitoring IIS7 already or when Windows is upgraded), you can:

- Uninstall AVIcode 5.7 agent from that computer.
- Repair install the Operations Manager agent, which will install the Application Performance Monitoring service.
- Manually reconfigure .NET Application Performance Monitoring for the application running on IIS7 with similar settings that you were using previously with AVIcode 5.7. For more information, see .NET Application Performance Monitoring Template.

Continuing to Use AVIcode 5.7 with System Center 2012 – Operations Manager

Features of AVIcode 5.7 and .NET Application Performance Monitoring can generally co-exist, but some cannot. For example, the AVIcode 5.7 SEViewer and the new Application Diagnostics cannot be installed on the same system. You can use both consoles in the same environment, but they must be installed on separate IIS hosts.

When monitoring applications using both AVIcode 5.7 and .NET Application Performance Monitoring in Operations Manager, data is shown in the respective monitoring views. For AVIcode 5.7, data continues to flow through SELog and SEViewer. For .NET Application Performance Monitoring in Operations Manager, monitoring data is viewed in Application Diagnostics.

Supported AVIcode Versions

Only AVIcode 5.7 when integrated with Operations Manager 2007 R2 with the latest cumulative updates is supported. Previous AVIcode versions are not supported. AVIcode 5.7 functionality has not been enhanced. The AVIcode 5.7 configurations you have been using to monitor applications have not been converted to .NET Application Performance Monitoring configurations. When upgrading from Operations Manager 2007 R2 to System Center 2012 – Operations Manager, you need to manually import new AVIcode 5.7 management packs. For more information, see Steps to import AVIcode 5.7 templates after upgrading.

How Upgrade Works with AVIcode 5.7 Agents and .NET Application Performance Monitoring Agents

Upgrading to Operations Manager behaves this way:

- Upgrading to Operations Manager is not blocked because AVIcode 5.7 agents are present. When an Operations Manager 2007 R2 agent and an AVIcode 5.7 agent are found, the upgrade to Operations Manager proceeds, but the .NET Application Performance Monitoring service is not installed. The AVIcode 5.7 service is left instead.

  Important
  You cannot have the AVIcode 5.7 service installed on the management servers. In this case, you will need to remove the AVIcode 5.7 service before upgrading.

- When Operations Manager 2007 R2 agents are found without AVIcode 5.7 on the system, the upgrade to Operations Manager proceeds and the .NET Application Performance Monitoring agent is installed.
- If .NET Application Performance Monitoring has already been deployed and you try to install AVIcode 5.7 on it, this is blocked through the push install. If you manually force it, you could succeed, but the agents will conflict with one another and neither will work correctly. There it is a monitor that targets activated Application Performance Monitoring agents that will put the agent into a warning state if both the AVIcode 5.7 and the Operations Manager Application Performance Monitoring agents are on the same server.

- If you are using AVIcode 5.7 and do not want to install .NET Application Performance Monitoring on your agent-managed computers, use the /NOAPM=1 agent manual install command line switch to prevent .NET Application Performance Monitoring from being installed. This leaves the AVIcode agent in place. For more information, see Install Agent Using the Command Line.

Note

There is a monitor named AVIcode Intercept Service found that targets the Agent class in System Center 2012 – Operations Manager that is disabled by default, but can be enabled to monitor for the AVIcode agents on systems where the Operations Manager agent is present alongside the AVIcode 5.7 service.

Manually Importing AVIcode 5.7 Management Packs

When the AVIcode.NET Enterprise Management Pack for Operations Manager 2007 is present in the management group, Setup will continue, but some management packs will need to be manually upgraded after setup has finished fixing incompatibilities with Operations Manager. The management pack files are in the /SupportTools directory on the Operations Manager media. They are not imported automatically.

The management packs that need to be imported are:

- AVIcode.DotNet.SystemCenter.Enterprise.Monitoring.mpb
- AVIcode.DotNet.SystemCenter.Client.Monitoring.mp

Monitoring Java Applications

Java Application Performance Monitoring (APM) in System Center 2012 R2 Operations Manager lets you monitor Java applications to get details about application performance and exception events that can help you determine the root causes of problems. The System Center 2012 Management Pack for Java Application Performance Monitoring lets you monitor Java application performance and exception events by using Operations Manager Application Advisor. With Operations Manager Application Advisor, you can investigate method and resource timing for performance events, stack traces for exception events, Java specific counters for events (such as Average Request Time, Requests Per Second, JVM Memory, and Class Loader), and run some of the standard Application Performance Monitoring reports. Additionally, you get Operations Manager level alerting on Java application server counters. Download the Management Pack for Java Application Performance Monitoring from the Microsoft Download Center.

Java Application Performance Monitoring shares many concepts with .NET Application Performance Monitoring. However, there are some important differences, including: object hierarchy, the method for working with overrides and alerting (Java Application Performance Monitoring has no authoring and configuration template, so you change configurations with management pack overrides), and sever-level information is not handled in Java Application Performance Monitoring reports.

Supported Configurations

The Management Pack for Java Application Performance Monitoring requires Windows Server 2012 R2, System Center 2012 R2 Operations Manager, and System Center 2012 R2.

Supported configurations:

- Tomcat 5, Tomcat 6, and Tomcat 7
  - Windows
  - Linux
- Java JDK 5, Java JDK 6
- Web Technologies
  - GenericServlet
  - Struts
  - Struts2
  - Axis2

Prerequisites

To run the Management Pack for Java Application Performance Monitoring, you must have the Management Pack for Java Enterprise Edition (JEE) configured for deep monitoring. This management pack monitors JEE application servers and provides initial application level discovery. For more information, see How to Configure Monitoring for Java Applications and the Management Pack Guide for JEE for your particular type of application server, available on the Microsoft Download Center.

Java Application Performance Monitoring Topics

- How to Configure Monitoring for Java Applications
- How to Monitor Java Applications
- Strategies for Monitoring a New Java Application

How to Configure Monitoring for Java Applications

Getting started with monitoring Java applications requires these four general steps:

1. Import and configure the Management Pack for Java Enterprise Edition (JEE) through the deep monitoring steps
2. Import the Management Pack for Java Application Performance Monitoring
3. Manually deploy the Java Application Performance Monitoring Agent
4. Verify the Java Application Performance Monitoring Agent deployment

To import and configure the Management Pack for Java Enterprise Edition through deep monitoring

1. Import and configure the Management Pack for Java Enterprise Edition (JEE) through deep monitoring, including installation of BeanSpy application. This is a requirement. Java Application Performance Monitoring will not work without JEE deep monitoring configured and BeanSpy installed.

   Important
   Although the Management Pack for JEE supports several types of application servers, Java Application Monitoring only supports Tomcat.

   Download the Management Pack for JEE and the Management Pack Guide for JEE. This management pack monitors JEE application servers and is available for IBM WebSphere, Oracle WebLogic, Red Hat JBoss, and Apache Tomcat. Go to the System Center Management Pack for Java Enterprise Edition (JEE) on the Microsoft Download Center, click **Download**, and then select the files you want to download. For example, select the management pack (SC2012OM_JEE_MP.msi) and select the Management Pack Guide for Tomcat (OpsMgr_MP_Tomcat.docx).

   Important
   Make sure to download the corresponding management pack guide (.docx file) for the application server you are using. It contains the details of how to install the management pack and describes what is monitored.

   The System Center Management Pack for Tomcat, for example, allows an IT administrator to monitor the health of JEE application server instances in Operations Manager. In addition, it provides the option to deploy BeanSpy, an open source technology from Microsoft, that provides deeper monitoring, which includes memory usage.
2. After the management packs for the JEE application servers are imported, the instances of Tomcat application servers will be automatically discovered. The discovery interval is set to 4 hours by default, so discovery can take up to that length of time. On Tomcat, an application server must be running for Operations Manager to discover it for the first time. After an instance of an application is discovered, the configuration is removed only when the application server is uninstalled.

   To monitor instances of the Tomcat Application Server, in the Operations console, click **Monitoring**, expand **Application Monitoring**, **expand Java Monitoring**, expand **JEE Application Servers**, expand **Tomcat Application Server**, and then select the monitoring folder you want. For details, see the Management Pack Guide for Tomcat or the management pack guide for JEE monitoring that you chose to download.
3. Follow the procedure to deploy BeanSpy to an application server. BeanSpy is an open source technology from Microsoft that relies on Java Management Extension (JMX) to enable the monitoring pack to get detailed information from the application server instances.
4. Using instructions in the Management Pack Guide for JEE, follow the procedure to

enable deep monitoring mode.

To import the Management Pack for Java Application Performance Monitoring

1. Now that the Management Pack for Java Enterprise Edition is imported and configured through deep monitoring and BeanSpy deployed, import the Management Pack for Java Application Performance Monitoring. Download the management pack from the Microsoft Download Center.
2. The Management Pack for Java Application Performance Monitoring (JavaAPMManagementPack.msi) contains these files:
   - Microsoft.JEE.APM.Library.mpb
   - Microsoft.JEE.Tomcat.APM.Library.mp
   - Microsoft.JEE.Tomcat.5.Apm.mp
   - Microsoft.JEE.Tomcat.6.Apm.mp
   - Microsoft.JEE.Tomcat.7.Apm.mp

   Import these library management packs:
   - Microsoft.JEE.APM.Library.mpb
   - Microsoft.JEE.Tomcat.APM.Library.mp
3. Import the management packs for the versions of the Tomcat application servers that you are monitoring.
   - Microsoft.JEE.Tomcat.5.Apm.mp
   - Microsoft.JEE.Tomcat.6.Apm.mp
   - Microsoft.JEE.Tomcat.7.Apm.mp

To manually deploy the Java Application Performance Monitoring Agent and enable Java Application Performance Monitoring

1. Now that you have configured the Management Pack for Java Enterprise Edition (JEE) through deep monitoring and imported the Management Pack for Java Application Performance Monitoring, you are ready to manually deploy the Java Application Performance Monitoring agent. To see application servers you have configured for monitoring, in **Monitoring**, click **Configurations**.
2. To enable Java Application Performance Monitoring, in the **Monitoring** pane, in the **Tasks** pane, click **Deep Monitored Configurations**, and then select a deep monitoring application server.
3. After you select an application server to enable Java Application Performance Monitoring on, in the **Tasks** pane, in **Monitored application server instance Tasks**, click **Extract APM Jar files**. This extracts the Java agent files to either the monitored machine (when a server is running Windows), or to the gateway or management server (when a server is running Linux). The Task output tells you which machine the files have been extracted to and where they were extracted. For more information, see the Management Pack Guide for Java Application Performance Monitoring available from the Microsoft Download Center.
4. Next, reconfigure the Java application server. To enable Java Application Performance

Monitoring, specify command line options that use Jar file as class loader and then restart the application. Another discovery after you install the agent enables Application Performance Monitoring.

To verify Application Performance Monitoring agent deployment and override monitors

1. To verify if Application Performance Monitoring is monitoring an application, right click an application and you can see a list of counters: Monitored Requests/sec, Average Request Time, Performance Events/sec, Exception Events/sec, and, importantly, values for each counter. Five monitors apply to these. For more information about monitors, see the Management Pack Guide for Java Application Performance Monitoring, available from the Microsoft Download Center.

   Important
   If you do not see values for the counters, Application Performance Monitoring is not enabled for these applications. This means that you might need to wait for Application Performance Monitoring discovery.

2. To see monitors, in Health Explorer, right-click an application, click **Open**, and then click **Performance View**. Some monitors some are disabled.
3. To override monitors, in Health Explorer, right-click a monitor and click **Monitor properties**. On the monitor's **Properties page**, click **Overrides** tab, click **Override** and then select the rule you want to override. On the **Override Properties page** you can enable/disable monitors and change the monitor threshold settings.

To view events using Application Diagnostics

1. Like .NET Application Performance Monitoring, you can use Application Diagnostics to view event information for Java Application Performance Monitoring. For information about opening and using Application Diagnostics, see Working with the Application Diagnostics Console and Working with Events by Using Application Diagnostics.

   Due to the way Java statistics are reported, some of the standard Application Performance Monitoring reports do not apply to Java Application Performance Monitoring. For instance, you might see **NA** in some of the report columns where Java Application Performance Monitoring does not apply. Additionally, due to the way that Java application containers map to servers, many server-level reports do not have data.

See Also

How to Monitor Java Applications

Strategies for Monitoring a New Java Application

Monitoring .NET Applications

How to Monitor Java Applications

When you have a new Java application that you are learning about, you use Java Application Performance Monitoring to get baseline measures before you gradually scale up deployment. Here are some settings to start with that will help you get to know your new application. In addition, it is ideal that you begin monitoring in a test or development environment.

Monitoring Settings for a New Application

Following this strategy for monitoring a new Java application will help you get to know how the application behaves within your system and for your customer.

Start Monitoring with a Simple Monitored System and Short-Term Settings

First, keep the configuration simple: monitor one application on one server. Second, when you first configure Java Application Performance Monitoring to monitor a new application, plan to keep the settings you implement long enough for you to understand some trends. A day's worth of data should provide you with insight into the performance and usage patterns of the application.

Establish Baseline Performance Using Default Settings and Some Specific Settings

For the most part, you will want to keep default settings. The default settings ensure that you will see any large issues with the application and keep the impact on the monitored application at a minimum.

If you are not getting any performance or exception events raised, you can use the following steps to get a feel for what the baseline performance looks like.

To begin monitoring, here are some settings you might want to adjust as noted here:

- Lower the thresholds for performance. This will help you establish a baseline performance measure by seeing what the current performance characteristics of the application are. For more information about performance thresholds, see How to Configure Monitoring for Java Applications.
- Examine all exceptions. You need to know what kinds of exceptions are being thrown. Using known exception handlers limits the exceptions you will receive.

This can result in a lot of data—more than you would want for long-term monitoring—but at first, this amount of data will be helpful as you will see trends, such as the kinds of paths customers are taking through the system and what normal performance looks like.

With the data collection complete, use the Application Advisor reports, such as Application Performance Analysis, to see how the monitored applications are looking. Using the report you will see what the average duration is for the heaviest (longest running) calls through the system

as well as the maximum amount of time spent processing requests. This allows you to set customized smart thresholds based on real application performance. You will also see which functions are running faster than others, and you can create specific web page, web method, and function transactions for the critical methods so that you can ensure they are responding under a tighter SLA than the application as a whole. For more information on viewing reports, see how to scope and run an Application Advisor report in Prioritizing Alerts by Using Application Advisor.

Adjust Settings and Compare to the Baseline

Once you have established a baseline performance measure, begin to adjust the settings to tune the monitoring so it catches the kinds of exceptions that are being raised. By reporting all exceptions, you will see if there are any default exception handlers in the application that are catching exceptions for which you would prefer receiving alerts. The data you get will be more meaningful and lower in volume with each adjustment.

- Remove the custom settings and set thresholds based on the data collected.
- Add exception handlers for any application level “catch all” handlers that keep exceptions from going outside the application.
- Add specialized transactions to monitor the performance of common methods that should be held to a stronger SLA than the application as a whole.

Compare the new data to your baseline. You will begin to see the real average response time, for instance. Now that you know the various performance exceptions the application is sending, you can add the specific namespaces you want rather than monitoring all namespaces. Your application will be configured to be monitored based on the observed performance levels and will be alerted if things move outside of normal levels.

Gradually Deploy the Application to More Monitored Servers in Your System

After monitoring the application for a time with the new monitoring configuration, when you feel your application is healthy, increase the number of servers you are running the application on and monitoring from one to 10, for example. Once you have it running healthy at that level, increase the deployment and monitoring to more servers, and so on. This gradual rollout approach will help you gain confidence in the monitoring for that application and help ensure the health of your system.

What the Operator can do with This Information

Using this basic information, the operator can have a better idea where the problem is with the application or with the infrastructure and know whether it is something only to the development team can fix or the operator can address directly.

See Also

How to Configure Monitoring for Java Applications

Strategies for Monitoring a New Java Application
Monitoring .NET Applications

Strategies for Monitoring a New Java Application

Here are some scenarios and settings to change during authoring that can help you receive the monitoring experience and data that are most helpful for you.

Monitoring a New Application for which the Administrator has Little Knowledge

Accepting all defaults can be a good way to start monitoring an application for which the administrator has very little or no knowledge. Then, after monitoring with all defaults for some time, the administrator can begin adjusting settings based on the monitoring alerts, Application Diagnostics data, and Application Advisor reports. For more information, see How to Monitor Java Applications.

Limit Monitoring to a Specific Set of Servers

Defining a targeted group allows you to limit monitoring to a specific set of servers. For very large application deployments, you typically do not need to monitor all instances of the application. A representative sample is enough to get the data you need. Using only a representative sample will keep the amount of data collected and stored lower.

Reduce the “Noise” by Defining How Much Data You Collect

Increasing the sensitivity threshold allows you to filter out fast-running methods, which reduces overall “noise”, or how deep the call stack is going to go, making it easier for you to determine where the problem is. It also reduces network bandwidth usage.

The sensitivity setting is used to determine if a function call should be included in the call stack. Any function that executes and returns faster than the sensitivity level is dropped, keeping small fast-running functions from hiding the actual problem. Remember that using sensitivity only reduces the number of functions shown in the call stack for specific events, but an event will still be generated if the overall threshold is surpassed.

You can adjust the sensitivity threshold in the configuration file as discussed in the Management Pack Guide for Java Application Performance Monitoring.

It is also possible for high sensitivity to hide problems. In the situation where you have a function that calls another function, if the callee’s response time increases even slightly, it might cause

issues for the application. For example, if you have a data processing function that calls a lookup function 1,000 times and the lookup's processing time increases by 1 ms, you will increase the response time for your top level function by a full second. This might be masked by the high sensitivity. When you find this kind of situation, you can add the callee as a method and set a custom sensitivity for it to ensure it is always measured according to the lower sensitivity threshold.

Application failure alerts are application, or code, failures that are detected within the application. You can choose not to receive application failure alerts, which will potentially occur very often if an application has problems because these kinds of alerts usually require code modifications to address. Turning this off reduces the "noise" of many alerts raised that cannot be directly resolved by the operations team.

See Also

How to Monitor Java Applications

How to Configure Monitoring for Java Applications

Monitoring .NET Applications

Fabric Monitoring

A close integration between System Center 2012 R2 Virtual Machine Manager and System Center 2012 R2 Operations Manager introduces System Center cloud monitoring of virtual layers for private cloud environments. The Management Pack for System Center 2012 - Virtual Machine Manager monitors availability of VMM and the availability, health, and performance of all virtual machines and virtual machine hosts that VMM manages. The Fabric Health Dashboard shows a detailed overview of the health of your private clouds and the fabric that services those clouds. The dashboard helps you answer questions like "What is the health of my clouds and the fabric serving those clouds?" and helps you understand how your fabric components are connected. At a glance, you can see cloud health and the health of the underlying fabric/virtual machines. You can also do root cause analysis by linking to existing dashboards, such as network monitoring dashboards and the Virtual Machine Manager diagram view can help you dive into network and storage monitoring.

To get the dashboard, use the System Center 2012 Management Pack for System Center 2012 R2 Virtual Machine Manager Fabric Health Dashboard, which is imported automatically when you integrate Operations Manager and Virtual Machine Manager.

What is the Fabric of a Private Cloud?

The fabric of a private cloud consists of physical and virtual elements that fall into three main categories: Compute, Storage, and Hardware.

- **Compute** includes hosts, operating systems/platforms that are running on the hosts, workloads (what's running on your private cloud, such as SQL, AD, DNS, DHCP), workload configuration, and management infrastructure.
- **Storage** includes file shares, LUNs, storage pools.
- **Hardware** includes physical and virtual network devices and networks, as well as fabric hardware.

Before You Begin

Virtual Machine Manager controls the private cloud. Before you can begin to monitor the fabric of your private clouds, you must integrate System Center 2012 R2 Operations Manager and Virtual Machine Manager. For details, see Configuring Operations Manager Integration with VMM. During the integration, several management packs are imported automatically, including the Management Pack for System Center 2012 - Virtual Machine Manager and the Management Pack for Virtual Machine Manager Fabric Health Dashboard.

The Management Pack for System Center 2012 - Virtual Machine Manager monitors availability of VMM and the availability, health, and performance of all virtual machines and virtual machine hosts that VMM manages. You must install this management pack before you can configure the following VMM features: Performance and Resource Optimization (PRO), Maintenance Mode integration, Reporting in VMM, and Support for SQL Server Analysis Services (SSAS).

The VMM management pack enables the integration of Operations Manager with VMM and monitors the health of virtual machines running on Microsoft Hyper-V, VMware ESX, and Citrix XenServer. In VMware vSphere 4 or VMware Infrastructure 3 (VI3) environments that are managed by using VMM, this management pack also monitors the health of virtual machines running on VMware ESX. For more information, see Guide for System Center Monitoring Pack for System Center 2012 - Virtual Machine Manager.

The VMM Fabric Health Dashboard management pack displays much of what the VMM management pack monitors into a dashboard view.

Fabric Monitoring Topics

- Getting Started with the Fabric Health Dashboard
- Scoping the Fabric Health Dashboard to a Specific Cloud and Investigating Details
- The Fabric Monitoring Diagram View: Displaying Health States of Cloud Environments
- Using System Center Advisor to Proactively Monitor Cloud Fabric

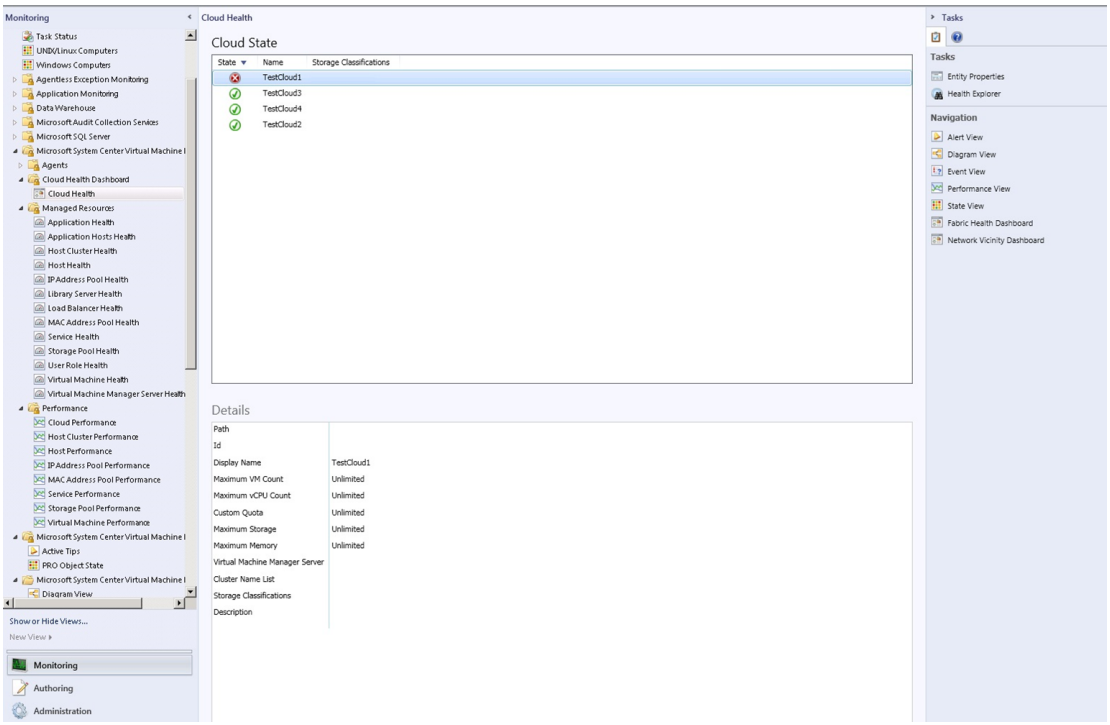
Getting Started with the Fabric Health Dashboard

The Fabric Health Dashboard shows a detailed overview of the health of your private clouds and the fabric that services them. The dashboard helps you answer questions like “What is the health of my clouds and the fabric serving those clouds?” You can see the overall cloud health, health across host, storage, and network components, active alerts related to that cloud, and drill down into other dashboards for views to help you resolve problems. Essentially, you can quickly see the fabric health of the components you care about and determine whether you have an urgent issue that needs fixing.

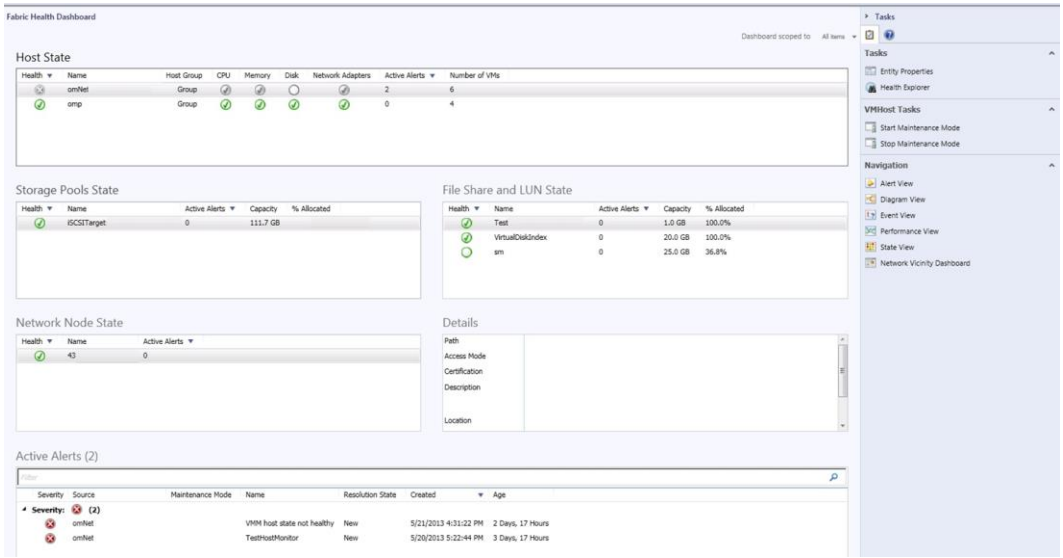
About the Fabric Health Dashboard

To view the Fabric Health Dashboard

1. Before you can begin to monitor the fabric of your private clouds, you must integrate System Center 2012 R2 Operations Manager and Virtual Machine Manager. For more information, see Configuring Operations Manager Integration with VMM. During the integration, the management pack for VMM Fabric Dashboard 2012 R2 is imported automatically.
2. To view the Fabric Health Dashboard, after you integrate System Center 2012 R2 Operations Manager and Virtual Machine Manager, click **Monitoring**, and in **Cloud Health Dashboard**, click **Cloud Health**.
3. In the **Cloud State** view, select the cloud you want to investigate.



4. In the **Tasks** pane, click **Fabric Health Dashboard**. From here, you get to other dashboards and other information to investigate issues across the areas that the Fabric Health Dashboard displays.



For each cloud, the Fabric Health Dashboard displays these aspects of the fabric:

- **Host State:** monitors the health state of the hosting groups or the computing aspects of the cloud, such as CPU, memory, disks, and network adapters

- **Storage Pools State File Share and LUN State:** monitors the health state of the storage aspect of fabric for issues, such as disk space capacity and allocation
- **Network Node State:** utilizes network monitoring in Operations Manager and displays the health state of network nodes (devices) that are relevant for the cloud you selected. Only physical network devices within one hop from the hosts are shown. To see the physical network devices, you must enable the Network Monitoring feature of Operations Manager and monitor the physical network devices connected to the hosts. Virtual networks are not shown in the dashboard.

The **Active Alerts** and **Number of VMs** fields on this dashboard help indicate which issues are having the greatest impact on your cloud and can help you prioritize your work.

Scoping the Fabric Health Dashboard to a Specific Cloud and Investigating Details

Using the Fabric Health Dashboard, you can see the overall cloud health and the health of its underlying fabric, but you can also use the Fabric Health Dashboard see the fabric health of any cloud you select. When you scope the dashboard to a particular cloud in the **Cloud State** view, the Fabric Health Dashboard you see a grouping of all of the components that are relevant for that cloud only. When you see a health issue with one component, you can then drill down to investigate a single component in terms of that cloud only. In this way, a fabric administrator can do root cause analysis by digging deeper into an issue, which can lead to other dashboard views, such as the network monitoring dashboard.

Looking at the Health Cloud by Cloud

To scope to a particular cloud

1. In the Operations Manager console, click **Monitoring**, expand **Cloud Health Dashboard**, click **Cloud Health**, and you see the private clouds you are monitoring in the **Cloud State** pane.
2. Select the cloud you want to investigate, then, in the **Tasks** pane, click **Fabric Health Dashboard**.
3. The Fabric Health Dashboard shows only what is related to the particular cloud you selected. You can see the health of each component, Host state, Storage, Networks, and active alerts. It displays a mixture of physical and virtual devices.

From the Fabric Health Dashboard for a particular cloud, you can investigate problems for each component of that particular cloud. In the Tasks pane, in Navagation, you can select from several views and a dashboard to get different information and insight about cloud health.

- **Alert View** shows active alerts related to the cloud.
- **Diagram View** shows a view of cloud health as a tree diagram that you can expand to drill down to the level where problems are occurring.

- **Event View** shows events related to the cloud.
- **Performance View** shows performance events related to the cloud.
- **State View** shows the state of the different parts of your cloud fabric.
- The **Network Vicinity Dashboard** shows information about your current network node in relation to other network nodes that it is attached to.

For example, if you saw a problem with the Network Node State, from the Fabric Health Dashboard, in the **Tasks** pane, click **Network Vicinity Dashboard**, and you can dig deeper into the problem of that particular cloud to see how this network node is affecting other network nodes that this one is attached to. It also places the network problem in context. The Network Node Dashboard shows the Vicinity view of nodes that are connected, an average availability, average response time, and details about the node. This is helpful when investigating particular deep diagnostic information about a networking device or processor use, go down deeper into the health of interfaces on this node.

The Fabric Monitoring Diagram View: Displaying Health States of Cloud Environments

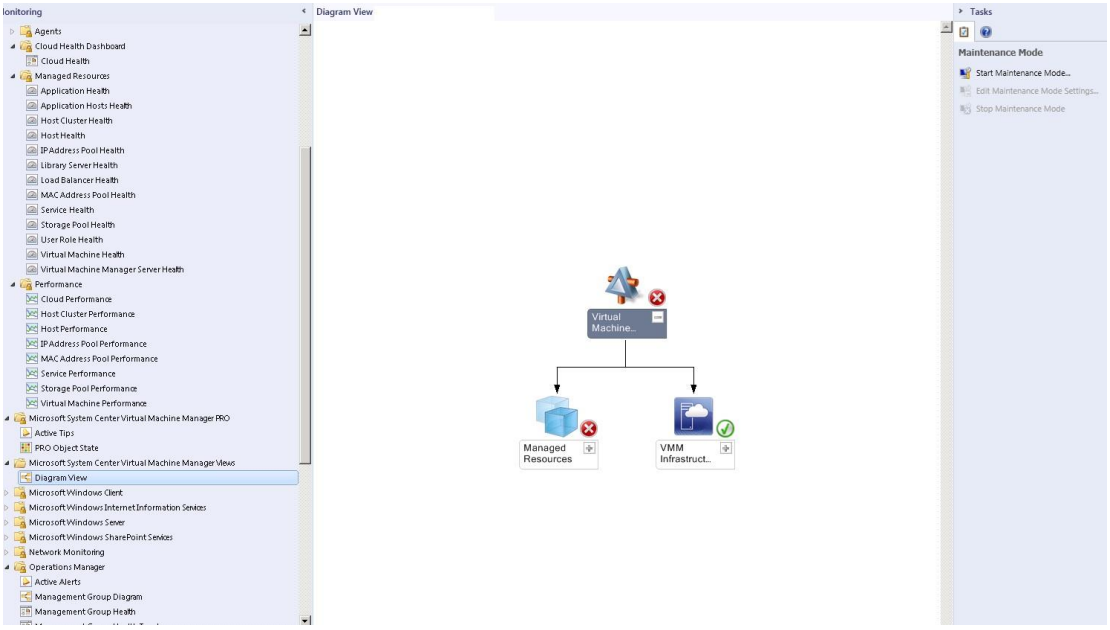
The Fabric Monitoring Diagram view gives you a diagram of the entire infrastructure and shows the health state of each part of the fabric. The Diagram view helps you answer questions, such as “What is the health of my entire fabric?” Improvements to the diagram ensure that health rolls up and that the relevant fabric components are part of the Diagram View.

Using Diagram View to Locate and Investigate Problems

To use Diagram View to locate and investigate problems

1. To open Diagram View, click **Monitoring**, and in **Microsoft System Center Virtual Machine Manager Views**, click **Diagram View** for the environment you want to see displayed as a diagram.

   Diagram View nodes show the health roll up, so if a node as healthy, you know that everything beneath is also healthy. Similarly, if a node is marked unhealthy, something in that node is having a problem.



2. To see where a problem is occurring, click a node that is marked as unhealthy and expand it until you begin to find unhealthy nodes within that tree. When you find the problem you want to investigate right-click the node and select **Health Explorer**.
3. In **Health Explorer**, click the monitor you want to investigate and you can see Knowledge and health for each monitor.
4. To see when and why a monitor became unhealthy, open **State Change Events**.

Using System Center Advisor to Proactively Monitor Cloud Fabric

Using System Center Advisor to Proactively Monitor Cloud Fabric

System Center Advisor is an online service that analyzes installations of Microsoft server software and covers fabric components. With the latest version of Advisor, you can now view Advisor alerts in the Operations Manager Operations console.

Advisor collects data from your installations, analyzes it, and generates alerts that identify potential issues (such as missing security patches) or deviations from identified best practices with regard to configuration and usage. Advisor also provides both current and historical views of the configuration of servers in your environment. Ultimately, Advisor recommendations help you proactively avoid configuration problems, reduce downtime, improve performance, and resolve

issues faster. For more information about Advisor, see Viewing System Center Advisor Alerts and Advisor online help

Monitoring UNIX and Linux Computers by Using Operations Manager

System Center 2012 – Operations Manager provides monitoring of UNIX and Linux computers similar to monitoring of Windows computers. You can monitor health, performance, obtain reports, run tasks, and implement needed customizations.

You can monitor the following aspects of UNIX and Linux computers:

- Services and applications
- File system, disk space, swap space, system memory
- Network interfaces
- Core processes and attributes
- Key configurations

Monitoring UNIX and Linux Computers by Using Operations Manager topics

- Supported UNIX and Linux Operating System Versions
- Using Templates for Additional Monitoring of UNIX and Linux
- Troubleshooting UNIX and Linux Monitoring
- Monitoring Linux Computers in Windows Azure by Using Operations Manager

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Initial Monitoring After Operations Manager Is Installed
- Managing Access in Operations Manager
- Getting Information from Operations Manager
- General Tasks in Operations Manager
- Maintenance of Operations Manager
- Operations Manager Report Authoring Guide
- Accessing UNIX and Linux Computers in Operations Manager
- Managing Discovery and Agents

Supported UNIX and Linux Operating System Versions

The following tables describe the required UNIX and Linux operating systems and package dependencies.

IBM AIX 5L 5.3

Required Package	Description	Minimum Version
OS version	Version of the operating system	AIX 5.3, Technology Level 6, Service Pack 5
xlC.rte	XL C/C++ Runtime	9.0.0.2
openssl.base	OpenSSL Libraries; Secure Network Communications Protocol	0.9.8.4

IBM AIX 6.1

Required Package	Description	Minimum Version
OS version	Version of operating system	AIX 6.1, any Technology Level and Service Pack
xlC.rte	XL C/C++ Runtime	9.0.0.5
OpenSSL/openssl.base	OpenSSL Libraries; Secure Network Communications Protocol	0.9.8.4

IBM AIX 7.1 (Power)

Required Package	Description	Minimum Version
OS version	Version of operating system	AIX 7.1, any Technology Level and Service Pack
xlC.rte	XL C/C++ Runtime	
OpenSSL/openssl.base	OpenSSL Libraries; Secure	

Required Package	Description	Minimum Version
	Network Communications Protocol	

HP-UX 11i v2 IA 64

Required Package	Description	Minimum Version
HPUXBaseOS	Base OS	B.11.23
HPUXBaseAux	HP-UX Base OS Auxiliary	B.11.23.0706
HPUXBaseAux.openssl	OpenSSL Libraries; Secure Network Communications Protocol	A.00.09.07l.003
PAM	Pluggable Authentication Modules	On HP-UX, PAM is part of the core operating system components. There are no other dependencies.

HP-UX 11i v2 PA-RISC

Required Package	Description	Minimum Version
HPUX11i-OE	HP-UX Foundation Operating Environment	B.11.23.0706
OS-Core.MinimumRuntime.CORE-SHLIBS	Compatible development tools libraries	B.11.23
HPUXBaseAux	HP-UX Base OS Auxiliary	B.11.23.0706
HPUXBaseAux.openssl	OpenSSL Libraries; Secure Network Communications Protocol	A.00.09.071.003
PAM	Pluggable Authentication Modules	On HP-UX, PAM is part of the core operating system components. There are no other dependencies.

HP-UX 11i v3 PA-RISC

Required Package	Description	Minimum Version
HPUX11i-OE	HP-UX Foundation Operating Environment	B.11.31.0709
OS-Core.MinimumRuntime.CORE2-SHLIBS	Specific IA emulator libraries	B.11.31
openssl/Openssl.openssl	OpenSSL Libraries; Secure Network Communications Protocol	A.00.09.08d.002
PAM	Pluggable Authentication Modules	On HP-UX, PAM is part of the core operating system components. There are no other dependencies.

HP-UX 11i v3 IA64

Required Package	Description	Minimum Version
HPUX11i-OE	HP-UX Foundation Operating Environment	B.11.31.0709
OS-Core.MinimumRuntime.CORE-SHLIBS	Specific IA development libraries	B.11.31
SysMgmtMin	Minimum Software Deployment Tools	B.11.31.0709
SysMgmtMin.openssl	OpenSSL Libraries; Secure Network Communications Protocol	A.00.09.08d.002
PAM	Pluggable Authentication Modules	On HP-UX, PAM is part of the core operating system components. There are no other dependencies.

Red Hat Enterprise Linux ES Release 4

Required Package	Description	Minimum Version
glibc	C Standard Libraries	2.3.4-2
Openssl	OpenSSL Libraries; Secure Network Communications Protocol	0.9.7a-43.1
PAM	Pluggable Authentication Modules	0.77-65.1

Red Hat Enterprise Linux Server release 5.1 (Tikanga)

Required Package	Description	Minimum Version
glibc	C Standard Libraries	2.5-12
Openssl	OpenSSL Libraries; Secure Network Communications Protocol	0.9.8b-8.3.el5
PAM	Pluggable Authentication Modules	0.99.6.2-3.14.el5

Red Hat Enterprise Linux Server release 6

Required Package	Description	Minimum Version
glibc	C Standard Libraries	2.12-1.7
Openssl	OpenSSL Libraries; Secure Network Communications Protocol	1.0.0-4
PAM	Pluggable Authentication Modules	1.1.1-4

Solaris 9 SPARC

Required Package	Description	Minimum Version
Required OS patch	PAM memory leak	112960-48
SUNWlibC	Sun Workshop Compilers Bundled libC	5.9,REV=2002.03.18
SUNWlibms	Forte Developer Bundled Shared libm	5.9,REV=2001.12.10
SMCosslg	OpenSSL Sun does not provide a version of OpenSSL for Solaris 9 SPARC. There is a version available from Sunfreeware.	0.9.7g
SUNWcsl	Core Solaris, (Shared Libs)	11.9.0,REV=2002.04.06.15.27

Solaris 10 SPARC

Required Package	Description	Minimum Version
Required OS patch	PAM memory leak	117463-05
SUNWlibC	Sun Workshop Compilers Bundled libC	5.10, REV=2004.12.22
SUNWlibms	Math & Microtasking Libraries (Usr)	5.10, REV=2004.11.23
SUNWlibmsr	Math & Microtasking Libraries (Root)	5.10, REV=2004.11.23
SUNWcslr	Core Solaris Libraries (Root)	11.10.0, REV=2005.01.21.15.53
SUNWcsl	Core Solaris Libraries (Root)	11.10.0, REV=2005.01.21.15.53
SUNWopenssl-libraries	SUNopenssl-libraries (Usr)	11.10.0,REV=2005.01.21.15.53
SUNWcsr	Core Solaris, (Root)	11.10.0, REV=2005.01.21.15.53

Solaris 10 x86

Required Package	Description	Minimum Version
Required OS patch	PAM memory leak	117464-04
SUNWlibC	Sun Workshop Compilers Bundled libC	5.10,REV=2004.12.20
SUNWlibmsr	Math & Microtasking Libraries (Root)	5.10, REV=2004.12.18
SUNWcsl	Core Solaris, (Shared Libs)	11.10.0,REV=2005.01.21.16.34
SUNWcslr	Core Solaris Libraries (Root)	11.10.0, REV=2005.01.21.16.34
SUNWopenssl-libraries	OpenSSL Libraries (Usr)	11.10.0, REV=2005.01.21.16.34
SUNWcsr	Core Solaris, (Root)	11.10.0,REV=2005.01.21.16.34

Solaris 11 SPARC

Required Package	Description	Minimum Version
SUNWlibC	Sun Workshop Compilers Bundled libC	5.11, REV=2011.04.11
SUNWlibmsr	Math & Microtasking Libraries (Root)	5.11, REV=2011.04.11
SUNWcslr	Core Solaris Libraries (Root)	11.11, REV=2009.11.11
SUNWcsl	Core Solaris, (Shared Libs)	11.11, REV=2009.11.11
SUNWcsr	Core Solaris, (Root)	11.11, REV=2009.11.11
SUNWopenssl-libraries	OpenSSL Libraries (Usr)	11.11.0,REV=2010.05.25.01.00

Solaris 11 x86

Required Package	Description	Minimum Version
SUNWlibC	Sun Workshop Compilers Bundled libC	5.11, REV=2011.04.11

Required Package	Description	Minimum Version
SUNWlibmsr	Math & Microtasking Libraries (Root)	5.11, REV=2011.04.11
SUNWcslr	Core Solaris Libraries (Root)	11.11, REV=2009.11.11
SUNWcsl	Core Solaris, (Shared Libs)	11.11, REV=2009.11.11
SUNWcsr	Core Solaris, (Root)	11.11, REV=2009.11.11
SUNWopenssl-libraries	OpenSSL Libraries (Usr)	11.11.0,REV=2010.05.25.01.00

Solaris UTF-8 Support

The Operations Manager agent requires Solaris UTF-8 code set conversion support under some circumstances. Consult the Solaris documentation for details on installing UTF-8 code set conversion support. The Operations Manager agent functions without UTF-8 support on Solaris, but unrecognized characters are translated to question mark (?) characters.

SUSE Linux Enterprise Server 9 (i586)

Required Package	Description	Minimum Version
Service Pack 4	SUSE Linux Enterprise Server 9	
OS Patch lib gcc-41.rpm	Standard shared library	41-4.1.2_20070115-0.6
OS Patch lib stdc++-41.rpm	Standard shared library	41-4.1.2_20070115-0.6
Openssl	OpenSSL Libraries; Secure Network Communications Protocol	0.9.7d-15.35
PAM	Pluggable Authentication Modules	0.77-221-11

SUSE Linux Enterprise Server 10 SP1 (i586)

Required Package	Description	Minimum Version
glibc-2.4-31.30	C Standard shared library	2.4-31.30

Required Package	Description	Minimum Version
OpenSSL	OpenSSL Libraries; Secure Network Communications Protocol	0.9.8a-18.15
PAM	Pluggable Authentication Modules	0.99.6.3-28.8

SUSE Linux Enterprise Server 11 (i586)

Required Package	Description	Minimum Version
glibc-2.9-13.2	C Standard shared library	2.9-13.2
PAM	Pluggable Authentication Modules	pam-1.0.2-20.1

Universal Linux (Debian package) Debian, Ubuntu Server

Required Package	Description	Minimum Version
libc6	C Standard shared library	2.3.6
OpenSSL	OpenSSL Libraries; Secure Network Communications Protocol	0.9.8 or 1.0
PAM	Pluggable Authentication Modules	0.79-3

Universal Linux (RPM package) CentOS, Oracle Linux

Required Package	Description	Minimum Version
glibc	C Standard shared library	2.5-12
OpenSSL	OpenSSL Libraries; Secure Network Communications	0.9.8 or 1.0

Required Package	Description	Minimum Version
	Protocol	
PAM	Pluggable Authentication Modules	0.99.6.2-3.14

See Also

Using Templates for Additional Monitoring of UNIX and Linux

Troubleshooting UNIX and Linux Monitoring

Accessing UNIX and Linux Computers in Operations Manager

Required Capabilities for UNIX and Linux Accounts

Managing Certificates for UNIX and Linux Computers

Managing Resource Pools for UNIX and Linux Computers

Install Agent on UNIX and Linux Using the Discovery Wizard

Using Templates for Additional Monitoring of UNIX and Linux

You can provide additional monitoring and interaction capabilities with your managed UNIX and Linux computers by using the UNIX and Linux monitoring pack templates. For more information, see UNIX or Linux Log File and UNIX or Linux Process in the Authoring Guide.

See Also

Supported UNIX and Linux Operating System Versions

Troubleshooting UNIX and Linux Monitoring

Accessing UNIX and Linux Computers in Operations Manager

Required Capabilities for UNIX and Linux Accounts

Managing Certificates for UNIX and Linux Computers

Managing Resource Pools for UNIX and Linux Computers

Install Agent on UNIX and Linux Using the Discovery Wizard

Troubleshooting UNIX and Linux Monitoring

The following topics provide information about issues that might occur with monitoring UNIX and Linux computers in System Center 2012 – Operations Manager.

- Certificate Issues
- Management Pack Issues
- Operating System Issues
- Logging and Debugging

See Also

Supported UNIX and Linux Operating System Versions

Using Templates for Additional Monitoring of UNIX and Linux

Accessing UNIX and Linux Computers in Operations Manager

Required Capabilities for UNIX and Linux Accounts

Managing Certificates for UNIX and Linux Computers

Managing Resource Pools for UNIX and Linux Computers

Install Agent on UNIX and Linux Using the Discovery Wizard

Certificate Issues

This topic describes resolutions to certificate issues for monitoring UNIX or Linux computers.

Certificate Signing Error Message

During the installation of UNIX/Linux agents, you might see the following error.

```
Event Type:        Error

Event Source:    Cross Platform Modules

Event Category:                None

Event ID:              256

Date:                     4/1/2009

Time:                     4:02:27 PM

User:                     N/A

Computer:          COMPUTER1

Description:

Unexpected ScxCertLibException: Can't decode from base64

; input data is:
```

This error occurs when the certificate signing module is called but the certificate itself is empty. This error can be caused by an SSH connection failure to the remote system.

If you see this error, do the following:

1. Make sure that the SSH daemon on the remote host is running.
2. Make sure that you can open an SSH session with the remote host by using the credentials specified in the Discovery Wizard.
3. Make sure that the credentials specified in the Discovery Wizard have the required privileges for discovery. For more information see Required Capabilities for UNIX and Linux Accounts.

Certificate Name and Host Name do not Match

The common name (CN) that is used in the certificate must match the fully qualified domain name (FQDN) that is resolved by Operations Manager. If the CN does not match, you will see the following error when you run the Discovery Wizard:

```
The SSL certificate contains a common name (CN) that does not match the hostname
```

You can view the basic details of the certificate on the UNIX or Linux computer by entering the following command:

```
openssl x509 -noout -in /etc/opt/microsoft/scx/ssl/scx.pem -subject -issuer -dates
```

When you do this, you will see output that is similar to the following:

```
subject= /DC=name/DC=newdomain/CN=newhostname/CN=newhostname.newdomain.name

issuer= /DC=name/DC=newdomain/CN=newhostname/CN=newhostname.newdomain.name

notBefore=Mar 25 05:21:18 2008 GMT

notAfter=Mar 20 05:21:18 2029 GMT
```

Validate the hostnames and dates and ensure that they match the name being resolved by the Operations Manager management server.

If the hostnames do not match, use one of the following actions to resolve the issue:

- If the UNIX or Linux hostname is correct but the Operations Manager management server is resolving it incorrectly, either modify the DNS entry to match the correct FQDN or add an entry to the hosts file on the Operations Manager server.
- If the UNIX or Linux hostname is incorrect, do one of the following:
  - Change the hostname on the UNIX or Linux host to the correct one and create a new certificate.
  - Create a new certificate with the desired hostname.

To Change the Name on the Certificate:

If the certificate was created with an incorrect name, you can change the host name and re-create the certificate and private key. To do this, run the following command on the UNIX or Linux computer:

```
/opt/microsoft/scx/bin/tools/scxsslconfig -f -v
```

The **–f** option forces the files in /etc/opt/microsoft/scx/ssl to be overwritten.

You can also change the hostname and domain name on the certificate by using the **–h** and **–d** switches, as in the following example:

```
/opt/microsoft/scx/bin/tools/scxsslconfig -f -h <hostname> -d <domain.name>
```

Restart the agent by running the following command:

```
/opt/microsoft/scx/bin/tools/scxadmin -restart
```

To add an entry to the hosts file:

If the FQDN is not in Reverse DNS, you can add an entry to the hosts file located on the management server to provide name resolution. The hosts file is located in the \Windows\System32\Drivers\etc folder. An entry in the hosts file is a combination of the IP address and the FQDN.

For example, to add an entry for the host named “newhostname.newdomain.name” with an IP address of 192.168.1.1, add the following to the end of the hosts file:

```
192.168.1.1      newhostname.newdomain.name
```

See Also

Using Templates for Additional Monitoring of UNIX and Linux

Troubleshooting UNIX and Linux Monitoring

Accessing UNIX and Linux Computers in Operations Manager

Required Capabilities for UNIX and Linux Accounts

Management Pack Issues

Operating System Issues

Logging and Debugging

Managing Certificates for UNIX and Linux Computers

Managing Resource Pools for UNIX and Linux Computers

Install Agent on UNIX and Linux Using the Discovery Wizard

Management Pack Issues

This topic describes issues that are specific to management packs and modules.

ExecuteCommand Does Not Support Pipeline Operators or Aliases

When you use an alias or a pipeline operator with the *ExecuteCommand* parameter, the command fails. The *ExecuteCommand* parameter does not support the pipeline operator, aliases, and shell-specific syntax.

In System Center Operations Manager management packs that are designed to manage UNIX and Linux computers, the *ExecuteCommand* parameter does not start a shell process, causing the custom action to fail.

For each of the following custom action types, you specify how the command arguments are invoked by using either the *ExecuteCommand* parameter or the *ExecuteShellCommand* parameter:

- Microsoft.Unix.WSMan.Invoke.ProbeAction
- Microsoft.Unix.WSMan.Invoke.WriteAction
- Microsoft.Unix.WSMan.Invoke.Privileged.ProbeAction
- Microsoft.Unix.WSMan.Invoke.Privileged.WriteAction

The *ExecuteCommand* parameter passes the command-line arguments to the console without starting a shell process.

The *ExecuteShellCommand* parameter passes the command arguments to a shell process using the user's default shell; this shell supports pipeline, aliases, and shell-specific syntax.

Note

The *ExecuteShellCommand* parameter uses the default shell of the user who is running the command. If you require a specific shell, use the *ExecuteCommand* parameter, and prefix the command arguments with the required shell.

The following examples show how to use the *ExecuteCommand* and *ExecuteShellCommand* parameters:

- To pass the command-line arguments to the console without starting a shell process:

```
<p:ExecuteCommand_INPUT xmlns:p="http://schemas.microsoft.com/wbem/wscim/1/cim-schema/2/SCX_OperatingSystem"> <p:Command> service syslog status </p:Command> <p:timeout>10</p:timeout> </p:ExecuteCommand_INPUT>
```

- To pass the command-line arguments to a shell process that references an explicit shell:

```
<p:ExecuteCommand_INPUT xmlns:p="http://schemas.microsoft.com/wbem/wscim/1/cim-schema/2/SCX_OperatingSystem"> <p:Command> /bin/sh ps -ef syslog | grep -v grep </p:Command> <p:timeout>10</p:timeout> </p:ExecuteCommand_INPUT>
```

- To pass the command arguments to a shell process that uses the user's default shell:

```
<p:ExecuteShellCommand_INPUT xmlns:p="http://schemas.microsoft.com/wbem/wscim/1/cim-schema/2/SCX_OperatingSystem"> <p:Command> uptime |  awk '{print $10}' |awk -F"," '{print $1}' </p:Command> <p:timeout>10</p:timeout> </p:ExecuteShellCommand_INPUT>
```

See Also

Using Templates for Additional Monitoring of UNIX and Linux

Troubleshooting UNIX and Linux Monitoring

Accessing UNIX and Linux Computers in Operations Manager

Required Capabilities for UNIX and Linux Accounts

Certificate Issues

Operating System Issues

Logging and Debugging

Managing Certificates for UNIX and Linux Computers

Managing Resource Pools for UNIX and Linux Computers

Install Agent on UNIX and Linux Using the Discovery Wizard

Operating System Issues

This topic describes issues that are specific to UNIX and Linux operating systems.

Incorrect Reports of Shared Resources from a Solaris 10-Based Server

When you monitor a Sun Solaris 10-based server that is configured to use zones, Operations Manager might appear to incorrectly report shared resources such as a physical disk or a network adapter. This behavior occurs by design.

On a Solaris 10-based server that is configured to use zones, Operations Manager does not differentiate shared resources such as a physical disk or a network adapter. For any local zone that shares a global zone resource, Operations Manager does not report the shared resource. Only one instance of each resource is monitored on each Solaris 10-based server. If two network adapters exist on a Solaris 10-based server, and one is attached to the global zone while the second is shared between two local zones, the first enumerated local zone reports the shared resource. The second local zone will have no data for the shared resource.

In Operations Manager, the behavior of a Solaris 10-based server that is deployed in a virtual machine might differ slightly from the behavior of a Solaris 10-based server that is deployed on a physical computer. Each network adapter that exists in a virtual machine appears to the Solaris 10-based server as a separate physical resource. If uniquely defined network adapters are attached to each zone that is configured on the Solaris-based server, Operations Manager collects data for each network adapter.

Agent Providers Might Fail If the Solaris Computer's File Descriptor Limit is Reached by the Process

On a monitored Solaris computer with a large number of monitored objects (such as file systems or processors), you may observe unreliable behavior of the Solaris agent. Symptoms can include file systems, disks, or other objects not being discovered. This can be caused by the agent process running out of available File Descriptors (FD).

To determine if an issue is the result of File Descriptor limits, inspect the agent log file: /var/opt/microsoft/scx/log/scx.log. If any error messages in the log contain the text: errno = 24 (Too many open files), a FD limit issue should be suspected.

To resolve this issue, perform the following steps:

1. Modify the scx-cimd startup script at /opt/microsoft/scx/bin/tools/scx-cimd (Solaris 10 or Solaris 11) or /etc/init.d/scx-cimd (Solaris 9). Find the section of the script with the following lines:

   ```
   start)
       # Start daemon
       echo "Starting $DESC"
       $DAEMON $OPTIONS -d
       exit $?
       ;;
   ```

   Modify this section to include a ulimit –n 1024 command, prior to the $DAEMON $OPTIONS –d line, where "1024" is the new process limit for File Descriptors.

   ```
   start)
       # Start daemon
       echo "Starting $DESC"
       ulimit –n 1024
       $DAEMON $OPTIONS -d
       exit $?
       ;;
   ```

2. Restart the agent:

   ```
   scxadmin -restart
   ```

3. If the issue persists, try the configuration again with a File Descriptor limit of 2048, and then restart the agent. If the process continues to exhaust File Descriptors with the 2048 limit set, contact support.

See Also

Using Templates for Additional Monitoring of UNIX and Linux

Troubleshooting UNIX and Linux Monitoring

Accessing UNIX and Linux Computers in Operations Manager

Required Capabilities for UNIX and Linux Accounts

Management Pack Issues

Certificate Issues

Logging and Debugging

Managing Certificates for UNIX and Linux Computers

Managing Resource Pools for UNIX and Linux Computers

Install Agent on UNIX and Linux Using the Discovery Wizard

Logging and Debugging

This topic describes how to enable logging and debug tools for troubleshooting issues with monitoring UNIX and Linux computers.

Enable EnableOpsmgrModuleLogging

These logs are used mainly to investigate discovery issues. The logs show details about agent push, installation, and certificate signing. If you need to troubleshoot a discovery wizard problem, these logs would be helpful.

Calls made outside of Windows Remote Management (WinRM) are made using SSH/SFTP. These components rely on a separate logging mechanism than Operations Manager.

To enable UNIX native module Logs

- Create a blank file named **EnableOpsmgrModuleLogging** in the \Temp directory for the user account calling these modules by typing at a command-line prompt **COPY /Y NUL %windir%\TEMP\EnableOpsMgrModuleLogging**.

  Note
  Generally, it is the SYSTEM account making the calls, and C:\Windows\Temp is the default SYSTEM temp folder.

  After creation of the blank file, Operations Manager will immediately begin logging SSH and Certificate activity to the \Temp directory.Scripts that call into SSH modules will log to <*Scriptname.vbs*>.log. Other modules have their own logs.

  In some cases, it may be required to restart the HealthService to get the EnableOpsmgrModuleLogging logging to take effect.

Enable Logging on the UNIX Agent

These logs will report the UNIX agent actions. If there is a problem with the data returned to Operations Manager, look in this log. These logs are used infrequently.

How to enable logging on the UNIX agent

1. Log in to the UNIX host as root.
2. From the shell, turn on full verbose logging by typing **scxadmin -log-set all verbose**.

The logs are located in /var/opt/microsoft/scx/log.

Enable Operations Manager Verbose Tracing

This verbose tracing method is used to see the Windows Remote Management (WinRM) queries used by Operations Manager to gather data from the agent. If you suspect there is a problem with the WinRM connection, this log provides detailed information that can help with troubleshooting.

To trace WinRM events

1. On the Management server that is monitoring the UNIX or Linux agent, open a command prompt.
2. Type the following commands at the command prompt:
   a. **cd C:\Program Files\System Center Operations Manager 2012\tools**
   b. **StopTracing.cmd**
   c. **StartTracing.cmd VER**
3. Reproduce the failing issue in Operations Manager.
4. Type the following commands at the command prompt:
   a. **StopTracing.cmd**
   b. **FormatTracing.cmd**
5. Search for **WS-Man** in the TracingGuidsNative.log file.

Note

WinRM is also known as WS-Management (WS-Man).

Note

The **FormatTracing** command opens a Windows Explorer window displaying the c:\Windows\temp\OpsMgrTrace directory. The TracingGuidsNative.log file is in that directory.

Use DebugView to Troubleshoot Discovery Issues

DebugView is an alternative method to EnableOpsmgrModuleLogging for troubleshooting discovery issues.

To use DebugView

1. Download DebugView from: http://go.microsoft.com/fwlink/?Linkid=129486.
2. Launch DebugView on the Management Server performing the discovery.
3. Start discovering the UNIX Agents. You should start seeing output in your DebugView windows.
4. DebugView will present a step-by-step readout of the discovery wizard process. This is often the fastest method of troubleshooting discovery issues.

See Also

Using Templates for Additional Monitoring of UNIX and Linux

Troubleshooting UNIX and Linux Monitoring

Accessing UNIX and Linux Computers in Operations Manager

Required Capabilities for UNIX and Linux Accounts

Management Pack Issues

Operating System Issues

Certificate Issues

Managing Certificates for UNIX and Linux Computers

Managing Resource Pools for UNIX and Linux Computers

Install Agent on UNIX and Linux Using the Discovery Wizard

Monitoring Linux Computers in Windows Azure by Using Operations Manager

System Center 2012 R2 Operations Manager provides monitoring of Linux computers both in your data center and hosted as persistent virtual machines in Windows Azure. This topic describes considerations for monitoring of Linux virtual machines in Windows Azure.

Supported Topologies

Monitoring of Linux computers running as persistent virtual machines in Windows Azure is supported in the following topologies:

- Operations Manager and supporting services (SQL Server and Active Directory) deployed in your on-premises data center with a site-to-site VPN connection to the Windows Azure virtual network where the Linux virtual machines are deployed.
    - More information about Windows Azure site-to-site VPN connections can be found here.

- Operations Manager and supporting services (SQL Server and Active Directory) deployed in Windows Azure, with virtual network connectivity between the Operations Manager Management Server and Linux virtual machines.

Note
Operations Manager monitoring of Linux virtual machines in Windows Azure over the public Internet without a VPN connection is not a supported configuration.

Supported Linux Operating Systems

All Linux operating systems and versions supported both by System Center 2012 R2 Operations Manager and Windows Azure are supported for monitoring in the Supported Topologies section above.

For more information about supported Linux operating systems, see the following:

- System Center 2012 R2 – Operations Manager supported Linux operating systems
- Windows Azure supported Linux operating systems

Certificate and Name Resolution Requirements

Whether Linux computers are running on-premises or in Windows Azure, the following requirements for Operations Manager monitoring of Linux computers apply:

- The Management Server can resolve the fully-qualified domain name and IP address of the managed Linux computer with forward and reverse DNS lookups.
- The agent certificate on the Linux computer is created with the fully-qualified domain name (for the Linux computer) that the Management Server uses to identify the Linux computer.

For Linux virtual machines deployed in Windows Azure, additional configuration may be required to meet the certificate configuration requirements, as the fully-qualified domain name known locally to the Linux computer may not be the FQDN used to reach the Linux computer. The following options can be used to ensure that the Operations Manageragent is able to generate a certificate with the correct FQDN during agent installation.

Option 1: Edit /etc/hosts

1. Confirm that `/etc/nsswitch.conf` (on the Linux VM) is configured to prioritize **files** before DNS.
2. Edit `/etc/hosts` so that an entry for the host exists with the following format:

   <IP Address> <hostname> <fully-qualified domain name>

   For example, reference the entry in the following hosts file for the linuxvm1.contoso.com host.

```
# IP-Address  Full-Qualified-Hostname  Short-Hostname

127.0.0.1       localhost
```

```
192.168.1.124   linuxvm1        linuxvm1.contoso.com
::1             localhost ipv6-localhost ipv6-loopback
```

Option 2: Configure DNS and DNS Search Suffixes

1. Configure the Windows Azure virtual network with your DNS server addresses. More information can be found here.
2. Configure the appropriate DHCP client settings on the Linux virtual machines so that the correct search suffix is configured (in `/etc/resolv.conf`). The following steps demonstrate this configuration on CentOS, SUSE Linux Enterprise Server, and Ubuntu Server.

   CentOS

   a. Edit the interface configuration script for eth0 (`/etc/sysconfig/network-scripts/ifcfg-eth0`). Add a **SEARCH** entry to the `ifcfg-eth0 script`. For example, if your domain name is contoso.com, the SEARCH entry to add is:

   ```
   SEARCH="contoso.com"
   ```

   b. Restart the network service:

   ```
   service network restart
   ```

   SUSE Linux Enterprise Server

   a. Edit the netconfig file:

   ```
   /etc/sysconfig/network/config
   ```

   b. Set the following property values in the file:

   ```
   NETCONFIG_DNS_POLICY="STATIC"
   NETCONFIG_DNS_STATIC_SEARCHLIST="<your DNS search suffixes>"
   NETCONFIG_DNS_STATIC_SERVERS="<your DNS server addresses>"
   ```

   For example:

   ```
   ## Type:        string
   ## Default:     "auto"
   #
   # Defines the DNS merge policy as documented in netconfig(8)
   manual page.
   # Set to "" to disable DNS configuration.
   #
   NETCONFIG_DNS_POLICY="STATIC"

   ## Type:        string
   ## Default:     "resolver"
   ```

```
#
# Defines the name of the DNS forwarder that has to be
configured.
#
NETCONFIG_DNS_FORWARDER="resolver"

## Type:        string
## Default:     ""
#
# List of DNS domain names used for host-name lookup.
#
NETCONFIG_DNS_STATIC_SEARCHLIST="contoso.com"

## Type:        string
## Default:     ""
#
# List of DNS nameserver IP addresses to use for host-name
lookup.
#
NETCONFIG_DNS_STATIC_SERVERS="192.168.1.8"
```

c. Restart the network service:

```
service network restart
```

Ubuntu Server

a. Edit the interface configuration file (`/etc/network/interfaces`).

b. Add a **dns-search** entry to the configuration for **eth0** to define the DNS search suffixes. For example:

```
# The primary network interface
auto eth0
iface eth0 inet dhcp
dns-search contoso.com
```

c. Restart the network service:

```
/etc/init.d/networking restart
```

Correcting Certificate Issues

If the agent certificate was created with an incorrect fully-qualified domain name for the Linux virtual machine, the **scxsslconfig** utility can be used to regenerate the certificate. More information and troubleshooting steps can be found here.

Additional Configuration

The following additional configuration steps may be necessary when managing Linux virtual machines in Windows Azure with Operations Manager.

Create a Group for Linux Computers hosted in Windows Azure

To simplify override configuration of rules and monitors, it is recommended to create a Group in Operations Manager that contains the Linux computer instances that are hosted in Windows Azure.

1. In the **Operations Console**, navigate to the **Authoring** pane.
2. Click **Groups**, and click **New Group**. This group will be used to identify Linux virtual machines in Windows Azure.
3. Provide a name and description for the group, and select a destination management pack.
4. Either add each discovered Linux computer that is hosted in Windows Azure as an **Explicit Member** to the group, or create **Dynamic Inclusion** rules that populate the group with Linux computers, based on a name or IP address pattern.
5. Complete the Group Creation Wizard.

Disable Available Swap Space monitors

Linux virtual machines created from Gallery images do not have swap space configured by default. This will cause the Available Swap Space monitors to generate alerts for the Linux virtual machines. It is recommended to disable these monitors with an override for Linux virtual machines in Windows Azure.

1. In the **Operations Console**, navigate to the **Authoring** pane.
2. Expand **Management Pack Objects** and click **Monitors**.
3. Search for the string: “Available Megabytes Swap” in the top search bar.

   There will be one monitor with the name: **Operating System Available Megabytes Swap Space** for each Linux operating system and version. For each of these that apply to the Linux virtual machines hosted in Windows Azure, right-click the monitor, and then select **Overrides -> Override the Monitor -> For a Group**.
4. Select the group created in the previous exercise that identifies Linux computers in Windows Azure.
5. Check the box next to the **Enabled** parameter, and set the **Override Value** to **False**.
6. Select the destination management pack, and click **OK**.

Disable the ACPI Daemon Monitor for SUSE Linux Enterprise Server Computers

The SUSE Linux Enterprise Server management packs include a default monitor for the acpi daemon (acpid). This daemon is not enabled by default in the SUSE Linux Enterprise Server images in the Windows Azure Gallery. This monitor should be disabled for any SUSE Linux Enterprise Server computer hosted in Windows Azure.

1. In the **Operations Console**, navigate to the **Authoring** pane.
2. Expand **Management Pack Objects** and click **Monitors**.
3. Search for the string: “Process Acpi” in the top search bar.

   There will be one monitor with the name: **Process Acpi Service Health** for each SUSE Linux Enterprise Server version. For each of these that apply to the Linux virtual machines hosted in Windows Azure, right click the monitor, and then select **Overrides -> Override the Monitor -> For a Group**.
4. Select the group created in the previous exercise that identifies Linux computers in Windows Azure.
5. Check the box next to the **Enabled** parameter, and set the **Override Value** to **False**.
6. Select the destination management pack, and click **OK**.

Additional Resources

- Monitoring UNIX and Linux Computers by Using Operations Manager
- Install Agent on UNIX and Linux Using the Discovery Wizard
- Accessing UNIX and Linux Computers in Operations Manager
- Troubleshooting UNIX/Linux Agent Discovery in System Center 2012 - Operations Manager
- Configuring sudo Elevation for UNIX and Linux Monitoring with System Center 2012 – Operations Manager
- Introduction to Linux on Windows Azure
- Create a Virtual Machine Running Linux
- Windows Azure Name Resolution

Collecting Security Events Using Audit Collection Services in Operations Manager

In System Center 2012 – Operations Manager, Audit Collection Services (ACS) provides a means to collect records generated by an audit policy and store them in a centralized database. By default, when an audit policy is implemented on a Windows computer, that computer automatically saves all events generated by the audit policy to its local Security log. This is true for Windows workstations as well as servers. In organizations that have strict security requirements, audit policies can quickly generate large volumes of events.

Using ACS, organizations can consolidate individual Security logs into a centrally managed database and can filter and analyze events using the data analysis and reporting tools provided by Microsoft SQL Server. With ACS, only a user who has specifically been given the right to access the ACS database can run queries and create reports on the collected data.

ACS requires the following components:

- ACS Forwarders
- ACS Collector
- ACS Database

Auditing is supported on UNIX and Linux computers. For more information, see ACS on UNIX and Linux in this topic.

(See list of Collecting Security Events Using Audit Collection Services topics.)

ACS Forwarders

The service that runs on ACS forwarders is included in the Operations Manager agent. By default, this service is installed but not enabled when the Operations Manager agent is installed. You can enable this service for multiple agent computers at the same time using the **Enable Audit Collection** task. After you enable this service, all security events are sent to the ACS collector in addition to the local Security log.

ACS Collector

The ACS collector receives and processes events from ACS forwarders and then sends this data to the ACS database. This processing includes disassembling the data so that it can be spread across several tables within the ACS database, minimizing data redundancy, and applying filters so that unnecessary events are not added to the ACS database.

The number of ACS forwarders that can be supported by a single ACS collector and ACS database can vary, depending on the following factors:

- The number of events that your audit policy generates.
- The role of the computers that the ACS forwarders monitor (such as domain controller versus member server).
- The level of activities on the computer.
- The hardware on which the ACS collector and ACS database run.

If your environment contains too many ACS forwarders for a single ACS collector, you can install more than one ACS collector. Each ACS collector must have its own ACS database.

The requirements for an ACS collector are as follows:

- An Operations Manager management server
- A member of an Active Directory domain
- A minimum of 1 gigabyte (GB) of RAM, with 2 GB recommended
- At least a 1.8 gigahertz (GHz) processor, with a 2.8 GHz processor recommended

- 10 GB of hard disk space available, at a minimum, with 50 GB recommended

On each computer on which you plan to install the ACS collector, you must download and install the latest version of the Microsoft Data Access Components (MDAC) from the Microsoft Web site. To learn more about MDAC, see at Learning Microsoft Data Access Components (MDAC).

ACS Database

The ACS database is the central repository for events that are generated by an audit policy within an ACS deployment. The ACS database can be located on the same computer as the ACS collector, but for best performance, each should be installed on a dedicated server.

The requirements for an ACS database are as follows:

- For System Center 2012 – Operations Manager: SQL Server 2005 or SQL Server 2008. You can choose an existing or new installation of SQL Server. The Enterprise edition of SQL Server is recommended because of the stress of daily ACS database maintenance.
- For System Center 2012 Service Pack 1 (SP1), Operations Manager: SQL Server SQL 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1. The Enterprise edition of SQL Server is recommended because of the stress of daily ACS database maintenance.
- A minimum of 1 GB of RAM, with 2 GB recommended

  Note
  If your SQL Server has more than 2 GB of memory some additional configuration steps are needed. For more information and the steps needed, see How to configure SQL Server to use more than 2 GB of physical memory. For a list of the minimum hardware and software requirements to install and run SQL Server 2012, see Hardware and Software Requirements for Installing SQL Server 2012.

- At least a 1.8 GHz processor, with a 2.8 GHz processor recommended
- 20 GB of hard disk space available, at a minimum, with 100 GB recommended

If you use SQL Server standard edition, the database must pause during daily maintenance operations. This may cause the ACS collector queue to fill with requests from ACS forwarders. A full ACS collector queue then causes ACS forwarders to be disconnected from the ACS collector. Disconnected ACS forwarders reconnect after the database maintenance is complete and the queue backlog is then processed. To ensure no audit events are lost, allocate a sufficient amount of hard disk space for the local security log on all ACS forwarder.

SQL Server enterprise edition can continue to service ACS forwarder requests, although at a lower performance level, during daily maintenance operations. For more information on the ACS collector queue and ACS forwarder disconnection see Audit Collection Services Capacity Planning and Monitoring Audit Collection Services Performance.

ACS support for Dynamic Access Control

System Center 2012 Service Pack 1 (SP1), Operations Manager provides ACS support for Dynamic Access Control as enabled by Windows Server 2012.

Windows Server 2012 enables business data owners to easily classify and label data allowing access policies to be defined for data classes that are critical to business. Compliance management in Windows Server 2012 becomes more efficient and flexible because access and audit policies can be based not only on user and group information but a richer set of user, resource and environmental claims, and properties from Active Directory and other sources. User claims such as roles, projects, organization, resource properties such as secrecy, and device claims such as health can be used in defining access and audit policies.

Windows Server 2012 enhances the existing Windows ACL model to support Dynamic Access Control where customers can define an expression based authorization access policy that includes conditions using user and machine claims, as well as resource (for example, file) properties. The following illustration is descriptive, and not an actual representation of an expression:

- Allow Read and Write access if User.Clearance >= Resource.Secrecy and Device. Healthy
- Allow Read and Write access if User.Project any_of Resource.Project

System Center 2012 Service Pack 1 (SP1) contributes to the fulfilling these scenarios by providing enterprise-wide visibility into the use of the Dynamic Access Control, leveraging Operations Manager's Audit Collection Services to collect events from the relevant machines (file servers, domain controllers) and providing reporting to enable auditors and compliance officers to report on the use of Dynamic Access Control – for example, audit changes in policies, object access (success and failure), and "what-if" assessment of what would happen if a certain policy were applied.

Configuration for Dynamic Access Control

No configuration to ACS handling Dynamic Access Control information is required by the customer. The only interaction with this feature is through a set of reports. No additional monitoring is required.

ACS on UNIX and Linux

There are a few differences in how ACS is performed on UNIX and Linux computers, as compared to Windows computers. They are as follows:

- You must import the ACS Management Packs for the UNIX and Linux operating systems.
- Events that are generated from the audit policy on UNIX and Linux computers are forwarded to the Windows Security Event log of the Windows management server that is monitoring the UNIX or Linux computers, and then collected in the centralized database.

  On the management server, a write action module parses the audit data from each managed UNIX and Linux computer and writes the information to the Windows Security Event log. A data source module communicates with agents that are deployed on the managed UNIX and Linux computers for log file monitoring.

- An agent (the Operations Manager agent for UNIX/Linux) resides on each UNIX or Linux computer that is being managed.
- The ACS Collector schema is extended to support the additional content and formatting of audit data sent by UNIX and Linux computers.

Collecting Security Events Using Audit Collection Services topics

- Audit Collection Services Security
- Audit Collection Services Capacity Planning
- Audit Collection Services Performance Counters
- How to Enable Audit Collection Services (ACS) Forwarders
- How to Enable Event Logging and ACS Rules on Solaris and AIX Computers
- How to Filter ACS Events for UNIX and Linux Computers
- How to Configure Certficates for ACS Collector and Forwarder
- Monitoring Audit Collection Services Performance
- How to Remove Audit Collection Services (ACS)
- Audit Collection Services Administration (AdtAdmin.exe)

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Initial Monitoring After Operations Manager Is Installed
- Managing Access in Operations Manager
- Getting Information from Operations Manager
- General Tasks in Operations Manager
- Maintenance of Operations Manager
- Operations Manager Report Authoring Guide
- Accessing UNIX and Linux Computers in Operations Manager
- Managing Discovery and Agents

Audit Collection Services Security

In System Center 2012 – Operations Manager, Audit Collection Services (ACS) requires mutual authentication between the ACS collector and each ACS forwarder. By default, Windows authentication, which uses the Kerberos protocol, is used for this authentication. After authentication is complete, all transmissions between ACS forwarders and the ACS collector are encrypted. You do not need to enable additional encryption between ACS forwarders and the

ACS collector unless they belong to different Active Directory forests that have no established trusts.

By default, data is not encrypted between the ACS collector and the ACS database. If your organization requires a higher level of security, you can use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to encrypt all communication between these components. To enable SSL encryption between the ACS database and the ACS collector, you need to install a certificate on both the database server and the computer hosting the ACS Collector service. After these certificates are installed, configure the SQL client on the ACS collector to force encryption.

For more information about installing certificates and enabling SSL or TLS, see SSL and TLS in Windows Server 2003 and Obtaining and installing server certificates. For a list of the steps to force encryption on a SQL client, see How to enable SSL encryption for SQL Server 2000 if you have a valid Certificate Server.

Limited Access to Audit Events

Audit events that are written to a local Security log can be accessed by the local administrator, but audit events that are handled by ACS, by default, do not allow users (even users with administrative rights) to access audit events in the ACS database. If you need to separate the role of an administrator from the role of a user who views and queries the ACS database, you can create a group for database auditors and then assign that group the necessary permissions to access the audit database. For step-by-step instructions, see How to Install Audit Collection Services (ACS).

Limited Communication for ACS Forwarders

Configuration changes to the ACS forwarder are not allowed locally, even from user accounts that have the rights of an administrator. All configuration changes to an ACS forwarder must come from the ACS collector. For additional security, after the ACS forwarder authenticates with the ACS collector, it closes the inbound TCP port used by ACS so that only outgoing communication is allowed. The ACS collector must terminate and then reestablish a communication channel to make any configuration changes to an ACS forwarder.

ACS Forwarders Separated from the ACS Collector by a Firewall

Because of the limited communication between an ACS forwarder and an ACS collector you only need to open the inbound TCP port 51909 on a firewall to enable an ACS forwarder, separated from your network by a firewall, to reach the ACS collector.

See Also

Collecting Security Events Using Audit Collection Services in Operations Manager

How to Configure Certficates for ACS Collector and Forwarder
Audit Collection Services Capacity Planning
Audit Collection Services Performance Counters
How to Enable Audit Collection Services (ACS) Forwarders
How to Enable Event Logging and ACS Rules on Solaris and AIX Computers
How to Filter ACS Events for UNIX and Linux Computers
Monitoring Audit Collection Services Performance
How to Remove Audit Collection Services (ACS)
Audit Collection Services Administration (AdtAdmin.exe)

Audit Collection Services Capacity Planning

Audit policies can generate a large amount of data. In System Center 2012 – Operations Manager, for better performance, you can change settings on the Audit Collection Services (ACS) collector to adjust for the actual auditing load. The queue that the ACS collector uses to store events that are ready to be written to the ACS database has a considerable impact on ACS's ability to handle a surge in the amount of generated security events. Balancing the capacity of this queue along with maintaining the correct amount of RAM on the ACS collector can improve the performance of ACS.

ACS Collector Queue

The ACS collector queue is used to store events after they are received from ACS forwarders but before they are sent to the ACS database. The number of events in the queue increases during periods of high audit traffic or when the ACS database is not available to accept new events, such as during database purging. Three registry values control how the ACS collector reacts when this queue is approaching maximum capacity.

The following table lists each registry entry and its default value. All registry entries in the table are located in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdtServer\Parameters key of the registry.

Entry Name	Default Value	Description
MaxQueueLength	0x40000	The maximum number of events that can queue in memory while waiting for the database. On average, each queue entry consumes 512 bytes of memory.
BackOffThreshold	75	How full the ACS collector queue

Entry Name	Default Value	Description
		can become before the ACS collector denies new connections from ACS forwarders. This value is expressed as a percentage of MaximumQueueLength.
DisconnectThreshold	90	How full the ACS collector queue can become before the ACS collector begins disconnecting ACS forwarders. This value is expressed as a percentage of MaximumQueueLength. ACS forwarders with the lowest priority value are disconnected first.

You might want to adjust the value of one or more of the preceding registry entries, depending on your environment. For best results, you should consider how a value change of one entry will affect the rest. For example, the value of BackOffThreshold should always be less than DisconnectThreshold, allowing the ACS collector to gracefully degrade performance when the ACS database cannot keep up with demand.

ACS Collector Memory

Memory on the ACS collector is used for caching ACS events that need to be written to the ACS database. The amount of memory needed by an ACS collector can vary depending on the number of ACS forwarders connected and the number of events generated by your audit policy. You can use the following formula, based on expected traffic, to calculate whether more memory is needed for better ACS performance:

Recommended Memory = (M x .5)+(50 x N)+(S x .5)+(P x .1)

The formula variables are defined in the following table.

Variable	Definition	Registry Key	Entry Name
M	Maximum number of events queued in	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdtServer\Parameters	MaxQueueLength

Vari-able	Definition	Registry Key	Entry Name
	memory on the ACS collector		
N	Number of forwarders connected to the ACS collector	No registry setting	NA
S	ACS uses the string cache for previously inserted strings, such as event parameters, to avoid unnecessary queries to the dtString tables in the ACS database. Size of the string cache on	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdtServer\Parameters	StringCacheSize

Vari-able	Definition	Registry Key	Entry Name
	the ACS collector, expressed by the maximum number of entries the cache can hold. On average, each queue entry consumes 512 bytes of memory. This cache is used for event record data.		
P	Size of the principal cache on the ACS collector, expressed as the maximum number of entries	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdtServer\Parameters	PrincipalCacheSize

Variable	Definition	Registry Key	Entry Name
	the cache can hold. This cache is used for data that pertains to the user and computer accounts that have access to ACS components.		

ACS Database Recommendations

When ACS is operating normally, the queue length should seldom reach the BackOffThreshold value. If the queue length frequently reaches this threshold, either you have more events than your database can handle or your database hardware should be upgraded.

To reduce the number of events written to the ACS database, you can change your audit policy to reduce the number of generated events or use filters, applied at the ACS collector, to discard unnecessary events and keep them out of the ACS database. You can also reduce the number of ACS forwarders that send events to the ACS database by deploying an additional ACS collector and database so that fewer ACS forwarders are serviced by each ACS collector.

For more information on filters, see the AdtAdmin.exe /SetQuery. For more information on the number of ACS forwarders that an ACS collector can support, see Collecting Security Events Using Audit Collection Services in Operations Manager.

UNIX and Linux Considerations

The performance for deploying ACS on UNIX and Linux computers diminishes with datasets that exceed 10,000 records.

See Also

Collecting Security Events Using Audit Collection Services in Operations Manager

How to Configure Certficates for ACS Collector and Forwarder

Audit Collection Services Security

Audit Collection Services Performance Counters

How to Enable Audit Collection Services (ACS) Forwarders

How to Enable Event Logging and ACS Rules on Solaris and AIX Computers

How to Filter ACS Events for UNIX and Linux Computers

Monitoring Audit Collection Services Performance

How to Remove Audit Collection Services (ACS)

Audit Collection Services Administration (AdtAdmin.exe)

Audit Collection Services Performance Counters

In System Center 2012 – Operations Manager, the Audit Collection Services (ACS) collector service includes two performance objects that have a total of 16 counters: the Collector object and the Collector Client object. The Collector object has 14 counters, and the Collector Client object has two counters. The counters in the Collector object record performance statistics from the perspective of the ACS collector. The Collector Client counters record performance statistics from the perspective of a single ACS forwarder.

Performance objects and counters are viewable in System Monitor, which is a part of Performance Console available in Windows Server products. For more information about monitoring performance and System Monitor, see System Monitor Overview.

Collector Object

The following table describes each counter in the Collector performance object. If the counter describes information that is added to a specific table in the ACS database, that table is defined in the counter description.

Connected Clients

The number of ACS forwarders currently connected to the ACS collector.

Database Queue % Full

The ratio of the number of events currently in the ACS database loader queue divided by the highest number of requests that the database loader queue has had. This ratio is expressed as a percentage.

Database Queue Length

The number of events currently in the database loader queue.

DB Loader Events Inserts/sec

The average number of records added, per second, to the dtEvent table in the ACS database, which contains event record entries.

DB Loader Principal Inserts/sec

The average number of records added, per second, to the dtPrincipal table in the ACS database, which contains information about the user and computer accounts that have access to the ACS components.

DB Loader String Inserts/sec

The average number of records added, per second, to the dtString table in the ACS database.

DB Principal Cache Hit %

The percentage of all handling requests that are serviced by the principal cache instead of the dtPrincipal table in the ACS database.

DB Request Queue Length

The number of requests from the ACS collector currently waiting to be serviced by the ACS database. These requests are used during forwarder handshake and during database maintenance. They are not part of normal event handling.

DB String Cache Hit %

The percentage of all handling requests that are serviced by the string cache, thereby avoiding a lookup in the dtString table in the ACS database.

Event time in collector in milliseconds

The amount of time, in milliseconds, between event arrival at the ACS collector and insertion into the ACS database queues.

Incoming Events/sec

The total number of events arriving, per second, at the collector from all connected ACS

forwarders.

Interface Audit Insertions/sec

The number of event records, per second, sent by the collector to Windows Management Instrumentation (WMI) for forwarding to an application outside of ACS.

Interface Queue Length

The average number of requests waiting on WMI resources.

Registered Queries

The total number of subscription requests that WMI has received for ACS events since the ACS Collector service was last started.

Collector Client Object

The Collector Client performance object displays statistics about events that occur on a specified ACS forwarder. The ACS Collector Client performance object is installed on the ACS collector. If multiple ACS forwarders are connected to the ACS collector, multiple instances of the counter are displayed. In large environments with more than 100 ACS forwarders connected to an ACS collector, the Collector Client performance object, by default, displays the statistics of the ACS forwarders with the highest asset values. ACS forwarders that have the most audit events are assigned higher asset values to ensure their connections are prioritized over ACS forwarders with fewer events.

Note

Asset values are assigned automatically by the ACS collector. You can change the assigned asset values using AdtAdmin.exe and the *UpdForwarder* parameter. For more information about the AdtAdmin.exe tool, see Audit Collection Services Administration (AdtAdmin.exe).

The Collector Client performance object has two counters. The following table describes each of these counters.

Average time between event generation

The average amount of time, in milliseconds, from the creation of an event to the time the event arrives at the ACS collector.

Incoming Audits/sec

The total number of events sent to the ACS collector from the ACS forwarder.

See Also

Collecting Security Events Using Audit Collection Services in Operations Manager

How to Configure Certficates for ACS Collector and Forwarder

Audit Collection Services Capacity Planning

Audit Collection Services Security

How to Enable Audit Collection Services (ACS) Forwarders

How to Enable Event Logging and ACS Rules on Solaris and AIX Computers

How to Filter ACS Events for UNIX and Linux Computers

Monitoring Audit Collection Services Performance

How to Remove Audit Collection Services (ACS)

Audit Collection Services Administration (AdtAdmin.exe)

How to Enable Audit Collection Services (ACS) Forwarders

Depending on your auditing needs, you might have several hundred to thousands of computers from which you want to collect audit events. By default, the service needed for an agent to be an Audit Collection Services (ACS) forwarder is installed but not enabled when the Operations Manager agent is installed. After you install the ACS collector and database you can then remotely enable this service on multiple agents through the Operations Manager console by running the **Enable Audit Collection** task.

This procedure should be run after the ACS collector and database are installed and can only be run against computers that already have the Operations Manager agent installed. In addition, the user account that runs this task must belong to the local Administrators group on each agent computer.

To enable audit collection on Operations Manager agents

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role. This account must also have the rights of a local administrator on each agent computer that you want to enable as an ACS forwarder.
2. In the Operations console, click **Monitoring**.
3. In the navigation pane, expand **Operations Manager**, expand **Agent Details**, and then click **Agent Health State**. This view has two panes, and the actions in this procedure are performed in the right pane.
4. In the details pane, click all agents that you want to enable as ACS forwarders. You can make multiple selections by pressing CTRL or SHIFT.
5. In the **Actions** pane, under **Health Service Tasks**, click **Enable Audit Collection** to open the **Run Task - Enable Audit Collection** dialog box.

6. In the **Task Parameters** section, click **Override** to open the **Override Task Parameters** dialog box.
7. In the **Override the task parameters with the new values** section, click the *CollectorServer* parameter; in the **New Value** column, type the FQDN of the ACS collector; and then click **Override**.

   Note
   If you are enabling ACS on a gateway or management server and you do not specify the *CollectorServer* parameter, the task will fail with a “Type Mismatch Error.” To avoid this, provide a value for the override.
8. In the **Task credentials** section, click **Other**. In the **User Name** box, type the name of a user account that belongs to the local Administrators group on the agent computers. In the **Password** box, type the password for this user account. Click to expand the **Domain** list to view the available domains, and then click the domain of the user account.
9. Click **Run Task**. The **Task Status** dialog box displays tracking the progress of the task.
10. When the task completes successfully, click **Close**.

See Also

Collecting Security Events Using Audit Collection Services in Operations Manager

How to Configure Certficates for ACS Collector and Forwarder

Audit Collection Services Capacity Planning

Audit Collection Services Performance Counters

Audit Collection Services Security

How to Enable Event Logging and ACS Rules on Solaris and AIX Computers

How to Filter ACS Events for UNIX and Linux Computers

Monitoring Audit Collection Services Performance

How to Remove Audit Collection Services (ACS)

Audit Collection Services Administration (AdtAdmin.exe)

How to Enable Event Logging and ACS Rules on Solaris and AIX Computers

This topic does not apply to Windows computers.

By default, Solaris and AIX computers do not log audit events. The logging configuration is controlled by the file located at /etc/syslog.conf. You must make edits to this file and then enable ACS rules.

To Configure the Solaris Syslog

1. Add the following code to the syslog.conf file:

```
auth.info;local2.info                                   /var/log/authlog
```

   Note
   Use the TAB key to separate log components from the log file names. Spaces do not work.

2. Restart the Syslog daemon.
3. On Solaris 5.8 and 5.9, enter the following commands:

```
/etc/init.d/syslog stop

/etc/init.d/syslog start
```

   On Solaris 5.10, enter the following commands:

```
svcadm refresh svc:/system/system-log
```

You now must enable the ACS rules.

To Configure the AIX Syslog

1. Add the following code to the syslog.conf file:

```
*.info  /var/log/syslog.log   rotate size 1m files 10
```

   The Syslog file is rotated when it becomes larger than 1 megabyte (MB) and the number of rotated files is limited to 10.

   Note
   Use the TAB key to separate log components from the log file names. Spaces do not work.

2. Enter the following command to refresh the computer's configuration:

```
# refresh -s syslogd
```

You now must enable the ACS rules.

To Enable ACS Rules

1. In the **Operations** console, click **Authoring**.
2. In the navigation pane, click **Authoring**, click **Management Pack Objects**, and then click **Rules**.
3. In the rules pane, search for the rule to be enabled. If the **Look for** bar is not available above the **Rule** list, navigate from the **View** menu, and then click **Find**.
4. Right-click the rule name for the rule that you want to enable, navigate to **Overrides** , click **Override the Rule**, and then click **For all object of class** for a class of objects to be monitored by the rule.
5. Set the **Enabled** parameter to **True**, modify the **Override Value** to **True**, and then click **OK**.

See Also

Collecting Security Events Using Audit Collection Services in Operations Manager

How to Configure Certficates for ACS Collector and Forwarder

Audit Collection Services Capacity Planning

Audit Collection Services Performance Counters

How to Enable Audit Collection Services (ACS) Forwarders

Audit Collection Services Security

How to Filter ACS Events for UNIX and Linux Computers

Monitoring Audit Collection Services Performance

How to Remove Audit Collection Services (ACS)

Audit Collection Services Administration (AdtAdmin.exe)

How to Filter ACS Events for UNIX and Linux Computers

By default, ACS collects and stores every event recorded in the Windows Security Event logs. A large number of the events can make it difficult to identify potential problems. You want to collect only the security events that meet your audit and security compliance requirements.

Best practice is to archive the data by using an ACS Archiver and then restore it to a historical repository. From this repository, you can run your filtering. The following procedure provides the ability to maintain all audit events and optimize the audit data report performance. For example, you may want to store all Successful Logon Events (540,528), but not report on them unless audited.

To filter Event IDs by using AdtAdmin

1. At a command prompt, change the working directory to **%windir%\system32\security\AdtServer**.
2. At the same command prompt, set the query parameters by entering **AdtAdmin /setquery /query:"select * from AdtsEvent where NOT (EventID=560 OR EventID=562 OR …)"**, where the EventIDs listed are the audit events to be ignored in the event log.

   For example, to set a filter so that only the UNIX and Linux security events are logged to the Windows Security Event log , set the query parameters by entering **AdtAdmin /setquery /query:"select * from AdtsEvent where NOT (EventID=560 OR EventID=562 OR EventID=569 OR EventID=570 OR EventID=571 OR EventID=26401 OR EventID=4665 OR EventID=4666 OR EventID=4667 OR EventID=4624 OR EventID=4634 OR EventID=4648 OR EventID=5156 OR EventID=4656 OR EventID=4658 OR EventID=5159)"**.

For additional information about how to use AdtAdmin.exe, see Audit Collection Services Administration (AdtAdmin.exe).

See Also

Collecting Security Events Using Audit Collection Services in Operations Manager

How to Configure Certficates for ACS Collector and Forwarder

Audit Collection Services Capacity Planning

Audit Collection Services Performance Counters

How to Enable Audit Collection Services (ACS) Forwarders

Audit Collection Services Security

Audit Collection Services Security

Monitoring Audit Collection Services Performance

How to Remove Audit Collection Services (ACS)

Audit Collection Services Administration (AdtAdmin.exe)

How to Configure Certficates for ACS Collector and Forwarder

When the Audit Collection Service (ACS) Forwarder is located in a domain separate from the domain where the ACS Collector is located, and no two-way trust exists between the two domains, certificates must be used so that authentication can take place between the ACS Forwarder and the ACS Collector.

Before you configure certificates, ensure that the following actions have been completed:

- On the ACS Forwarder:
  - An agent is installed on the computer that will serve as the ACS Forwarder. For more information, see Operations Manager Agent Installation Methods.
  - A certificate and certification authority [CA] certificate is installed on the computer hosting the agent. For more information, see Authentication and Data Encryption for Windows Computers in the Deployment Guide.
- On the ACS Collector:
  - A certificate (and CA certificate) is installed on the management server hosting the ACS Collector. For more information, see Authentication and Data Encryption for Windows Computers in the Deployment Guide.
  - The pending agent is approved and communication between the agent and the management server is operating properly. For more information, see Process Manual Agent Installations.
  - The ACS Collector and database is installed. For more information, see How to Install an Audit Collection Services (ACS) Collector and Database in the Deployment Guide.

The following is a high-level overview of the steps that need to be performed to use certificates with ACS.

Important
Certificates used on various components in Operations Manager (for example, ACS Collector, ACS Forwarder, agent, gateway server, or management server) must be issued by the same CA.

On the computer hosting the ACS Collector:

- Run ADTServer -c.
- Map the ACS Forwarder Certificate in Active Directory.
- In the Operations console, enable ACS.

On the computer hosting the ACS Forwarder:

- Export the certificate to a disk, USB flash drive, or network share.
- Run ADTAgent -c.

To assign a certificate to the ACS Collector

1. On the Windows desktop, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command prompt, type <*drive_letter*>: (where <*drive_letter*> is the drive where the operating system is installed), and then press ENTER.
4. Type **cd %systemroot%**, and then press ENTER.
5. Type **cd system32\security\adtserver**, and then press ENTER.
6. Type **net stop adtserver**, and then press ENTER.
7. Type **adtserver -c**, and then press ENTER.
8. In the numbered list of certificates, find the certificate used for Operations Manager, type the number in the list (should be 1), and then press ENTER.
9. Type **net start adtserver** and then press ENTER.

To configure named mapping to the certificate

1. Log on to the computer hosting Active Directory.
2. On the Windows desktop, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
3. Expand the domain name, right-click **Computers**, point to **New**, and then click **Computer**.
4. In the **New Object - Computer** dialog box, enter the NetBIOS name of the computer that is hosting the ACS Forwarder, and then click **Next**. Repeat this step for every computer that hosts an ACS Forwarder.
5. In the **Managed** dialog box, ensure that **This is a managed computer** is not selected, and then click **Next**.
6. In the **New Object - Computer** dialog box, click **Finish**.

7. In **Active Directory Computers and Users**, in the right pane, right-click the computer (or computers) you added, and then click **Name Mappings**.
8. In the **Security Identity Mapping** dialog box, click **X.509 Certificates**, and then click **Add**.
9. In the **Add Certificate** dialog box, click the **Look in** menu, select the location where the exported certificate is located, and then click **Open**.
10. In the **Add Certificate** dialog box, ensure that **Use Subject for alternate security identity** is selected, and then click **OK**.
11. In the **Security Identity Mapping** dialog box, click **OK**.
12. Repeat steps 4–11 for each computer you have added.

After you complete these procedures, you need to enable the ACS Forwarders. For more information, see How to Enable Audit Collection Services (ACS) Forwarders.

To export the certificate

1. On the Windows desktop, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **mmc**, and then click **OK**.
3. On the **File** menu, click **Add/Remove Snap-in**.
4. In the **Add/Remove Snap-in** dialog box, click **Add**.
5. In the **Add Standalone Snap-in** dialog box, click **Certificates**, and then click **Add**.
6. In the **Certificates snap-in** dialog box, select **Computer account**, and then click **Next**.
7. In the **Select Computer** dialog box, select **Local computer (the computer this console is running on)**, and then click **Finish**.
8. In the **Add Standalone Snap-in** dialog box, click **Close**.
9. In the **Add/Remove Snap-in** dialog box, click **OK**.
10. In the Console Root\Certificates (Local Computer) pane, expand **Certificates (Local Computer)**, expand **Personal**, and then click **Certificates**.
11. In the results pane, right-click the certificate you are using for Operations Manager, point to **All Tasks**, and then click **Export**.
12. In the **Certificate Export Wizard**, on the **Welcome** page, click **Next**.
13. On the **Export Private Key** page, select **No, do note export the private key**, and then click **Next**.
14. On the **Export File Format** page, select **DER encoded binary X.509 (.CER)**, and then click **Next**.
15. On the **File to Export** page, click **Browse**.
16. On the **Save As** page, select a folder and file name for the certificate, ensure that the **Save as type** is set to **DER Encoded Binary X.509 (*.cer)**, and then click **Save**.

    Note
    You will need to copy this certificate to the computer hosting the ACS Collector, so choose a location that the ACS Collector can read from, or consider saving the certificate to a disk, USB flash drive, or network share. In addition, it is

recommended that you include the computer name in the file name if you are exporting certificates from more than one computer.

17. On the **File to Export** page, ensure that the path and file name are correct, click **Next**, and then click **Finish**.

To run the adtagent command

1. On the Windows desktop, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command prompt, type <*drive_letter*>: (where <*drive_letter*> is the drive where the Operating System is installed), and then press ENTER.
4. Type **cd %systemroot%** and then press ENTER.
5. Type **cd system32** and then press ENTER.
6. Type **adtagent -c** and then press ENTER.
7. You will see a numbered list of certificates. Find the certificate used for Operations Manager, type the number in the list (should be 1), and then press ENTER.
8. Type **exit** to close the command window.

See Also

Collecting Security Events Using Audit Collection Services in Operations Manager

Audit Collection Services Security

Audit Collection Services Capacity Planning

Audit Collection Services Performance Counters

How to Enable Audit Collection Services (ACS) Forwarders

How to Enable Event Logging and ACS Rules on Solaris and AIX Computers

How to Filter ACS Events for UNIX and Linux Computers

Monitoring Audit Collection Services Performance

How to Remove Audit Collection Services (ACS)

Audit Collection Services Administration (AdtAdmin.exe)

Monitoring Audit Collection Services Performance

In System Center 2012 – Operations Manager, the Audit Collection Services (ACS) collector service includes two performance objects that have a total of 16 counters: the Collector object and the Collector Client object. The Collector object has 14 counters, and the Collector Client object has two counters. The counters in the Collector object record performance statistics from

the perspective of the ACS collector. The Collector Client counters record performance statistics from the perspective of a single ACS forwarder.

Performance objects and counters are viewable in Windows Reliability and Performance Monitor, which is a Microsoft Management Console (MMC) snap-in that combines the functionality of previous stand-alone tools including Performance Logs and Alerts, Server Performance Advisor, and System Monitor.

Collector Object

The following table describes each counter in the Collector performance object. If the counter describes information that is added to a specific table in the ACS database, that table is defined in the counter description.

Counter	Description
Connected Clients	The number of ACS forwarders currently connected to the ACS collector.
Database Queue % Full	The ratio of the number of events currently in the ACS database loader queue divided by the highest number of requests that the database loader queue has had. This ratio is expressed as a percentage.
Database Queue Length	The number of events currently in the database loader queue.
DB Loader Events Inserts/sec	The average number of records added, per second, to the dtEvent table in the ACS database, which contains event record entries.
DB Loader Principal Inserts/sec	The average number of records added, per second, to the dtPrincipal table in the ACS database, which contains information about the user and computer accounts that have access to the ACS components.
DB Loader String Inserts/sec	The average number of records added, per second, to the dtString table in the ACS database.
DB Principal Cache Hit %	The percentage of all handling requests that are serviced by the principal cache instead of the dtPrincipal table in the ACS database.
DB Request Queue Length	The number of requests from the ACS collector currently waiting to be serviced by the ACS

Counter	Description
	database. These requests are used during forwarder handshake and during database maintenance. They are not part of normal event handling.
DB String Cache Hit %	The percentage of all handling requests that are serviced by the string cache, thereby avoiding a lookup in the dtString table in the ACS database.
Event time in collector in milliseconds	The amount of time, in milliseconds, between event arrival at the ACS collector and insertion into the ACS database queues.
Incoming Events/sec	The total number of events arriving, per second, at the collector from all connected ACS forwarders.
Interface Audit Insertions/sec	The number of event records, per second, sent by the collector to Windows Management Instrumentation (WMI) for forwarding to an application outside of ACS.
Interface Queue Length	The average number of requests waiting on WMI resources.
Registered Queries	The total number of subscription requests that WMI has received for ACS events since the ACS Collector service was last started.

Collector Client Object

The Collector Client performance object displays statistics about events that occur on a specified ACS forwarder. The ACS Collector Client performance object is installed on the ACS collector. If multiple ACS forwarders are connected to the ACS collector, multiple instances of the counter are displayed. In large environments with more than 100 ACS forwarders connected to an ACS collector, the Collector Client performance object, by default, displays the statistics of the ACS forwarders with the highest asset values. ACS forwarders that have the most audit events are assigned higher asset values to ensure their connections are prioritized over ACS forwarders with fewer events.

Note

Asset values are assigned automatically by the ACS collector. You can change the assigned asset values using AdtAdmin.exe and the *UpdForwarder* parameter. For more

information about the AdtAdmin.exe tool, see Audit Collection Services Administration (AdtAdmin.exe).

The Collector Client performance object has two counters. The following table describes each of these counters.

Counter	Description
Average time between event generation	The average amount of time, in milliseconds, from the creation of an event to the time the event arrives at the ACS collector.
Incoming Audits/sec	The total number of events sent to the ACS collector from the ACS forwarder.

See Also

Collecting Security Events Using Audit Collection Services in Operations Manager

How to Configure Certficates for ACS Collector and Forwarder

Audit Collection Services Capacity Planning

Audit Collection Services Performance Counters

How to Enable Audit Collection Services (ACS) Forwarders

Audit Collection Services Security

How to Filter ACS Events for UNIX and Linux Computers

Audit Collection Services Security

How to Remove Audit Collection Services (ACS)

Audit Collection Services Administration (AdtAdmin.exe)

How to Remove Audit Collection Services (ACS)

Each component of System Center 2012 – Operations Manager Audit Collection Services (ACS) has a separate procedure for removing it.

The ACS collector is removed by using the Audit Collection Services Collector Setup wizard. When you remove the ACS collector, the ACS database is not deleted. You delete the ACS database from within Microsoft SQL Server.

To delete the ACS database you must be a member of the SQL Admins group or have the right to delete a database delegated to you. You must also have read access to the ACS database. As a best practice for security, consider using Run as to perform this procedure.

Because service for the ACS forwarder is part of the Operations Manager agent, you can either disable service for the ACS forwarder and keep the Operations Manager agent or uninstall the agent from the computer. If you do not need to monitor the computer after it is removed from an ACS deployment, you should uninstall the Operations Manager agent. If you want to monitor other services or applications on the computer even though it is no longer acting as an ACS forwarder, you can disable service for the ACS forwarder.

To remove an ACS collector

1. Insert the Operations Manager CD in the management server that you selected to be the ACS collector.
2. On the root of the CD, double-click **SetupOM.exe**. In the **Install** section, click **Audit collection services**. The Audit Collection Services Collector Setup wizard starts.
3. On the **Welcome** page click **Next**.
4. On the ACS Collector Maintenance page, click **Remove the ACS collector** and then click **Next**.
5. On the **Summary** page, the wizard lists the actions it performs to remove the ACS collector. Review the list and click **Next**.
6. When the removal of the ACS collector is complete, click **Finish**.

To delete an ACS database

1. Click **Start**, point to **All Programs**, point to **SQL Enterprise Manager**, and click **Query Analyzer**.
2. In the console tree, right-click the name of the ACS database that you want to remove, click **Delete**, and then click **OK**.

To disable ACS forwarders

1. Log on to the computer with an account that has the rights of the Operations Manager Administrator Operator role. This account must also have the rights of a local administrator on each ACS forwarder.
2. In the Operations console, click **Monitoring**.
3. If you already have already created a state view for ACS, you can skip this step. Right-click in the Monitoring navigation pane, point to **New**, and then click **State View**.
4. In **Name**, type a descriptive name, such as ACS Forwarders, and a short description in **Description**.
5. If necessary, click the **Criteria** tab. In **Show data related to**, click **Agent** and then click **OK**.
6. In the **Actions** pane, under **Health Service Tasks**, click **Disable Audit Collection**. The **Run Task - Enable Audit Collection** dialog box displays.
7. In the **Specify the credentials you want to run the task with** section, click **Other**. In the **User Name** box, type the name of a user account that belongs to the local Administrators group on the agent computers. In the **Password** box, type the password

for this user account. Click to expand the **Domain** drop-down list to view the available domains, and then click the domain of the user account.

8. Click **Run Task**. The Task Status dialog box displays tracking the progress of the task.
9. When the task completes successfully, click **Close**.

See Also

Collecting Security Events Using Audit Collection Services in Operations Manager

How to Configure Certficates for ACS Collector and Forwarder

Audit Collection Services Capacity Planning

Audit Collection Services Performance Counters

How to Enable Audit Collection Services (ACS) Forwarders

Audit Collection Services Security

How to Filter ACS Events for UNIX and Linux Computers

Monitoring Audit Collection Services Performance

Audit Collection Services Security

Audit Collection Services Administration (AdtAdmin.exe)

Audit Collection Services Administration (AdtAdmin.exe)

The primary tool for managing Audit Collection Services (ACS) in System Center 2012 – Operations Manager is a command-line tool, AdtAdmin.exe, which is run locally on an ACS collector. You can use AdtAdmin to view current configurations and change the default configurations that apply to the ACS collector and ACS forwarders. AdtAdmin also allows you to apply filters that limit the events that are stored in the ACS database. These filters are formatted as Windows Management Instrumentation (WMI) Query Language (WQL) queries. (WQL is a subset of the American National Standards Institute Structured Query Language (ANSI SQL) with minor semantic changes to support WMI.)

AdtAdmin Syntax

AdtAdmin has 12 parameters, each of which has a few to several subparameters. The general syntax of AdtAdmin is as follows:

```
AdtAdmin.exe /<Parameter> [/<Subparameter>:<Value>]
```

The following table lists each parameter of AdtAdmin along with a description. For more information about the syntax of a specific parameter, click the name of the parameter in the table to link to the topic that describes it.

Parameter	Description
AdtAdmin.exe /AddGroup	Creates a group on an ACS collector. Groups are used to organize ACS forwarders.
AdtAdmin.exe /DelGroup	Deletes a previously created group on an ACS collector.
AdtAdmin.exe /Disconnect	Disconnects an ACS forwarder or group of forwarders from an ACS collector.
AdtAdmin.exe /GetDBAuth	Displays the authentication method used by the ACS collector to connect to the ACS database.
AdtAdmin.exe /GetQuery	Displays the WQL queries currently in use on an ACS collector. WQL queries are used to filter events before they are saved to the ACS database.
AdtAdmin.exe /ListForwarders	Displays the name and some statistical information on the ACS forwarders that are connected to an ACS collector.
AdtAdmin.exe /ListGroups	Displays the groups that are present on an ACS collector.
AdtAdmin.exe /SetDBAuth	Specifies which authentication method the ACS collector uses to connect to the ACS database. Windows Authentication and SQL authentication are the available authentication methods.
AdtAdmin.exe /SetQuery	Defines a WQL query that the ACS collector uses to filter the audit event data.
AdtAdmin.exe /Stats	Displays statistical information about the ACS forwarders that are connected to an ACS collector.
AdtAdmin.exe /UpdForwarder	Allows you to change the name and the value of an ACS forwarder and also to change the group to which an ACS forwarder belongs
AdtAdmin.exe /UpdGroup	Allows you to rename a group.

Common Subparameters

Each AdtAdmin parameter has from a few to several subparameters. The subparameters allow you to apply a command to a specific ACS collector, a specific ACS forwarder, or group of forwarders and are the same for most AdtAdmin parameters. The subparameters, defined in the following table, can be used with an AdtAdmin parameter unless otherwise noted.

Subparameter	Description
/Collector:CollectorName	Specifies an ACS collector to run a command against. If this subparameter is omitted, the local ACS collector is assumed.
/Forwarder:Name	Specifies an ACS forwarder by its computer name.
/ForwarderID:ForwarderIDNumber	Specifies an ACS forwarder by its identification number. An identification number is assigned to an ACS forwarder when it first connects to the ACS collector.
/ForwarderSID:SID	Specifies an ACS forwarder by its computer security identification number (SID).
/Group:GroupName	Specifies a group of ACS forwarders by the group's name.
/GroupID: IdentificationNumber	Specifies a group of ACS forwarders by the group's identification number. An identification number is assigned to a group when it is first created.
/Value:ValueNumber	Specifies an ACS forwarder or ACS group by its assigned connection value. The ACS collector prioritizes connections from ACS forwarders using connection values that range from -1 through 99. A -1 value means the forwarder is part of an ACS group and that the group's value is used to determine the forwarder's priority. A 0 value means the ACS collector ignores data from that ACS forwarder or group. If event saturation is detected, a collector disconnects forwarders or a group of forwarders with lower values before disconnecting forwarders with higher values.

See Also

Collecting Security Events Using Audit Collection Services in Operations Manager

How to Configure Certficates for ACS Collector and Forwarder

Audit Collection Services Capacity Planning

Audit Collection Services Performance Counters

How to Enable Audit Collection Services (ACS) Forwarders

Audit Collection Services Security

How to Filter ACS Events for UNIX and Linux Computers

Monitoring Audit Collection Services Performance

How to Remove Audit Collection Services (ACS)

Audit Collection Services Security

AdtAdmin.exe /AddGroup

The */AddGroup* parameter creates a group that is used to organize ACS forwarders. The group does not contain any ACS forwarders when it is created. Use the */UpdForwarder* parameter to add ACS forwarders to a group. This command does not generate output. You can use the */ListGroups* parameter to verify that the group was created.

Syntax

```
AdtAdmin.exe /AddGroup [/Collector:<CollectorName>] [/Group:<GroupName>]
```

Subparameter	Description
/Collector:CollectorName	Specifies an ACS collector on which you want to create a group. If this subparameter is omitted, the local ACS collector is assumed.
/Group:GroupName	Specifies the name of the new group. Replace *GroupName* with the name of the new group.

Example

Use the following example to create a group called "Accounting Computers":

```
adtadmin /addgroup /group:"Accounting Computers"
```

See Also

Audit Collection Services Administration (AdtAdmin.exe)

AdtAdmin.exe /DelGroup

AdtAdmin.exe /Disconnect

AdtAdmin.exe /GetDBAuth

AdtAdmin.exe /GetQuery

AdtAdmin.exe /ListForwarders

AdtAdmin.exe /ListGroups

AdtAdmin.exe /SetDBAuth

AdtAdmin.exe /SetQuery

AdtAdmin.exe /Stats

AdtAdmin.exe /UpdForwarder

AdtAdmin.exe /UpdGroup

AdtAdmin.exe /DelGroup

The */DelGroup* parameter deletes a group from an ACS collector by using its name or group identification number. When a group is deleted, the forwarders that belong to the group are not deleted. Any forwarders assigned to a group when it is deleted are added to or still belong to the default top-level groups.

No output is generated from this command. You can use the */ListGroups* parameter to verify that the group was created and also to determine a group's assigned identification number.

Syntax

```
AdtAdmin.exe /DelGroup [/Collector:<CollectorName>] {[/Group:<GroupName>] |
[/GroupID:<IdentificationNumber>]}
```

Subparameter	Description
/Collector:CollectorName	Specifies the ACS collector on which the group was created. If this subparameter is omitted, the local ACS collector is assumed.
/Group:GroupName	Specifies an ACS group to delete by the group's name.
/GroupID:IdentificationNumber	Specifies an ACS group to delete by the group's identification number. An identification number is assigned to a group when it is first

Subparameter	Description
	created.

Example

Use the following example to delete an ACS group that has the name "Accounting Computers":

```
adtadmin /delgroup /group:"Accounting Computers"
```

See Also

Audit Collection Services Administration (AdtAdmin.exe)

AdtAdmin.exe /AddGroup

AdtAdmin.exe /Disconnect

AdtAdmin.exe /GetDBAuth

AdtAdmin.exe /GetQuery

AdtAdmin.exe /ListForwarders

AdtAdmin.exe /ListGroups

AdtAdmin.exe /SetDBAuth

AdtAdmin.exe /SetQuery

AdtAdmin.exe /Stats

AdtAdmin.exe /UpdForwarder

AdtAdmin.exe /UpdGroup

AdtAdmin.exe /Disconnect

The */Disconnect* parameter disconnects a specified ACS forwarder or group of forwarders from the ACS collector. No output is generated from the */Disconnect* parameter. To check an ACS forwarder's status after using the */Disconnect* parameter, use the*/Connected* subparameter of the */Stats* parameter.

Syntax

```
AdtAdmin.exe /Disconnect [/Collector:<CollectorName>] {/Forwarder:<Name> |
/ForwarderSid:<SID> | /Group:<GroupName> | /GroupID:<IdentificationNumber> |
/Value:<ValueNumber>}
```

Subparameter	Definition
/Collector:CollectorName	Specifies an ACS collector you want to disconnect. If this subparameter is omitted, the local ACS collector is assumed.
/Forwarder:Name	Specifies an ACS forwarder by its computer name.
/ForwarderID:ForwarderIDNumber	Specifies an ACS forwarder by its identification number. An identification number is assigned to an ACS forwarder when it first connects to the ACS collector.
/ForwarderSID:SID	Specifies an ACS forwarder by its computer security identification number.
/Group:GroupName	Specifies a group of ACS forwarders by the group's name.
/GroupID: IdentificationNumber	Specifies a group of ACS forwarders by the group's identification number. An identification number is assigned to a group when it is first created.
/Value:ValueNumber	Specifies an ACS forwarder or ACS group by its assigned connection value. The ACS collector prioritizes connections from ACS forwarders using connection values. Connection values range from -1 through 99. A value of -1 means the forwarder is part of an ACS group and that the group's value is used to determine the forwarder's priority. A value of 0 means the ACS collector ignores data from that ACS forwarder or group. If event saturation is detected, a collector will disconnect forwarders or a group of forwarders with lower values before disconnecting forwarders with higher values.

Example

This example disconnects an ACS forwarder named Server1:

```
adtadmin /disconnect /forwarder:"Server1"
```

See Also

Audit Collection Services Administration (AdtAdmin.exe)

AdtAdmin.exe /AddGroup

AdtAdmin.exe /DelGroup

AdtAdmin.exe /GetDBAuth

AdtAdmin.exe /GetQuery

AdtAdmin.exe /ListForwarders

AdtAdmin.exe /ListGroups

AdtAdmin.exe /SetDBAuth

AdtAdmin.exe /SetQuery

AdtAdmin.exe /Stats

AdtAdmin.exe /UpdForwarder

AdtAdmin.exe /UpdGroup

AdtAdmin.exe /GetDBAuth

The */GetDBAuth* parameter displays the current authentication method used by the ACS collector to access the ACS database. The two available authentication methods are Windows Authentication and SQL authentication. If SQL authentication is used, the */GetDBAuth* parameter displays the name of the user account currently in use by the ACS collector to connect to the ACS database.

Syntax

```
AdtAdmin.exe /GetDBAuth [/Collector:<CollectorName>]
```

Subparameter	Definition
/Collector:CollectorName	Specifies an ACS collector whose database authentication account you want to display. If this subparameter is omitted, the local ACS collector is assumed.

Example

This example retrieves the authentication method used by the ACS collector to connect to the ACS Database. In the following example, the local ACS collector is assumed:

```
AdtAdmin /GetDBAuth
```

See Also

Audit Collection Services Administration (AdtAdmin.exe)

AdtAdmin.exe /AddGroup

AdtAdmin.exe /DelGroup

AdtAdmin.exe /Disconnect

AdtAdmin.exe /GetQuery

AdtAdmin.exe /ListForwarders

AdtAdmin.exe /ListGroups

AdtAdmin.exe /SetDBAuth

AdtAdmin.exe /SetQuery

AdtAdmin.exe /Stats

AdtAdmin.exe /UpdForwarder

AdtAdmin.exe /UpdGroup

AdtAdmin.exe /GetQuery

The */GetQuery* parameter lists the Windows Management Instrumentation (WMI) Query Language (WQL) queries that are currently in use as filters on the ACS collector(s). Only the */Collector* subparameter applies to the */GetQuery* parameter.

Note

The */SetQuery* parameter applies a WQL filter. For more information about the */SetQuery* parameter, see **AdtAdmin.exe /SetQuery**.

Syntax

```
AdtAdmin.exe /GetQuery [/Collector:CollectorName]
```

Subparameter	Definition
/Collector:*CollectorName*	Specifies a single ACS collector from which to retrieve a list of current WQL queries that are applied as filters.

See Also

Audit Collection Services Administration (AdtAdmin.exe)

AdtAdmin.exe /AddGroup

AdtAdmin.exe /DelGroup
AdtAdmin.exe /Disconnect
AdtAdmin.exe /GetDBAuth
AdtAdmin.exe /ListForwarders
AdtAdmin.exe /ListGroups
AdtAdmin.exe /SetDBAuth
AdtAdmin.exe /SetQuery
AdtAdmin.exe /Stats
AdtAdmin.exe /UpdForwarder
AdtAdmin.exe /UpdGroup

AdtAdmin.exe /ListForwarders

The */ListForwarders* parameter lists the ACS forwarders, along with some statistics on each, that have ever connected to the ACS collector. The data that displays is a subset of the data that displays using the */Stats* parameter. If no subparameters are used, all ACS forwarders that have ever connected to the ACS collector are included. If you specify an ACS group, all ACS forwarders that belong to the group are listed.

Syntax

```
AdtAdmin.exe /ListForwarders [/Collector:<CollectorName>] {/[Forwarder:<Name>] |
[/ForwarderSid:<SID>] | } {[/Group:<GroupName>] | [/GroupID:<IdentificationNumber>] |
[/Value:<ValueNumber>]}
```

Subparameter	Definition
/Collector:CollectorName	Specifies an ACS collector whose statistics you want to list. If this subparameter is omitted, the local ACS collector is assumed.
/Forwarder:Name	Specifies an ACS forwarder by its computer name.
/ForwarderID:ForwarderIDNumber	Specifies an ACS forwarder by its identification number. An identification number is assigned to an ACS forwarder when it first connects to the ACS collector.
/ForwarderSID:SID	Specifies an ACS forwarder by its computer security identification number.

Subparameter	Definition
/Group:GroupName	Specifies a group of ACS forwarders by the group's name.
/GroupID: IdentificationNumber	Specifies a group of ACS forwarders by the group's identification number. An identification number is assigned to a group when it is first created.
/Value:ValueNumber	Specifies an ACS forwarder or ACS group by its assigned connection value. The ACS collector prioritizes connections from ACS forwarders using connection values. Connection values range from -1 through 99. A value of -1 means the forwarder is part of an ACS group and that the group's value is used to determine the forwarder's priority. A value of 0 means the ACS collector ignores data from that ACS forwarder or group. If event saturation is detected, a collector will disconnect forwarders or a group of forwarders with lower values before disconnecting forwarders with higher values.

Examples

Use the following example to list all ACS forwarders, along with some statistics on each, that have connected to this ACS collector:

```
adtadmin /listforwarders
```

Use the following example to list the ACS forwarders, along with some statistics on each, that belong to the ACS group that has a group identification number of 4:

```
adtadmin /listforwarders /groupid:4
```

Note

Use quotation marks if the name contains spaces.

Use the following example to list statistics on an ACS forwarder that has the name PC 101:

```
adtadmin /listforwarders /forwarder:"PC 101"
```

See Also

Audit Collection Services Administration (AdtAdmin.exe)

AdtAdmin.exe /AddGroup

AdtAdmin.exe /DelGroup
AdtAdmin.exe /Disconnect
AdtAdmin.exe /GetDBAuth
AdtAdmin.exe /GetQuery
AdtAdmin.exe /ListGroups
AdtAdmin.exe /SetDBAuth
AdtAdmin.exe /SetQuery
AdtAdmin.exe /Stats
AdtAdmin.exe /UpdForwarder
AdtAdmin.exe /UpdGroup

AdtAdmin.exe /ListGroups

The output of the */ListGroups* parameter is a comma-separated list of groups that is maintained by an ACS collector. If no subparameters are used, all groups from this ACS collector are listed. None of the subparameters that specify individual ACS forwarders apply to the */ListGroups* parameter.

Syntax

```
AdtAdmin.exe /ListGroups [/Collector:<CollectorName>] {[/Group:<GroupName>] |
[/GroupID:<IdentificationNumber>] | [/Value:<ValueNumber>]}
```

Subparameter	Definition
/Collector:CollectorName	Specifies an ACS collector whose groups you want to list. If this subparameter is omitted, the local ACS collector is assumed.
/Group:GroupName	Specifies a group of ACS forwarders by the group's name.
/GroupID: IdentificationNumber	Specifies a group of ACS forwarders by the group's identification number. An identification number is assigned to a group when it is first created.
/Value:ValueNumber	Specifies an ACS forwarder or ACS group by its assigned connection value. The ACS collector prioritizes connections from ACS forwarders using connection values. Connection values range from -1 through 99.

Subparameter	Definition
	A value of -1 means the forwarder is part of an ACS group and that the group's value is used to determine the forwarder's priority. A value of 0 means the ACS collector ignores data from that ACS forwarder or group. If event saturation is detected, a collector will disconnect forwarders or a group of forwarders with lower values before disconnecting forwarders with higher values.

Example

Use the following example to list all ACS groups defined on this ACS collector:

```
adtadmin /listgroups
```

See Also

Audit Collection Services Administration (AdtAdmin.exe)

AdtAdmin.exe /AddGroup

AdtAdmin.exe /DelGroup

AdtAdmin.exe /Disconnect

AdtAdmin.exe /GetDBAuth

AdtAdmin.exe /GetQuery

AdtAdmin.exe /ListForwarders

AdtAdmin.exe /SetDBAuth

AdtAdmin.exe /SetQuery

AdtAdmin.exe /Stats

AdtAdmin.exe /UpdForwarder

AdtAdmin.exe /UpdGroup

AdtAdmin.exe /SetDBAuth

The */SetDBAuth* parameter specifies the authentication method that the ACS collector uses to access the ACS database. The two available authentication methods are Windows Authentication and SQL authentication. Windows Authentication is the most secure method but can be used only if the computer that runs the ACS collector and the computer that hosts the ACS database belong to the same Active Directory domain or to domains that trust each other.

Using the */Name* and the */Pwd* subparameters automatically configures the ACS collector to use SQL authentication. To check which authentication method the ACS collector is using, run the */GetDBAuth* parameter.

Syntax

To specify that the ACS collector use Windows Authentication, use the following syntax:

```
AdtAdmin.exe /SetDBAuth [/Collector:<CollectorName>]
```

To specify that the ACS collector use SQL authentication and identify the user name and password of the user account that can access the ACS database, use the following syntax:

```
AdtAdmin.exe /SetDBAuth [/Collector:<CollectorName>] /Name:<UserAccount> /Pwd:<Password>
```

Subparameter	Description
/Collector:CollectorName	Specifies an ACS collector whose database authentication account you want to change. If this subparameter is omitted, the local ACS collector is assumed.
/Name:UserAccount	Identifies the new user account name for the ACS collector to use to connect to the ACS database. This subparameter should be used only when you want to use SQL authentication as the authentication method between the ACS collector and the ACS database.
/Pwd:Password	Specifies the password for the user account identified with the */Name* parameter.

Example

Use the following example to change the user account used by the ACS collector to connect to the ACS Database to an account that has a user name of "SQLDatabase" and a password of "SQLPass#1":

```
AdtAdmin /SetDBAuth /Name:SQLDatabase /Password:SQLPass#1
```

See Also

Audit Collection Services Administration (AdtAdmin.exe)

AdtAdmin.exe /AddGroup

AdtAdmin.exe /DelGroup

AdtAdmin.exe /Disconnect

AdtAdmin.exe /GetDBAuth
AdtAdmin.exe /GetQuery
AdtAdmin.exe /ListForwarders
AdtAdmin.exe /ListGroups
AdtAdmin.exe /SetQuery
AdtAdmin.exe /Stats
AdtAdmin.exe /UpdForwarder
AdtAdmin.exe /UpdGroup

AdtAdmin.exe /SetQuery

An ACS collector can use Windows Management Instrumentation (WMI) Query Language (WQL) queries as filters to limit the events that are stored in the ACS database. The */SetQuery* parameter implements the filter before events are saved to the ACS database. For more information on WQL and WQL queries, see Querying with WQL.

Note
Because ACS supports only event queries, it does not support WQL aggregation operators.

Syntax

```
AdtAdmin.exe /SetQuery [/Collector:CollectorName] /Query:QuerySyntax
```

Subparameter	Definition
/Collector:*CollectorName*	Specifies an ACS collector to query. If this subparameter is omitted, the local ACS collector is assumed.
/Query:*QuerySyntax*	Specifies the query syntax that defines the filter to apply.

Example

This example uses the */SetQuery* parameter to define a WQL query that filters out specified events. When applied, this query filters out events generated by System, Local Service, and Network Service services, and it also filters events that have specified event ID numbers.

```
adtadmin /setquery /collector:"Collector Name" /query:"SELECT * FROM AdtsEvent WHERE NOT
((HeaderUser='SYSTEM' OR HeaderUser='LOCAL SERVICE' OR HeaderUser='NETWORK SERVICE') OR
```

```
(EventId=538 OR EventId=566 OR EventId=672 OR EventId=680 OR (EventId>=541 AND
EventId<=547))"
```

See Also

Audit Collection Services Administration (AdtAdmin.exe)

AdtAdmin.exe /AddGroup

AdtAdmin.exe /DelGroup

AdtAdmin.exe /Disconnect

AdtAdmin.exe /GetDBAuth

AdtAdmin.exe /GetQuery

AdtAdmin.exe /ListForwarders

AdtAdmin.exe /ListGroups

AdtAdmin.exe /SetDBAuth

AdtAdmin.exe /Stats

AdtAdmin.exe /UpdForwarder

AdtAdmin.exe /UpdGroup

AdtAdmin.exe /Stats

The */Stats* parameter lists statistical information about ACS forwarders that are connected to the ACS collector. These statistics include identification numbers, SIDs, names, and assigned value numbers. The */Stats* parameter is used to verify recently completed configuration changes and to retrieve information that is needed when using other AdtAdmin parameters, such as */Disconnect* or */Setquery*. All ACS collectors, ACS groups, and ACS forwarders are included in the list unless you specify otherwise. Also, every statistic is listed, by default. If you want only a single statistic, you can specify which statistic that you want to display as part of the command syntax.

Syntax

After you chose a parameter, you can then choose to list all statistics or you can choose to list a particular statistic. This topic includes a table of the parameters that specify the ACS forwarder or group of ACS forwarders that you want to list and a second table that includes the individual statistic subparameters that you can specify.

The syntax of the AdtAdmin.exe /Stats parameter is as follows:

```
AdtAdmin.exe /Stats [/Collector:<CollectorName>] {/[Forwarder:<Name>] |
[/ForwarderSid:<SID>] | [/Value:<ValueNumber>} | {[/Group:<GroupName>] |
[/GroupID:<IdentificationNumber>]} [<StatisticParameter>]
```

Subparameter	Definition
/Collector:CollectorName	Specifies an ACS collector whose statistics you want to list. If this subparameter is omitted, the local ACS collector is assumed.
/Forwarder:Name	Specifies an ACS forwarder by its computer name.
/ForwarderID:ForwarderIDNumber	Specifies an ACS forwarder by its identification number. An identification number is assigned to an ACS forwarder when it first connects to the ACS collector.
/ForwarderSID:SID	Specifies an ACS forwarder by its computer security identification number.
/Group:GroupName	Specifies a group of ACS forwarders by the group's name.
/GroupID: IdentificationNumber	Specifies a group of ACS forwarders by the group's identification number. An identification number is assigned to a group when it is first created.
/Value:ValueNumber	Specifies an ACS forwarder or ACS group by its assigned connection value. The ACS collector prioritizes connections from ACS forwarders using connection values. Connection values range from -1 through 99. A value of -1 means the forwarder is part of an ACS group and that the group's value is used to determine the forwarder's priority. A value of 0 means the ACS collector ignores data from that ACS forwarder or group. If event saturation is detected, a collector disconnects forwarders or a group of forwarders with lower values before disconnecting forwarders with higher values.

The following table lists the available statistic parameters. If you do not list a statistic parameter, all statistics display.

Statistic Parameter	Definition
Average event rate	Displays the average number of events per second received from an ACS forwarder or

Statistic Parameter	Definition
	group of forwarders over the current connection.
Average time to collector	Displays the average number of milliseconds elapsed from the time an event is generated on an ACS forwarder or group of forwarders to the time the ACS collector receives that event.
Connect time	Displays the date and time that an ACS forwarder connected to the ACS collector. This parameter is valid only if the */Connected* parameter has a value of 1 (connected).
Connected	Displays the current connection status of an ACS forwarder or group of forwarders. The value of this parameter is either a 0 (not connected) or a 1 (connected).
Current event rate	Displays the events per second currently being received from an ACS forwarder or group of forwarders.
Last action	Displays the date and time of the last transmission from an ACS forwarder.
Seconds since connection	Displays the number of seconds an ACS forwarder has been connected to the ACS collector. This parameter is valid only if the */Connected* subparameter has a value of 1 (connected).
Total transmitted events	Displays the number of audit events received from an ACS forwarder or group of forwarders over the present connection.
Version	Displays the version of an ACS forwarder's ACS software.

See Also

Audit Collection Services Administration (AdtAdmin.exe)

AdtAdmin.exe /AddGroup

AdtAdmin.exe /DelGroup

AdtAdmin.exe /Disconnect
AdtAdmin.exe /GetDBAuth
AdtAdmin.exe /GetQuery
AdtAdmin.exe /ListForwarders
AdtAdmin.exe /ListGroups
AdtAdmin.exe /SetDBAuth
AdtAdmin.exe /SetQuery
AdtAdmin.exe /UpdForwarder
AdtAdmin.exe /UpdGroup

AdtAdmin.exe /UpdForwarder

Using the */UpdForwarder* parameter, you can change the name and the value of an ACS forwarder and also change the group membership of an ACS forwarder.

Syntax

```
AdtAdmin.exe /UpdForwarder [/Collector:<CollectorName>] {/Forwarder:<Name> |
/ForwarderID:<ForwarderIDNumber> | /ForwarderSid:<SID> | /Group:<GroupName> |
/GroupID:<IdentificationNumber> | /GroupValue:<ValueNumber> | /Value:<ValueNumber>}
{/Name:<NewName> | /Value:<NewValueNumber> /GroupValue:<NewValue>}
```

Subparameter	Definition
/Collector:CollectorName	Specifies the ACS collector to which the ACS forwarder or forwarders sends audit events. If this subparameter is omitted, the local ACS collector is assumed.
/Forwarder:Name	Specifies an ACS forwarder by its computer name.
/ForwarderID:ForwarderIDNumber	Specifies an ACS forwarder by its identification number. An identification number is assigned to an ACS forwarder when it first connects to the ACS collector.
/ForwarderSID:SID	Specifies an ACS forwarder by its computer security identification number.
/Group:GroupName	Specifies a group of ACS forwarders by the group's name.

Subparameter	Definition
/GroupID: IdentificationNumber	Specifies a group of ACS forwarders by the group’s identification number. An identification number is assigned to a group when it is first created.
/Value:ValueNumber	Specifies an ACS forwarder or ACS group by its assigned connection value. The ACS collector prioritizes connections from ACS forwarders using connection values. Connection values range from -1 through 99. A value of -1 means the forwarder is part of an ACS group and that the group's value is used to determine the forwarder's priority. A value of 0 means the ACS collector ignores data from that ACS forwarder or group. If event saturation is detected, a collector will disconnect forwarders or a group of forwarders with lower values before disconnecting forwarders with higher values.
/GroupValue:NewValue	Specifies a new value for a group to which the ACS forwarder belongs.
/Name:NewName	Specifies a new name for the ACS forwarder.
/Value:NewValueNumber	Specifies a new value for the ACS forwarder.

Example

In this example, an ACS forwarder identified as Server1 has a current connection value of 5. This connection value is changed to 3:

```
adtadmin /updforwarder /forwarder:Server1 /value:5 /value:3
```

In this example, an ACS forwarder named "Accounting Computer" is assigned a new configuration value of 99:

```
adtadmin /updforwarder /forwarder:"Accounting Computer" /value:99
```

In this example, a group that contains the ACS forwarder named "Accounting Computer" is assigned a new configuration value of 2:

```
adtadmin /updforwarder /forwarder:"Accounting Computer" /groupvalue:2
```

In this example, the connection value of a group, specified by its identification number, is changed to 50:

```
adtadmin /updforwarder /forwarderid:1 /value:50
```

Note
An ACS forwarder can be a member of only one group at a time. If the ACS forwarder is already a member of an ACS group, running this command removes the forwarder from that group. All names with spaces must be contained within parentheses.

See Also

Audit Collection Services Administration (AdtAdmin.exe)
AdtAdmin.exe /AddGroup
AdtAdmin.exe /DelGroup
AdtAdmin.exe /Disconnect
AdtAdmin.exe /GetDBAuth
AdtAdmin.exe /GetQuery
AdtAdmin.exe /ListForwarders
AdtAdmin.exe /ListGroups
AdtAdmin.exe /SetDBAuth
AdtAdmin.exe /SetQuery
AdtAdmin.exe /Stats
AdtAdmin.exe /UpdGroup

AdtAdmin.exe /UpdGroup

The */UpdGroup* parameter renames an existing group. Groups are used in ACS to organize ACS forwarders.

Syntax

```
AdtAdmin.exe /UpdGroup {/Group:<ExistingName> | /GroupID:<IdentificationNumber>}
/Name:<NewName>
```

Subparameter	Description
/Group	Specifies an ACS group to rename. You can specify the group using its name or identification number.
ExistingName	Identifies the ACS group to rename by its group name.

Subparameter	Description
IdentificatonNumber	Identifies the ACS group to rename by its group identification number.
/Name:*NewName*	Specifies the new name for the ACS group.

Note
A group's identification number can be obtained using the AdtAdmin */ListGroups* command.

Example

Use the following example to rename the Accounting Computers ACS group to "Desktop Computers":

```
AdtAdmin /UpdGroup /Group:"Accounting Computers" /Name:"Desktop Computers"
```

See Also

Audit Collection Services Administration (AdtAdmin.exe)
AdtAdmin.exe /AddGroup
AdtAdmin.exe /DelGroup
AdtAdmin.exe /Disconnect
AdtAdmin.exe /GetDBAuth
AdtAdmin.exe /GetQuery
AdtAdmin.exe /ListForwarders
AdtAdmin.exe /ListGroups
AdtAdmin.exe /SetDBAuth
AdtAdmin.exe /SetQuery
AdtAdmin.exe /Stats
AdtAdmin.exe /UpdForwarder

Connecting Operations Manager With Other Management Systems

Product connectors are used to synchronize System Center 2012 – Operations Manager data with other management systems, such as those that monitor non-Windows computers or create trouble-tickets. Product connectors can integrate a deployment of Operations Manager into

another management platform or connect other management systems into a full Operations Manager management solution.

A unidirectional connector forwards alerts to another management system. A bidirectional connector both forwards alerts to another management system and receives messages from the originating system when the issue is resolved.

Connections to Other Management Systems

Product connectors allow communication between Operations Manager and other management systems, regardless of whether Operations Manager is the highest level management system or not. If Operations Manager is not the top-tier management system, a product connector can forward all Windows-generated alerts for consolidation at another management system. If the connector is bidirectional, Operations Manager can update the state of the monitored component in the Operations Console when it receives notification from the top-level management system. If Operations Manager is the top-tier management system, a product connector allows it to receive and consolidate alert information from another management system.

Operations Manager and Trouble-Ticketing Systems

In Operations Manager, alerts occur when an issue requires action. A trouble-ticketing system can automatically open trouble tickets when it receives an alert generated from Operations Manager via a product connector.

Product Connector Installation

If you want to connect to a particular management system, you should ask the vendor of that management system for a product connector. Installation instructions should be included in the download of the product connector files. After a product connector is installed, you can configure which events you want the product connector to accept or forward using subscriptions. The product connectors you install are displayed in the Administration workspace in **Product Connectors**. See How to Configure a Product Connector Subscription for more information.

Connecting Operations Manager With Other Management Systems topics

How to Configure a Product Connector Subscription

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager

- Initial Monitoring After Operations Manager Is Installed
- Managing Access in Operations Manager
- Getting Information from Operations Manager
- General Tasks in Operations Manager
- Maintenance of Operations Manager
- Operations Manager Report Authoring Guide
- Managing Discovery and Agents

How to Configure a Product Connector Subscription

System Center 2012 – Operations Manager supports the ability to synchronize alert data with other applications, such as other management systems, using product connectors. After a product connector is installed, by default, all alerts are forwarded through the product connector. In the following procedure, you use the Product Connector Subscription Wizard to specify which alerts you want the product connector to forward.

Note

You must have a product connector installed prior to beginning this procedure. Install the product connector according to the product connector vendor's installation instructions.

To configure a subscription for a product connector

1. Log on to the computer with an account that is a member of the Operations Manager Administrators user role.
2. In the Operations console, click **Administration**.
3. In the Administration pane, click **Product Connectors**. In the Product Connectors pane, right-click the product connector and then click **Properties**. The **Product Connector Properties** dialog box displays. In the **Subscriptions** section, click the **Add** button. The **Product Connector Subscription Wizard** starts.

   Note

   Operations Manager internal product connectors are listed in the Operations console. These connectors are used for discovery workflows. Do not create subscriptions for these internal product connectors.
4. On the **General** page, type a name and a short description for the subscription you are creating, and then click **Next**.
5. On the **Groups** page, you can filter which alerts this connector forwards to an external management system based on groups. By default, all check boxes are selected, so alerts from all groups are forwarded. To enable the child check boxes, clear the top-level check box. After you make your selections, click **Next**.
6. On the **Targets** page, you can filter which alerts this connector forwards based on object

type. By default, alerts are accepted from all object types in all management packs. You can specify particular management packs or certain monitored objects from which you want to forward alerts. To accept alerts from only specified types of objects, click **Forward alerts from targets explicitly added to the 'Approved targets' grid are approved** and then click the **Add** button to select individual targets.

7. On the **Criteria** page, you can filter which alerts this connector forwards based on the severity, priority, resolution state, and category of the alert. By default, all criteria are selected, so all alerts are forwarded. However, you can individually select which alerts you want forwarded. After you make your selections, click **Create** to create the product connector subscription. You can view the newly created subscription in the details pane.

See Also

Connecting Operations Manager With Other Management Systems

Monitoring Operations Manager from a Second Management Group

Businesses using System Center 2012 – Operations Manager in multiple management groups sometimes want to monitor one management group from another management group. This topic provides some tips for monitoring one management group (management group A) from a second management group (management group B).

- You can install an agent on management servers in management group A from management group B. If you install the agent manually, configure the agent to report to a management server in management group B.
- Disable Active Directory integration for the agent you install on the management server in management group A.
- To upgrade the management server in management group A, you must remove the management group B agent first.
- After the agent is installed, ensure that you do not configure the agent to also report to management group A (“multihome” the agent).
- Ensure that the Run As accounts for the Default Action Account and Privileged Monitoring Account profiles for the management server in management group B are using credentials that can remotely authenticate and that have sufficient permissions on the management servers in management group A.

See Also

Operations Manager Monitoring Scenarios

Integrating Active Directory and Operations Manager

Connecting Operations Manager With Other Management Systems

Collecting Security Events Using Audit Collection Services in Operations Manager

Monitoring UNIX and Linux Computers by Using Operations Manager

Monitoring .NET Applications

Monitoring Service Level Objectives by Using Operations Manager

Monitoring Networks by Using Operations Manager

Monitoring Clusters by Using Operations Manager

Client Monitoring Using Agentless Exception Monitoring in Operations Manager

Monitoring Across Untrusted Boundaries in Operations Manager

Agentless Monitoring in Operations Manager

Integrating Active Directory and Operations Manager

Integrating Active Directory and Operations Manager topics

- Using Active Directory Domain Services to Assign Computers to Operations Manager Management Groups
- How to Create an Active Directory Domain Services Container for a Management Group
- How to Use Active Directory Domain Services to Assign Computers to Management Servers
- Changing the Active Directory Integration Setting for an Agent

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Initial Monitoring After Operations Manager Is Installed
- Managing Access in Operations Manager
- Getting Information from Operations Manager
- General Tasks in Operations Manager
- Maintenance of Operations Manager
- Operations Manager Report Authoring Guide
- Managing Discovery and Agents

Using Active Directory Domain Services to Assign Computers to Operations Manager Management Groups

System Center 2012 – Operations Manager allows you to take advantage of your investment in Active Directory Domain Services (AD DS) by enabling you to use it to assign agent-managed computers to management groups.

To assign computers to management groups by using AD DS:

- The functional level of AD DS domains must be Windows 2000 native or Windows Server 2003.
- Agent-managed computers and all managements servers in the AD Agent Assignment resource pool must be in the same or two-way trusted domains.

> **Note**
> Regardless of whether AD DS is used to assign computers to a management group, agent-managed computers and their primary management server and secondary management server must be in the same or two-way trusted domains or a gateway server must be used. For more information about gateway servers, see About Gateway Servers in Operations Manager.

Following are the phases for using AD DS to assign computers to Operations Manager management groups.

1. A domain administrator uses MOMADAdmin.exe to create an AD DS container for an Operations Manager management group in the domains of the computers it will manage. The AD DS security group that is specified when running MOMADAdmin.exe is granted Read and Delete Child permissions to the container. By creating a container this way, Operations Manager administrators are given the permission necessary to add management servers to the container and assign computers to them, without needing to be domain administrators.
2. An Operations Manager administrator uses the Agent Assignment and Failover Wizard to assign computers to a primary management server and secondary management server.

   > **Note**
   > Domain controllers cannot be assigned to a management group using Active Directory Domain Services.

3. The Operations Manager agent is deployed using MOMAgent.msi to the desired computers and configured to get its management group information from Active Directory.

   > **Note**
   > Active Directory Integration is disabled for agents that were installed from the Operations console. By default, Active Directory Integration is enabled for agents installed manually using MOMAgent.msi. To disable Active Directory Integration for manual installs, use the command line parameter **USE_SETTINGS_FROM_AD=0** as explained in Install Agent Using the Command Line.

Configuring agents to get their management group information from AD DS is also helpful if your organization uses images to deploy computers. For example, add the Operations Manager agent to the SQL Server 2005 image and configure the agent to get its management group information from Active Directory. When you bring up a new SQL Server 2005 server from an image, the server is automatically configured to be managed by the appropriate Operations Manager management group and download the applicable management packs.

See Also

Integrating Active Directory and Operations Manager

How to Create an Active Directory Domain Services Container for a Management Group

How to Use Active Directory Domain Services to Assign Computers to Management Servers

Changing the Active Directory Integration Setting for an Agent

How to Create an Active Directory Domain Services Container for a Management Group

You can use the following command-line syntax and procedure to create an Active Directory Domain Service (AD DS) container for a System Center 2012 – Operations Manager management group. MOMADAdmin.exe is provided for this purpose and is installed with the Operations Manager management server. MOMADAdmin.exe must be run by an administrator of the specified domain. It can be run on a computer running Microsoft Windows 2000 SP4, Windows XP SP2, and Windows Server 2003 with Microsoft .NET Framework 2.0 installed.

Command line syntax:

<path>\MOMADAdmin.exe <ManagementGroupName> <MOMAdminSecurityGroup> < RunAsAccount> <Domain>

Important
You must put a value inside quotation marks if the value contains a space.

ManagementGroupName is the name of the management group for which an AD container is being created.

MOMAdminSecurityGroup is a domain security group, **domain\security_group** format, which is a member of the Operations Managers Administrators security role for the management group.

- For Active Directory integration to work, the security group must be either a global security group (if Active Directory integration needs to function in multiple domains with 2 way trusts) or a local domain group (if Active Directory integration is only used in one domain)
- To make a security group to be the Management Group Operations Manager Group Administrator, use the following procedure.
  a. In Operations console, select **Administration**.
  b. In the **Administration** workspace, select **User Roles** under **Security**.

c. In **User Roles**, select **Operations Manager Administrators** and click the **Properties** action or right click **Operations Manager Administrators** and select **Properties**.

d. Click **Add** to open the **Select Group** dialog box.

e. Select the desired security group, and then click **OK** to close the dialog box.

f. Click **OK** to close **User Role Properties**.

Note

We recommend one security group, which might contain several groups, be used for the Operations Manager Administrators role. That way, groups and members of groups can be added and removed from groups without a domain administrator needing to perform manual steps to assign them Read and Delete Child permissions to the Management Group container.

RunAsAccount: This is the domain account which will be used by the management server to read, write, and delete objects in AD. Use the format domain\username.

Domain is the name of the domain in which the management group container will be created. MOMADAdmin.exe can be run across domains only if a two-way trust exists between them.

To create an Active Directory Domain Services container for a management group

1. Open the command window.
2. At the prompt, for example, type the following:

   "C:\Program Files\System Center Operations Manager 2012\MOMADAdmin.exe" "Message Ops" MessageDom\MessageMOMAdmins MessageDom\ MessageAdAcct MessageDom
3. The preceding command-line example will:
   a. Run the MOMADAdmin.exe utility from the command line.
   b. Create the **"Message Ops"** Management Group AD DS container in the AD DS schema root of the **MessageDom** domain. To create the same Management Group AD DS container in additional domains, run MOMADAdmin.exe for each domain.
   c. Add the **MessageDom\MessageAdAcct** domain user account to the **MessageDom\MessageMOMAdmin** AD DS security group and assign the security AD DS group the rights necessary to manage the AD DS container.

See Also

Integrating Active Directory and Operations Manager

Using Active Directory Domain Services to Assign Computers to Operations Manager Management Groups

How to Use Active Directory Domain Services to Assign Computers to Management Servers

Changing the Active Directory Integration Setting for an Agent

How to Use Active Directory Domain Services to Assign Computers to Management Servers

The Operations Manager Agent Assignment and Failover Wizard creates an agent assignment rule that uses Active Directory Domain Services (AD DS) to assign computers to a management group and assign the computers' primary management server and secondary management servers. Use the following procedures to start and use the wizard.

Important
The Active Directory Domain Services container for the management group must be created prior to running the Agent Assignment and Failover Wizard.

The Agent Assignment and Failover Wizard does not deploy the agent. You must deploy the agent to the computers using MOMAgent.msi.

Changing the agent assignment rule can result in computers no longer being assigned to, and therefore monitored by, the management group. The state of these computers will change to critical, because the computers no longer send heartbeats to the management group. These computers can be deleted from the management group and, if the computer is not assigned to other management groups, the Operations Manager agent can be uninstalled.

To start the Operations Manager Agent Assignment and Failover Wizard

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. In the Administration workspace, click **Management Servers**.
4. In the **Management Servers** pane, right-click the management server or gateway server to be **Primary Management Server** for the computers returned by the rules you will create in the following procedure, and then click **Properties**.

   Note
   Gateway servers work like management servers in this context.
5. In the **Management Server Properties** dialog box, click the **Auto Agent Assignment** tab, and then click **Add** to start the Agent Assignment and Failover Wizard.

To use the Operations Manager Agent Assignment and Failover Wizard to assign computers to a management group

1. In the **Agent Assignment and Failover Wizard**, on the **Introduction** page, click **Next**.

   Note
   The **Introduction** page does not appear if the wizard has been run and **Do not show this page again** was selected.

2. On the **Domain** page, do the following:

   Note
   To assign computers from multiple domains to a management group, run the **Agent Assignment and Failover Wizard** for each domain.

   - Select the domain of the computers from the **Domain name** drop-down list. The management server and all computers in the AD Agent Assignment resource pool must be able to resolve the domain name.

     Important
     The management server and the computers that you want to manage must be in two-way trusted domains.

   - Set **Select Run As Profile** to the Run As profile associated with the Run As account provided when MOMADAdmin.exe was run for the domain. The default account used to perform agent assignment is the default action account specified during Setup, also referred to as the **Active Directory Based Agent Assignment Account**. This account represents credentials used when connecting to the specified domain's Active Directory and modifying Active Directory objects, and should match the account specified when running MOMAdmin.exe. If this was not the account used to run MOMADAdmin.exe, select **Use a different account to perform agent assignment in the specified domain,** and then select or create the account from the **Select Run As Profile** drop-down list. The **Active Directory Based Agent Assignment Account** profile must be configured to use an Operations Manager administrator account which is distributed to all servers in the AD Agent Assignment resource pool.

     Note
     For more information about Run As profiles and Run As accounts, see Managing Run As Accounts and Profiles.

3. On the **Inclusion Criteria** page, either type the LDAP query for assigning computers to this management server in the text box and then click **Next,** or click **Configure**. If you click **Configure**, do the following:

   a. In the **Find Computers** dialog box, type the desired criteria for assigning computers to this management server.

   b. Click **OK,** and then click **Next**.

      Note
      The following LDAP query will return computers with a name starting with MsgOps, **(&(sAMAccountType=805306369)(objectCategory=computer)(cn=MsgOps*))**. For more information about LDAP queries, see Creating a Query Filter.

4. On the **Exclusion Criteria** page, type the FQDN of computers that you explicitly want to prevent from being managed by this management server, and then click **Next**.

Important
You must separate the computer FQDNs that you type with a semicolon, colon, or a new line (CTRL+ENTER).

5. On the **Agent Failover** page, either select **Automatically manage failover** and click **Create** or select **Manually configure failover**. If you select **Manually configure failover**, do the following:
   a. Clear the check boxes of the management servers to which you do not want the agents to failover.
   b. Click **Create**.

      Note
      With the **Manually configure failover** option, you must run the wizard again if you subsequently add a management server to the management group and want the agents to failover to the new management server.
6. In the **Management Server Properties** dialog box, click **OK**.

Note
It can take up to one hour for the agent assignment setting to propagate in AD DS.

See Also

Integrating Active Directory and Operations Manager

Using Active Directory Domain Services to Assign Computers to Operations Manager Management Groups

How to Create an Active Directory Domain Services Container for a Management Group

Changing the Active Directory Integration Setting for an Agent

Changing the Active Directory Integration Setting for an Agent

You can use the following procedure to change the Active Directory integration setting for an agent.

To change the Active Directory integration setting for an agent

1. On the agent-managed computer, in Control Panel, double-click Operations Manager Agent. (In the category view of Control Panel in Windows Server 2008, Operations Manager Agent is in the **System and Security** category.)
2. On the **Management Group** tab, clear or select **Automatically update management group assignments from AD DS**. If you select this option, on agent startup, the agent

will query Active Directory for a list of management groups to which it has been assigned. Those management groups, if any, will be added to the list. If you clear this option, all management groups assigned to the agent in Active Directory will be removed from the list.

3. Click **OK**.

See Also

Integrating Active Directory and Operations Manager

How to Create an Active Directory Domain Services Container for a Management Group

How to Use Active Directory Domain Services to Assign Computers to Management Servers

Getting Information from Operations Manager

Operations Manager, a component of System Center 2012, collects an immense amount of information about your environment, such as events, performance data, health states, and availability. To use Operations Manager effectively, you need to know how to get the information that is important to you.

Getting Information from Operations Manager topics

- Using the Operations Manager Consoles

  Operations Manager provides an Operations console and a web console that you can use to view and work with the monitoring data for your environment. This section explains how to run the consoles and describes the information and tasks available in each workspace in the Operations console.

- Finding Data and Objects in the Operations Manager Consoles

  The Operations Manager consoles provide find, scope, and search functions to help you filter and locate specific data and objects. This section explains how to use these functions effectively.

- Using Views in Operations Manager

  Views are one of your primary monitoring tools. This section describes the standard views included in Operations Manager, and explains how to create, customize, and target views.

- Using SharePoint to View Operations Manager Data

  Dashboard views from Operations Manager can be displayed on a SharePoint site, which is useful for providing current status views to individuals in your organization who are not

Operations Manager users. This section explains how to display dashboard views in SharePoint.

- Subscribing to Alert Notifications

  Operations Manager can send notifications of alerts by email, text (SMS) message, and instant message, and can execute commands in response to alerts. This section explains how to set up the channels for notifications and how to configure subscribers and subscriptions.

- Using Reports in Operations Manager

  Reports are a valuable tool for communicating status and trends. This section explains how to use the standard reports that are provided in Operations Manager

- Not Monitored and Gray Agents

  This topic explains what is going on when you see agents in a “gray” state or labeled as “not monitored”.

- How to View All Rules and Monitors Running on an Agent-Managed Computer

  This topic explains how to view all rules and monitors running on an agent-managed computer.

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Initial Monitoring After Operations Manager Is Installed
- Managing Access in Operations Manager
- Operations Manager Monitoring Scenarios
- General Tasks in Operations Manager
- Maintenance of Operations Manager
- Operations Manager Report Authoring Guide

Using the Operations Manager Consoles

Using the Operations Manager Consoles topics

- Comparing the Operations Console and Web Console in Operations Manager
- How to Connect to the Operations Console
- How to Connect to the Web Console
- Using the Monitoring Workspace in Operations Manager
- Using Health Explorer in Operations Manager
- Using My Workspace in Operations Manager

- Using the Administration Workspace in Operations Manager
- Using the Reporting Workspace in Operations Manager
- Using the Authoring Workspace in Operations Manager

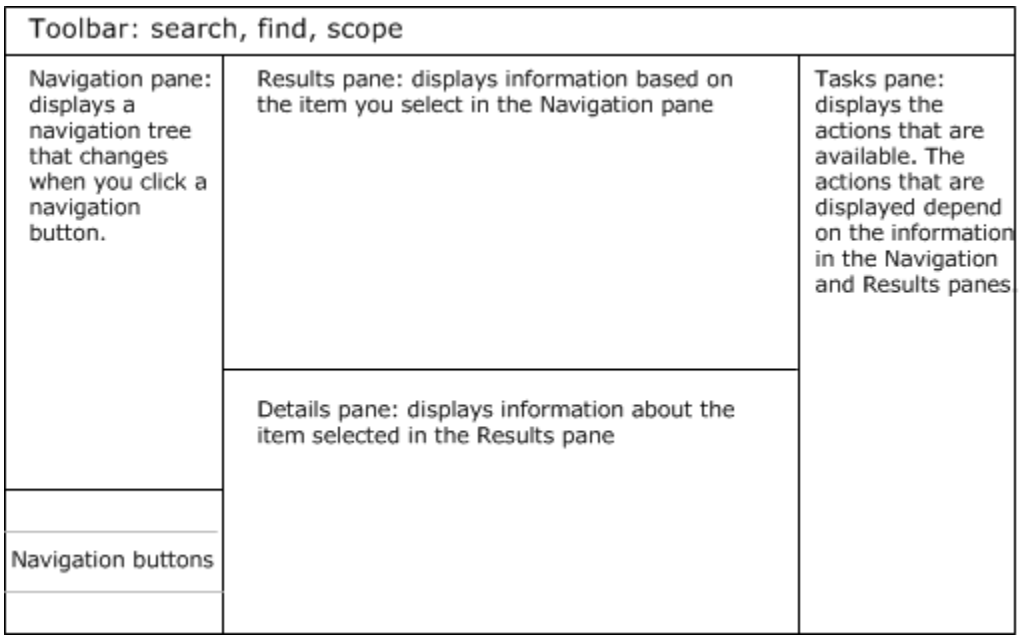
See Also

Getting Information from Operations Manager

Comparing the Operations Console and Web Console in Operations Manager

System Center 2012 – Operations Manager operators use a console to view monitoring data. The consoles available are the Operations console and the web console. The Operations console allows you to perform all actions that your user role allows, while the web console displays only My Workspace and the Monitoring workspace.

Both consoles share a similar layout:



Each navigation button opens a specific workspace, such as Monitoring or Administration. In the Operations console, the following navigation buttons may be available, depending on the user role you are assigned:

In the web console, only Monitoring and My Workspace are available:

Tip

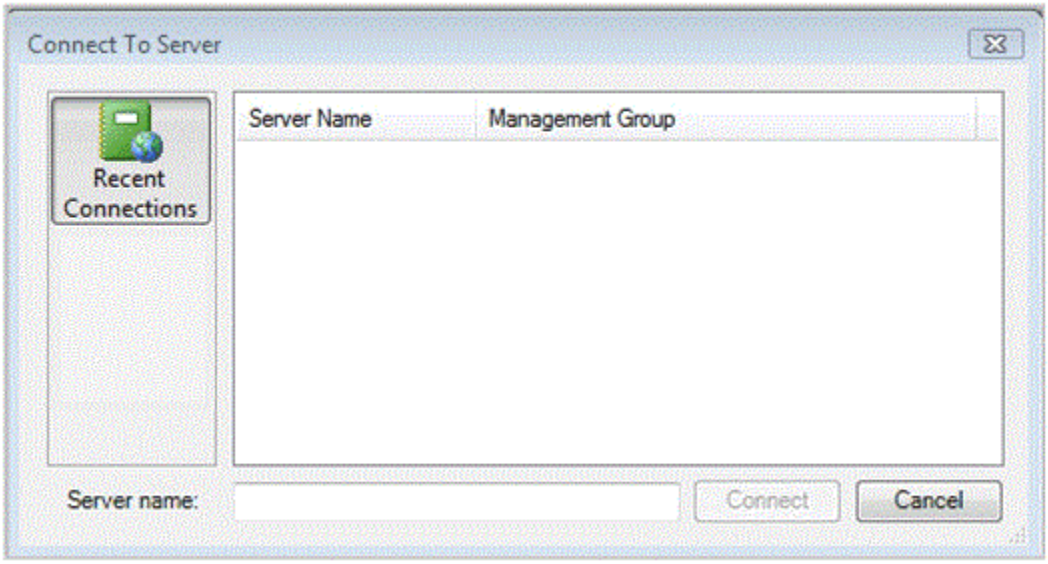
In the Operations console, you can change the navigation buttons into small icons and increase the space available in the navigation pane by clicking on the top border of the navigation buttons and dragging downward. You can also hide and reveal the navigation and task panes.

There are a few differences between the Operations console and web console that you should be aware of:

- There are minor differences in sort. For example, in the web console, when you sort alerts, only the alerts visible on the page are sorted rather than all alerts.
- Fewer alerts display per page in the web console.
- You cannot run tasks that require elevated access in the web console.
- You do not have the options to show, hide, personalize, or create views in the web console, although you can create a dashboard view in My Workspace in the web console.
- There are no subscription options in the web console.

How to Connect to the Operations Console

The System Center 2012 – Operations Manager Operations console can be installed on any computer that meets the system requirements. When you open the Operations console on a management server, the console connects to that management server, however you can use the following procedure to connect to a different management server. When you initially open the Operations console on a computer that is not a management server, you must specify the management server to connect to. The following image shows the **Connect To Server** dialog box.



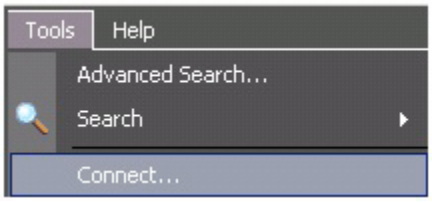
To connect an Operations console to a management server

1. Click **Start**, click **All Programs**, click **System Center Operations Manager 2012**, and click **Operations Console** to open the Operations console.
2. In the **Connect To Server** dialog box, type in the server name or select a server from the list. (In the image above, the console has not yet connected to any management group. If the console has previously connected to any management servers, the servers will be listed in **Recent Connections**.)

The Operations console opens with the focus on the most recently viewed workspace. For example, if the Authoring workspace is selected when the console is closed, the next time that the console is started, it will open to the Authoring workspace. To switch to a different workspace, click the appropriate navigation button.

To change the management server that the Operations console is connected to

- In the Operations console, click **Tools** and then click **Connect** as shown in the following image, which will open the **Connect To Server** window.



See Also

Comparing the Operations Console and Web Console in Operations Manager

Connecting Management Groups in Operations Manager
Using the Reporting Workspace in Operations Manager
Using the Administration Workspace in Operations Manager
Using My Workspace in Operations Manager
Using Health Explorer in Operations Manager
Using the Monitoring Workspace in Operations Manager
How to Connect to the Web Console
Using the Authoring Workspace in Operations Manager
Using the Operations Manager Consoles

How to Connect to the Web Console

In System Center 2012 – Operations Manager, the web console provides a monitoring interface for a management group that can be opened on any computer that has connectivity to the web console server. The web console is limited to My Workspace and the Monitoring workspace.

Note

You must use Internet Explorer 7, Internet Explorer 8, or Internet Explorer 9 to connect to the Operations Manager web console. In addition, the Operations Manager web console requires that JavaScript be enabled. To enable JavaScript in Internet Explorer, open **Internet Options**, and click the **Security** tab. Select the zone for the web console (Internet, Local intranet, or Trusted sites), and then click **Custom level**. Enable **Active scripting**, click **OK**, click **OK**, and then connect to the web console.

The Operations Manager environment must have the web console installed on a management server for users to connect to the web console by using a web browser.

By default, the web console session is limited to 30 minutes. You can change this limit by editing the web.config file (Program Files\System Center Operations Manager 2012\WebConsole\WebHost) and changing the autoSignOutInterval value from “30” to a shorter or longer interval, or disable the session limit by changing the value to “0”, as shown in the following example.

```
<connection autoSignIn=”true” autoSignOutInterval=”0”>
```

Note

After you change the web.config file, you must open a new web console session for the changes to take effect.

To connect to a web console

- Open a web browser on any computer and enter **http://***servername*/**OperationsManager**, where *servername* is the name of the computer hosting the web console.

For information on installing the web console, see Deployment Guide for Operations Manager 2012.

See Also

Comparing the Operations Console and Web Console in Operations Manager

Using the Monitoring Workspace in Operations Manager

Using My Workspace in Operations Manager

Managing Alerts

Using the Monitoring Workspace in Operations Manager

In System Center 2012 – Operations Manager, the Monitoring workspace is the primary workspace for operators. The Monitoring workspace is basically the same in both the Operations and Web consoles.

When you open the Monitoring workspace, you see an overview that summarizes the health of distributed applications and computers, as well as the objects that are in maintenance mode, as shown in the following image.

In the **State and Alerts** overview, click any of the numbers to see a detailed view. For example, if you click the number shown for **Maintenance Mode**, a state view of all computers in maintenance mode opens.

The health states that are summarized in the overview only tell you part of what is going on in your environment. You will also want to review the alerts that have been generated. In the navigation pane, click **Active Alerts** to see all alerts. For more information about dealing with alerts, see Managing Alerts.

There are number of views in the **Monitoring** workspace that allow you to view the status of your environment. For information on each view, see Standard Views in Operations Manager. You can change the display options of a view and save it as a personalized view. For more information, see How to Personalize a View in Operations Manager.

As you work with Operations Manager, you may discover that there are specific views that you frequently access. You can create a customized workspace that displays your favorite views and searches. For more information, see Using My Workspace in Operations Manager.

See Also

Using My Workspace in Operations Manager

Comparing the Operations Console and Web Console in Operations Manager

Standard Views in Operations Manager

How to Personalize a View in Operations Manager

Finding Data and Objects in the Operations Manager Consoles

Using the Reporting Workspace in Operations Manager

Using the Administration Workspace in Operations Manager

Using My Workspace in Operations Manager

Using Health Explorer in Operations Manager

Using the Authoring Workspace in Operations Manager

How to Connect to the Web Console

How to Connect to the Operations Console

Using the Operations Manager Consoles

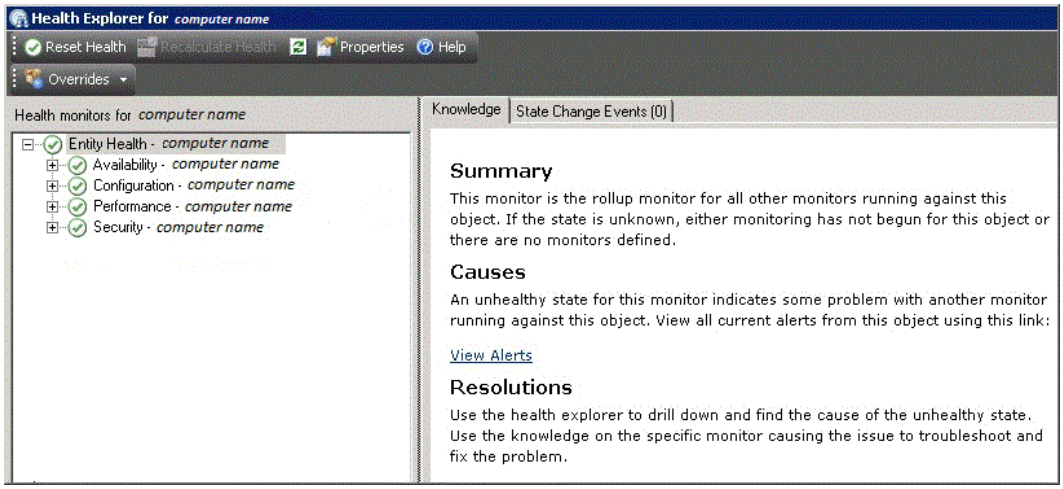
Using Health Explorer in Operations Manager

In System Center 2012 – Operations Manager, you can use the Health Explorer tool to define and diagnose failures on your network. Health Explorer gives you the ability to view and then take action on alerts, state changes, and other significant issues generated by monitoring objects on your network.

You can start Health Explorer from the **Tasks** pane after you select an object, alert, or event in the results pane. Health Explorer organizes health information into the following categories:

- Performance
- Security
- Availability
- Configuration

All monitors and rules that are defined for a selected object display in the appropriate category.



The icons used to indicate state are as follows:

Icon	Meaning
	Unknown, unmonitored (blank)
	Success, health is OK (green)
	Warning (yellow)
	Critical (red)
	Maintenance mode (gray)
	Out of contact (gray)

By default, when the Health Explorer windows first opens, all monitors that are in a failed, or red, state are expanded. If a monitor contains other monitors, as in the case of a roll-up monitor, all monitors are shown in a hierarchical layout so that monitoring data for all dependent services and applications is displayed. If you want to view more detail on any dependent monitor, right-click that monitor and then click **Monitor Properties** to open another Health Explorer window.

When the Health Explorer window is open, you can review a history of diagnostic tests that have run automatically and the output from those tasks. You can also run additional diagnostic tasks. Any task that is formatted as a hyperlink can run directly from the **Knowledge** tab.

The Health Explorer window refreshes automatically every 30 seconds. Press the F5 function key for an immediate refresh.

For more information on using Health Explorer, see Using Health Explorer to Investigate Problems.

See Also

Using the Reporting Workspace in Operations Manager

Using the Administration Workspace in Operations Manager

Using My Workspace in Operations Manager

Using the Authoring Workspace in Operations Manager

Using the Monitoring Workspace in Operations Manager

How to Connect to the Web Console

How to Connect to the Operations Console

Using the Operations Manager Consoles

Using My Workspace in Operations Manager

My Workspace provides you with a private area in the Operations console that you can customize for your specific needs. Using My Workspace, you can create folders to organize the workspace, add shortcuts to favorite views, save useful searches, and create views that are only visible to you. Your configuration of My Workspace will be available to you in any Operations console that you log in to using the same Windows credentials.

This topic contains the following procedures:

- Create Folders in My Workspace
- Add Shortcuts to Views
- Save Searches
- Create Views

Create Folders in My Workspace

My Workspace contains two default folders: **Favorite Views** and **Saved Searches**. You can create additional folders to better organize your workspace. All new folders that you create will be created under **Favorite Views**.

To create a new folder in My Workspace

1. Right-click in the navigation pane.

   Note
   To create a nested folder, right-click the folder in which you want to create a child folder, and then continue to step 2.
2. Point to **New** and click **Folder**.
3. Type a folder name, and then click **OK**.

Add Shortcuts to Views

In My Workspace, you can add shortcuts to any existing views in the Monitoring workspace.

To add a view to My Workspace

1. In the **Monitoring** workspace, select a view, right-click, and then click **Add to My Workspace**.
2. Specify the folder in My Workspace where you want the view to appear.
3. Click **OK**.

When you go to My Workspace, you will see the view that you added listed in the navigation pane.

Save Searches

You can save useful searches in My Workspace to run at any time.

To save a search in My Workspace

1. Click **Saved Searches**.
2. In the **Tasks** pane, click **Create New Search**.
3. In the **Advanced Search** window, select the object type for your search. Your options are:
   - Alerts
   - Events
   - Managed Objects
   - Monitors
   - Object Discoveries
   - Rules
   - Tasks
   - Views

   Each object type will display a unique set of criteria for your search. For more information on advanced search criteria, see Using Advanced Search.
4. In the displayed criteria for the object type, select the condition that you want to search

against.

5. Each condition that you select is added to the **Criteria description**. Click the underlined value in each condition to edit the value. After you edit a value, click **OK** and then edit the next value. Continue until all conditions have values specified.
6. Click **Save parameters to My Favorites**.
7. Enter a name for the saved search and click **OK**.

You can run saved searches right-clicking a search in the list and then clicking **Search Now**.

Create Views

Views that you create in My Workspace are unique views, not shortcuts to existing views. As an operator, you can create views in the My Workspace pane. You must have the rights of the Author role to create a view in the Monitoring workspace.

Note

The general instructions in the following procedure do not apply to Diagram, Web Page, or Dashboard views. For more information on creating a view, see the specific view type in Creating Views in Operations Manager.

To create a view in My Workspace

1. Right-click in the folder where you want to store the view and point to **New**. You can select any view type. For more information on the view types available, see View Types in Operations Manager.
2. In the view properties, enter a name and description for the view. The view properties dialog box contains two tabs: **Criteria** and **Display**.

   On the **Criteria** tab, in the **Show data related to** field, specify the item to target. The item you select will display related conditions in the **Select conditions** section. For more information, see Guidance for Scoping and Targeting Views.

   After you select a condition, you can edit the value for that condition in the **Criteria description** section.
3. In the **Show data contained in a specific group** field, you can select a group to limit the search results to members of that group.
4. On the **Display** tab, select the columns that you want displayed in the view. You can also specify how to sort the columns and group the items.
5. After you have specified the conditions and values for the view, click **OK**. The new view will appear in the navigation pane.

See Also

Standard Views in Operations Manager

How to Personalize a View in Operations Manager

Using Advanced Search
Guidance for Scoping and Targeting Views
Using the Reporting Workspace in Operations Manager
Using the Administration Workspace in Operations Manager
Using the Authoring Workspace in Operations Manager
Using Health Explorer in Operations Manager
Using the Monitoring Workspace in Operations Manager
How to Connect to the Web Console
How to Connect to the Operations Console
Using the Operations Manager Consoles

Using the Administration Workspace in Operations Manager

In the System Center 2012 – Operations Manager Operations console, the Administration workspace is the primary workspace for administrators. You use the Administration workspace to configure a management group and its managed objects.

When you first open the Administration workspace or when you click **Administration** in the navigation pane, the Administration Overview opens, which displays task links for any required or optional configuration steps that have not been completed yet.

The sections below describe the different options in the Administration workspace and link to more detailed information about the task or option.

Connected Management Groups

You can connect management groups to enable the forwarding of alerts and other monitoring data from a connected management group to the local management group. Tasks can be initiated from a local management group to run on managed objects of a connected management group.

Use **Connected Management Groups** in the Administration workspace to connect a management group or to edit the properties of a connected management group.

For more information, see Connecting Management Groups in Operations Manager.

Device Management

You can use **Device Management** in the Administration workspace to perform configuration of specific management servers, agent-managed computers, agentless-managed computers, UNIX servers, and Linux servers. The following table summarizes the uses of the items in Device Management and provides links to more detailed information.

Item	Use	For more information
Agent Managed	To modify the configuration of agent-managed computers, such as: • Change the primary management server for agent-managed computers. • Repair the agent installation. • Uninstall an agent. • Override the management group agent heartbeat settings on a specific agent. A heartbeat is a periodic pulse from an agent to its management server. • Configure an agent-managed computer as a proxy for agentless-managed computers.	• Managing Discovery and Agents • Agentless Monitoring in Operations Manager
Agentless Managed	To change the proxy agent for an agentless-managed computer. The proxy agent can be any agent-managed computer in the management group configured to be a proxy.	Agentless Monitoring in Operations Manager
Management Servers	To modify the configuration of management servers, such as: • Override the management group heartbeat failure setting and configure the number of missed heartbeats a management server will allow for an agent before it changes the state of the respective computer to critical. • Override the Management Group Manual Agent Installs setting and configure a management server to reject or put in	• How Heartbeats Work in Operations Manager • Managing Discovery and Agents • Agentless Monitoring in Operations Manager • How to Configure the Internet Proxy Settings for an Operations Manager 2012 Management Server in the Deployment Guide

Item	Use	For more information
	Pending Management agents installed with MOMAgent.msi. • Configure a management server as a proxy for agentless managed computers. • Configure the Internet proxy settings for a management server.	
Pending Management	To approve or reject an agent that was installed with MOMagent.msi if the management group for the agent is configured to **Review new manual agent installations in pending management view** but not **Auto-approve new manually installed agents**. Agents pending approval are displayed for this item.	Process Manual Agent Installations
UNIX/Linux Servers	To modify the configuration of agent-managed UNIX and Linux servers.	• Managing Discovery and Agents • Monitoring UNIX and Linux Computers by Using Operations Manager

Management Packs

When you select **Management Packs** in the Administration workspace, you see a list of all management packs imported into your management group. When you right-click an individual management pack in the results pane, you can view its properties, delete it, or export any customizations to another management group. You can use links in the tasks pane to create, import, and download management packs.

For more information, see Using Management Packs.

Network Management

You can use **Network Management** in the Administration workspace to discover network devices and managed discovered network devices. The following table summarizes the uses of the items in Network Management and provides links to more detailed information.

Item	Use	For more information
Discovery Rules	• To create rules for discovering network devices • To modify existing discovery rules	How to Discover Network Devices in Operations Manager
Network Devices	To view properties of discovered network devices	Monitoring Networks by Using Operations Manager
Network Devices Pending Management	To retry or reject discovered network devices that are pending management	How to Discover Network Devices in Operations Manager

Notifications

Notifications generate messages or run commands automatically when an alert is raised on a monitored system. By default, notifications for alerts are not configured. For Operations Manager users to be notified immediately when an alert is generated, you need to configure a channel for notifications, add subscribers, and then create a notification.

In **Notifications** in the Administration workspace, you can create channels, subscribers, subscriptions, and modify the channels, subscribers, and subscriptions that you create. For more information, see Subscribing to Alert Notifications.

Product Connectors

Product connectors are used to synchronize Operations Manager data with other management systems such as those that monitor non-Windows computers or create trouble-tickets. Product connectors can integrate a deployment of Operations Manager into another management platform or connect other management systems into a full Operations Manager management solution. Any product connectors that you integrate with Operations Manager will be displayed in this section of the Administration workspace.

When you install Operations Manager, two internal product connectors are installed. These are used by Operations Manager.

For more information, see Connecting Operations Manager With Other Management Systems.

Run As Configuration

You can use **Run As Configuration** in the Administration workspace to manage Run As accounts and profiles. The following table summarizes the uses of the items in **Run As Configuration** and provides links to more detailed information.

Item	Use	For more information
Accounts	To modify the credentials and distribution for Run As accounts.	Managing Access in Operations Manager
Profiles	To add, edit, and remove Run As accounts associated with a Run As profile.	Managing Access in Operations Manager

Security

In Operations Manager, operations such as resolving alerts, running tasks, overriding monitors, viewing alerts, viewing events, and so on have been grouped into user roles, with each user role representing a particular job function. Role-based security allows you to limit privileges that users have for various aspects of Operations Manager. In **Security** in the Administration workspace, you can add and remove users to specific user roles. You can also modify the properties of user roles that you create.

For more information, see Implementing User Roles.

Settings

The following table summarizes the settings you can manage in **Settings** in the Administration workspace.

Item	Use	For more information
Agent Heartbeat	Agents generate a heartbeat at specific intervals to ensure they are operating properly. You can adjust the interval.	How Heartbeats Work in Operations Manager
Alerts	• To configure alert resolution states. • To configure automatic alert resolution.	• How to Set Alert Resolution States • How to Configure Automatic Alert Resolution
Database Grooming	To configure how long different types of data should be retained	Maintenance of Operations

Item	Use	For more information
	in the operational database.	Manager
Privacy	To modify the settings for the following programs: • Customer Experience Improvement Program (CEIP) • Operational Data Reporting • Error Reporting	Sending Data to Microsoft in the Deployment Guide
Reporting	Configure the path for the reporting server.	Using the Reporting Workspace in Operations Manager
Web Addresses	Designate web addresses for the Web console and online company knowledge.	How to Connect to the Web Console
Server Heartbeat	Configure the number of missed heartbeats before the management server pings the agent-managed computer.	How Heartbeats Work in Operations Manager
Server Security	Specify how the management server should handle manually-installed agents.	Process Manual Agent Installations

See Also

Using the Reporting Workspace in Operations Manager

Using the Authoring Workspace in Operations Manager

Using My Workspace in Operations Manager

Using Health Explorer in Operations Manager

Using the Monitoring Workspace in Operations Manager

How to Connect to the Web Console

How to Connect to the Operations Console

Using the Operations Manager Consoles

Using the Reporting Workspace in Operations Manager

System Center 2012 – Operations Manager provides extensive reporting capabilities, including multiple report libraries that you can select from to customize reports for your specific requirements. Reports perform a query against the data warehouse database and return the results in an easy-to-read format.

Important
Users must be a member of the Report Operator Users role to run reports.

Reporting

Reporting in the Reporting workspace contains all reports installed with Operations Manager, as well as those reports included in management packs that you have imported.

The report library contains generic reports (for example, Availability and Configuration Changes reports). Generic reports have no specified context. The context for the report is defined in the parameter header, located at the top of the Report window.

For more information on using the reports library, see Using Reports in Operations Manager.

Authored Reports

Authored reports are based on existing reports from the report library. You configure a report with prepopulated parameters and then make it available to other users.

After you run a report, click **File**, and then click **Publish** to publish the report with the configured parameters to **Authored Reports**.

Favorite Reports

You can save configured reports to **Favorite Reports** to make them continually available to you and to save you the time of reconfiguring a report you run frequently.

After you run a report, click **File**, and then click **Save to favorites** to save the report.

Scheduled Reports

You can schedule configured reports to run on a one-time or recurring basis.

After you run a report, click **File**, and then click **Schedule** to configure the report subscription. For more information, see Scheduling Reports.

See Also

Using the Authoring Workspace in Operations Manager

Using the Administration Workspace in Operations Manager

Using My Workspace in Operations Manager

Using Health Explorer in Operations Manager

Using the Monitoring Workspace in Operations Manager

How to Connect to the Web Console

How to Connect to the Operations Console

Using the Operations Manager Consoles

Using the Authoring Workspace in Operations Manager

The options in the Authoring workspace allow you to create new monitoring scenarios. This could be to change or add monitoring in an existing management pack or to create a new management pack for an application that doesn't have one.

Authoring is described in detail in the Operations Manager 2012 Authoring Guide. The sections below describe the different options in the Authoring workspace.

Management Pack Templates

Management Pack Templates allow you to create complete monitoring scenarios with minimal input. Once you complete a wizard, the management pack template creates monitors, rules, and even classes to implement the particular scenario. There is no requirement for you to understand the management pack elements that are created since you can continue to use the template to perform configuration. It will make any necessary modifications to the underlying elements.

OLE DB Data Source	Monitor the availability and performance of a database. Sample queries can be executed from one or more watcher nodes.
Process Monitoring	Monitor the availability and performance of a wanted process or verify that an unwanted process is not running.
TCP Port	Monitor the availability of an application listening on a specific TCP port. Test can be performed from one or more watcher nodes.
Unix/Linux LogFile	Monitor a Unix or Linux log file for a specific log

	entry one a specific computer or group of computers.
Unix/Linux Service	Monitor the availability of a service on a Unix or Linux computer or group of computers.
Windows Service	Monitor the availability and performance of a service running on one or more Windows computers.

Distributed Applications

Distributed Applications allow you to group together multiple components that are part of a single application. The health of each included object are used to calculate an overall health for the application itself. This health can be used to support alerts, views, and reports.

Groups

Groups contain a particular set of managed objects. They are used to scope views, reports, and certain monitoring scenarios. Criteria can be provided to automatically populate a group based on properties of the objects, or you can add specific objects to a group.You can create new groups and edit existing groups. You can also view the current members of a group. Once it has been created, a group can be used in the Monitoring workspace for scoping views, the Reporting workspace for scoping reports, or in the Authoring workspace for overrides, management pack templates, or service level objects.

Management Pack Objects

The Management Pack Objects section provides access to the different elements that are available. Depending on the kind of object, you may be able to create new objects, edit existing objects, or view existing objects.

Attributes	An *attribute* is a property of a class in a management pack. You can add additional attributes to collect additional information about managed objects. These attributes can be used to support group membership or accessed by monitors or rules.
Monitors	*Monitors* are workflows that run on an agent and determine the current health of an object. Each monitor uses a particular data source as the event log, performance data, or a script to

	collect its information. You can create new monitors and edit existing monitors in the Operations console for specific monitoring scenarios which will address the requirements of most users. More complex monitors must be created and modified using the Authoring console.
Object Discoveries	*Object Discoveries* are workflows that run on an agent and discover objects to manage. You cannot create new object discoveries in the Operations console. You can view existing object discoveries in management packs and use overrides to modify the frequency that they run and potentially other parameters.
Overrides	*Overrides* are used to change parameters on workflows including monitors, rules, and discoveries. Overrides are created from the property page of the workflow that they apply to. This option allows you to view and modify existing overrides.
Rules	*Rules* are workflows that run on an agent that create an alert, collect information for analysis and reporting, or run a command on a schedule. Each rule uses a particular data source as the event log, performance data, or a script to collect its information. You can create new rules and edit existing rules in the Operations console for specific monitoring scenarios which will address the requirements of most users. More complex rules must be created and modified using the Authoring console.
Service Level Tracking	*Service Level Tracking* allows you to compare the availability of managed objects to a specific object. This option allows you to create new *Service Level Objectives* and edit existing Service Level Objectives.

Tasks	*Tasks* are workflows that run when you request them in the Operations console. *Agent tasks* run on one more agent computers. *Console tasks* run on the Operations console workstation. You can create new tasks and edit existing tasks in the Operations console for specific monitoring scenarios which will address the requirements of most users. More complex tasks must be created and modified using the Authoring console.
Views	*Views* display managed objects and collected data in the Operations Console. Views are created and modified in the Monitoring workspace. This option displays the existing views available for each target class.

See Also

Using the Reporting Workspace in Operations Manager

Using the Administration Workspace in Operations Manager

Using My Workspace in Operations Manager

Using Health Explorer in Operations Manager

Using the Monitoring Workspace in Operations Manager

How to Connect to the Web Console

How to Connect to the Operations Console

Using the Operations Manager Consoles

Finding Data and Objects in the Operations Manager Consoles

System Center 2012 – Operations Manager, with the appropriate management packs imported, will provide you with a comprehensive view of what is going on with your monitored applications, hardware, and processes. This can result in a very large volume of data being displayed in the Operations console. Learning how to quickly locate the data you need is essential to efficient interaction with the console. You can use the **Scope**, **Find**, and **Search** buttons on the Operations console toolbar to filter your view of monitoring data so that you can find the exact

monitoring object or group of objects that you need. You can also filter your data based on the number of hours or days you would like to show.

Note
Any time that you do not see the information you expect in the results pane, check the scope and time filters to ensure that the correct objects and time period are set for the results you need.

The **Scope**, **Search**, **Find**, and **Time** tools apply a temporary filter to the data you are viewing in the console. While you can locate a specific object using Search or Find, you can also use Scope or Time to display a set of objects that meet a set of criteria. The following table shows the differences between the different filtering options.

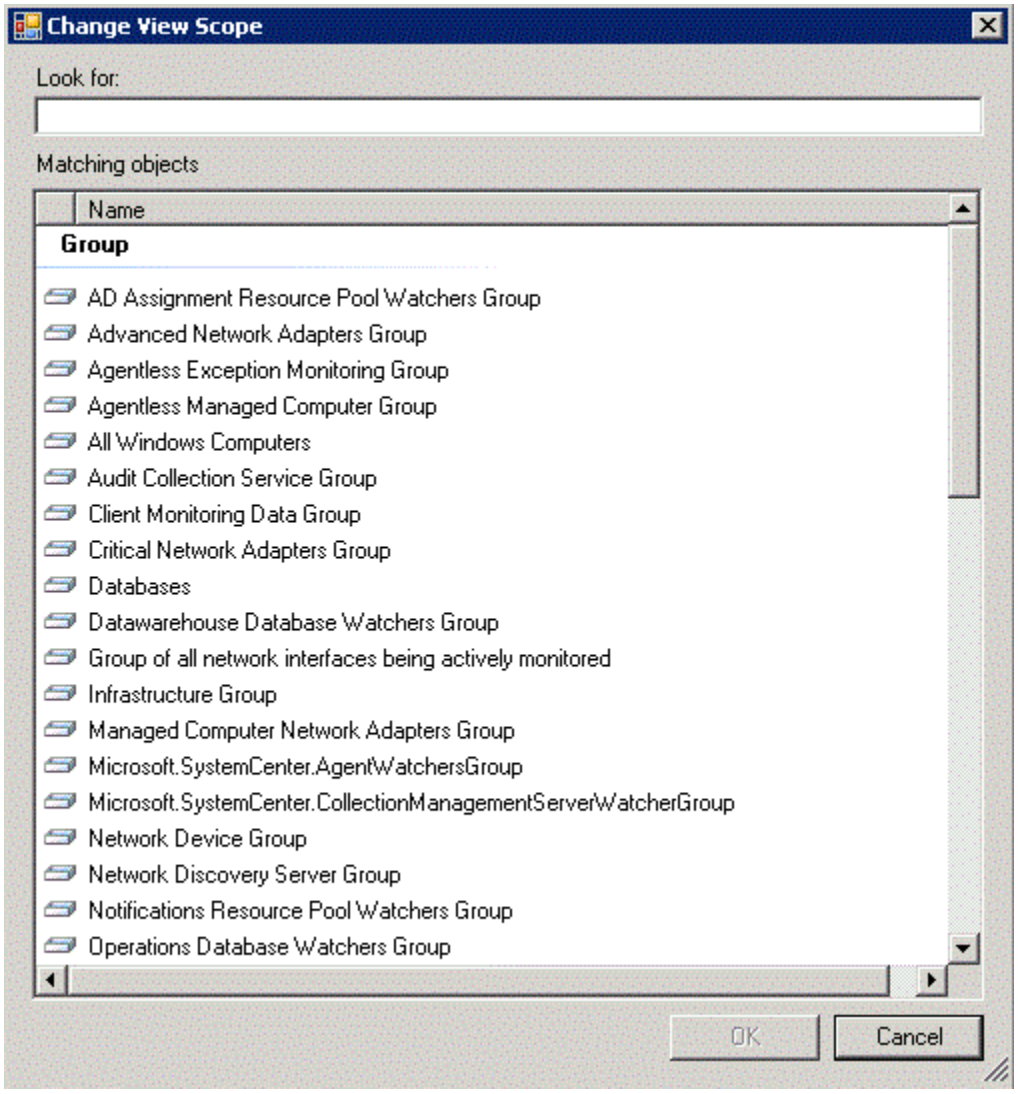
Filter	When to use	For more information, see
Scope	Use to limit the data in a view to only those objects that meet your criteria. This scope remains in place until you clear it.	• How to Change Scope • Define a Scope Using Operations Manager Groups
Search	Use to display a list of objects that meet your criteria. You can then act on those objects; however, when you navigate away from this list, the filter is removed, and any view will show all objects (not just those from your search criteria).	• How to Use Find and Search • Using Advanced Search • Examples of Using Advanced Search in Operations Manager
Find	Use to display a known single object.	How to Use Find and Search
Time	Use to limit the data displayed to only that data (such as alerts) that has been generated within a defined time frame.	How to Change the Time Criteria

How to Change Scope

Changing the scope of the monitoring view enables you to view only those objects that meet a certain criteria, such as management servers. For example, if you want to view only those computers in your environment that are running Windows XP, you can apply a scope that uses “Windows XP” as the criteria; no other computers are displayed.

To change the scope of the monitoring view

1. In the Operations console, click **Monitoring** to display the objects in your monitoring environment.
2. Click the **Scope** button on the Operations Manager toolbar. If this button is not available, check to make sure that you have an object, not a folder, selected in the Monitoring pane. The **Change View Scope** dialog box displays a list of existing groups and distributed applications.



3. If the list is too long, you can find a specific group or distributed application by entering a word or phrase in the **Look for** field. After you make a selection, click **OK**. Now only the objects that meet the scope criteria are shown in the Results pane.

How to Use Find and Search

Use the **Find** button when the list of objects in the Results pane is too long to quickly pick out a particular object. Use the **Search** button when you want to find all objects that meet a certain criteria.

To use Find to locate an object within a list

1. In the Operations console, click **Monitoring**.
2. Select a view that is available in the Monitoring workspace. This displays a list of objects in the Results pane.
3. Check to see whether a **Look for** box is at the top of the Results pane. If there is no **Look for** box, click the **Find** button on the toolbar. In **Look for**, type a word, such as the name of an object, that you want to find in the list, and then click **Find**.

   The object that you are looking for is displayed.
4. Click **Clear** to go back to the original list of objects.

To use Search to create a list of objects

1. In the Operations console, click **Monitoring**.
2. Click the **Search** button on the toolbar.
3. In the **Search** window, type the word or phrase that describes the set of objects you want to find. A list of objects that meet your criteria is displayed. The list is sorted by object type.

How to Change the Time Criteria

Changing the time criteria of the monitoring view enables you to view only those objects that meet a certain criteria, such as **Last 12 hours**. When you change the time criteria, you limit the display to only that time period. For example, if you want to view the last week of data, you can change the time criteria to **Last 1 week**.

You can filter your view to the following time periods:

- Last 1 hour
- Last 2 hours
- Last 4 hours
- Last 8 hours
- Last 12 hours
- Last 1 day
- Last 2 days
- Last 3 days
- Last 4 days
- Last 5 days

- Last 6 days
- Last 1 week
- Last 2 weeks
- Last 3 weeks
- Last 1 month
- All

To change the time criteria

1. In the Operations console, click **Monitoring** to display the objects in your monitoring environment.
2. Click the **Calendar** button on the toolbar. If this button is not available, check to make sure that you have an object, not a folder, selected in the navigation pane.
3. Select the time criteria you are interested in.

   Now only the objects that meet the time criteria are shown in the Results pane.

Using Advanced Search

In System Center 2012 – Operations Manager, advanced search is available in My Workspace, when you create a new search. You can also open advanced search in the Monitoring workspace on the **Tools** menu.

Use advanced search to search for a specific object type that meets specified criteria. Advanced search has two steps:

- Select the Specific Object Type and Criteria
- Set the Criteria Values

You can also save the searches you create. For more information, see Running and Saving Searches.

Select the Specific Object Type and Criteria

Each object type will display a unique set of criteria for your search. The following table lists the object types and the criteria available for each.

Object type	Criteria associated with the object type
Alerts	• Of a specific severity • Of a specific priority • Created by specific sources • With specific resolution state

Object type	Criteria associated with the object type
	• With a specific name • With specific text in the description • Created in specific time period • Assigned to a specific owner • Raised by an instance with a specific name • Last modified by a specific user • That was modified in specific time period • Had its resolution state changed in a specific time period • That was resolved in a specific time period • Resolved by specific user • With a specific ticket ID • Was added to the database in a specific time period • For a specific site • With specific text in the available custom fields
Events	• Generated by specific rules • With a specific event number • From a specific source • Generated in specific time period • Raised by an instance with a specific name • With specific severity level • From a specific user • Logged by a specific computer
Managed Objects	• With a specific name • In specific health state • Contained in a specific group
Monitors	• With a specific name • With specific text in the description • The monitor has been overridden for any context (excluding category overrides) • With specific category • Creates an alert when specific state is detected • The monitor generates alerts of specific priority

Object type	Criteria associated with the object type
	• Auto-resolves alerts • The monitor is a unit monitor • The monitor is an aggregate monitor • The monitor is a dependency monitor
Object Discoveries	• With a specific name • With specific text in the description • The object discovery has been overridden for any context (excluding category overrides) • With specific category • Is enabled • The object discovery confirms delivery • The rule is remotable [1] • Was added in a specified time period • Was modified in a specified time period
Rules	• With a specific name • With specific text in the description • The rule has been overridden for any context (excluding category overrides) • With specific category • The rule generates alerts of specific priority • Is enabled • The rule confirms delivery • The rule is remotable [1] • Was added in a specified time period • Was modified in a specified time period
Tasks	• With a specific name • With specific text in the description • Is enabled • Was added in a specified time period • Was modified in a specified time period
Views	• With a specific name • With specific text in the description • Was added in a specified time period • Was modified in a specified time period

[1] A remotable rule or discovery can run against a computer that does not have an agent installed.

Set the Criteria Values

If you have ever created a rule in Microsoft Outlook, setting criteria values for an advanced search will be familiar to you. When you select a criterion for an object, it is added to the **Criteria description** section. Most criteria contain a variable value. For example, in the criterion **With a specific name**, *specific* is a variable and will be underlined in the **Criteria description** section. (The criterion **Is enabled** is only true or false, so it contains no variables; you either select it or you do not select it.)

To assign a value to the variable, click the underlined portion of the criterion. A dialog box appears. In the example of **With a specific name**, you enter a text string for the specific name. For variables with limited values, such as alert priorities, the dialog box provides checkboxes that you can select.

Running and Saving Searches

After you set the values for the search criteria, you can run the search by clicking **Search** or you can save the search by clicking **Save parameters to My Favorites**. Saved searches are displayed in My Workspace and can be run at any time.

When you run a search or a saved search, a window opens with a view appropriate to the object type of your search. For example, a search on object type **Alerts** opens an Alert View window. A hyperlinked action, **Show parameters**, is displayed below the view title bar. You can click **Show parameters** to change the search parameters.

Note

When you run a saved search, change the parameters, click **Search**, and then close the results window, you will be asked if you want to save the changes to the search.

See Also

Finding Data and Objects in the Operations Manager Consoles

Examples of Using Advanced Search in Operations Manager

Examples of Using Advanced Search in Operations Manager

The following table lists examples of using advanced search to find objects in System Center 2012 – Operations Manager:

To find	Use this object, condition, and value
All alerts closed in the previous 2 hours.	• **Object:** Alerts • **Condition/Value:** With specific resolution state/Closed • **Condition/Value:** That was resolved in a specific time period/Last 2 Hours
All rules that have overrides	• **Object:** Rules • **Condition:** the rule has been overridden for any context (excluding category overrides)
All monitors that auto-resolve alerts	• **Object:** Monitors • **Condition:** auto-resolves alerts
All Unix computers in a warning or critical state	• **Object:** Managed Objects • **Condition/Value:** In specific health state/warning, critical • **Condition/Value:** Contained in a specific group/Unix Computer Group

See Also

Finding Data and Objects in the Operations Manager Consoles

Using Advanced Search

Using Views in Operations Manager

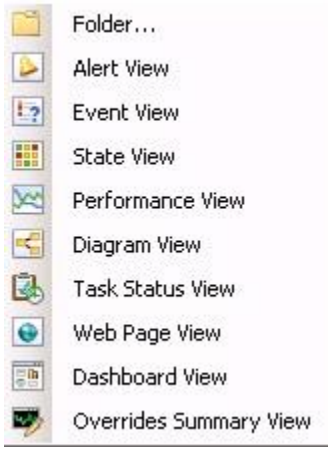
For a description of the differences between dashboard views and reports, see this System Center Operations Manager blog post.

Using Views in Operations Manager topics

- View Types in Operations Manager
- Standard Views in Operations Manager
- Creating Views in Operations Manager
- How to Personalize a View in Operations Manager
- Guidance for Scoping and Targeting Views

View Types in Operations Manager

Each view type in System Center 2012 – Operations Manager displays a different aspect of monitoring data. Each view type has a different icon as shown in the following image.

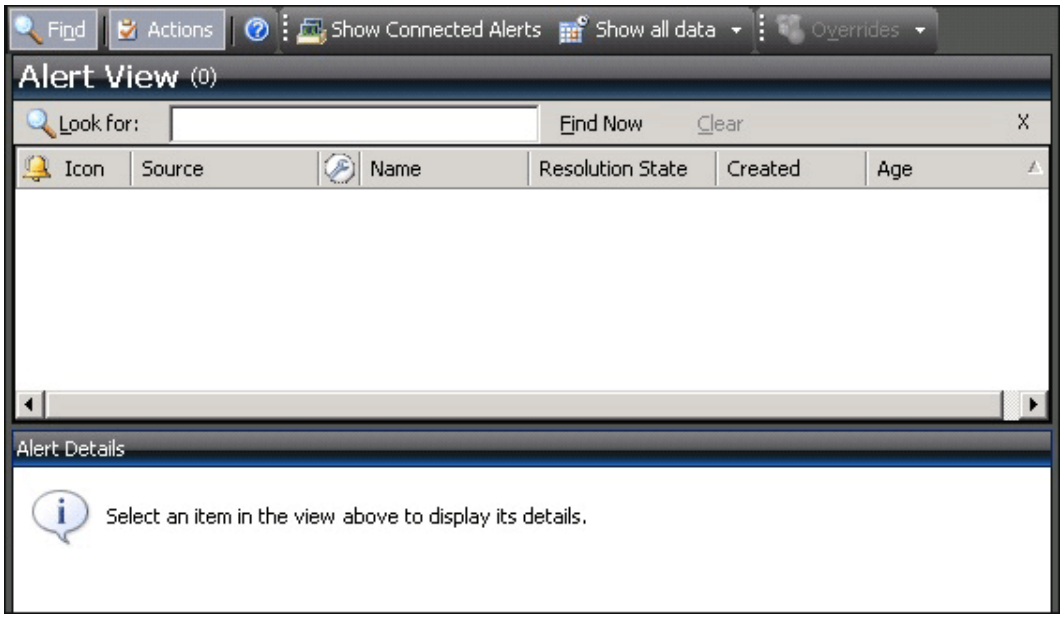


For more information on specific view types, see:

- Alert View Type
- Event View Type
- State View Type
- Performance View Type
- Diagram View Type
- Task Status View Type
- Web Page View Type
- Overrides Summary View Type
- Dashboard View Type

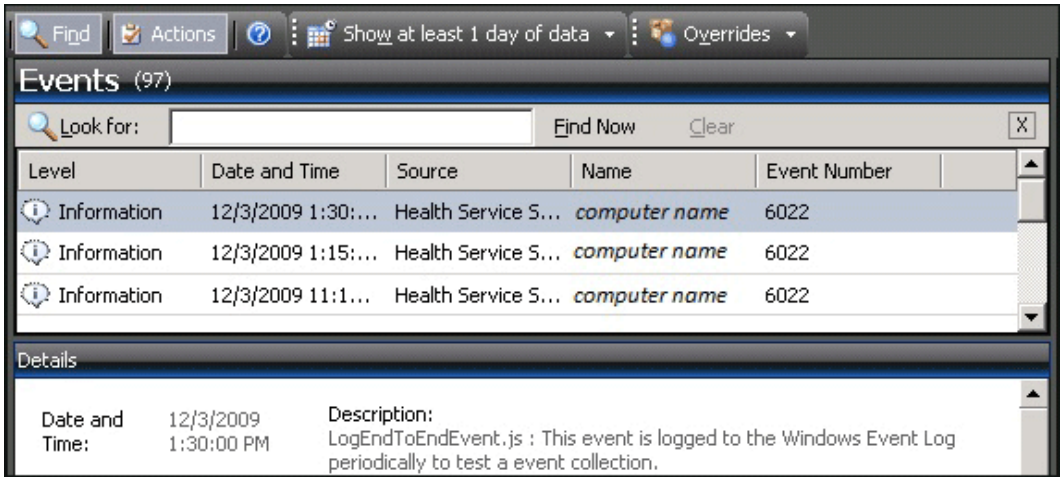
Alert View Type

The alert view displays alerts that meet your specific criteria, such as alert severity, resolution state, or alerts that are assigned to you. For information on creating an alert view, see How to Create an Alert View.



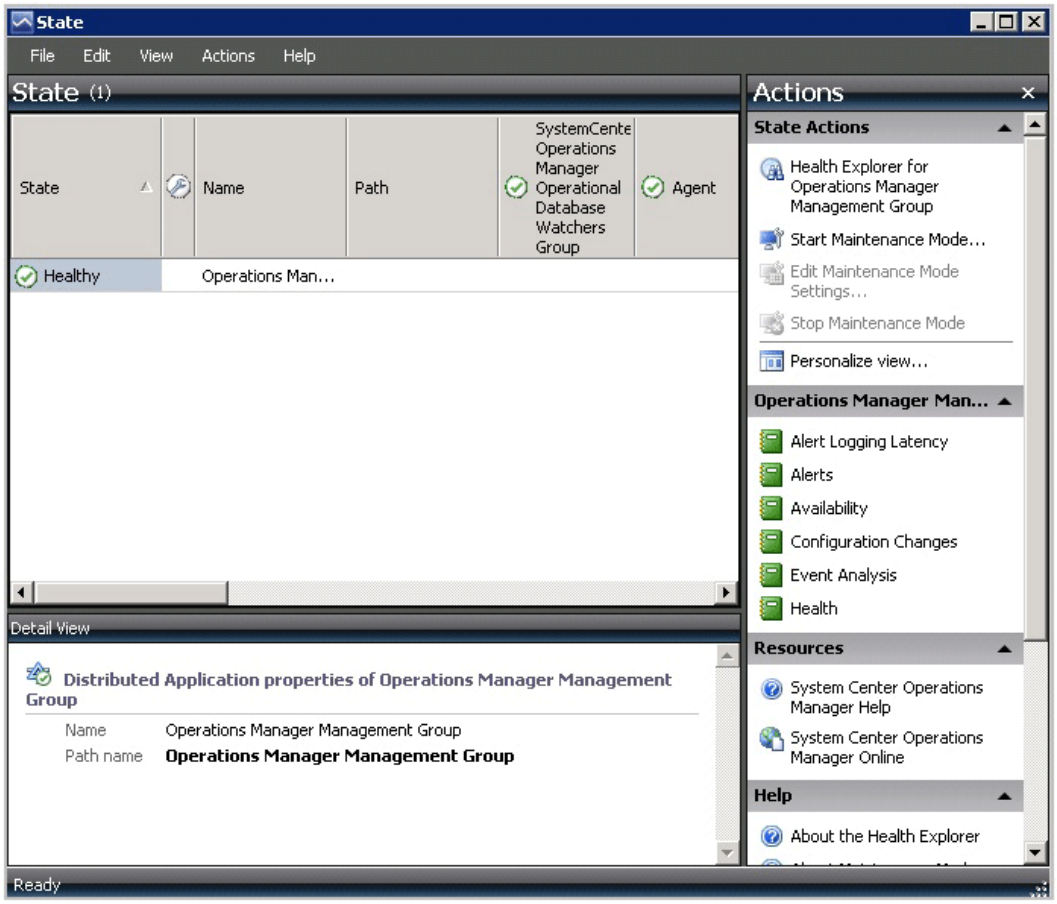
Event View Type

The event view queries the event logs and displays events that are based on criteria specified in the event view properties. For information on creating an event view, see How to Create an Event View.



State View Type

The state view displays relationships between components, computers, and computer groups. For information on creating a state view, see How to Create a State View.



Performance View Type

The performance view allows you to customize how you want to view performance data collected from performance objects and counters. This includes the ability to view historical and current operational data together. You must select **Show** in the Details pane to display data from a rule in the graph in the Results pane. For information on creating a performance view, see How to Create a Performance View.

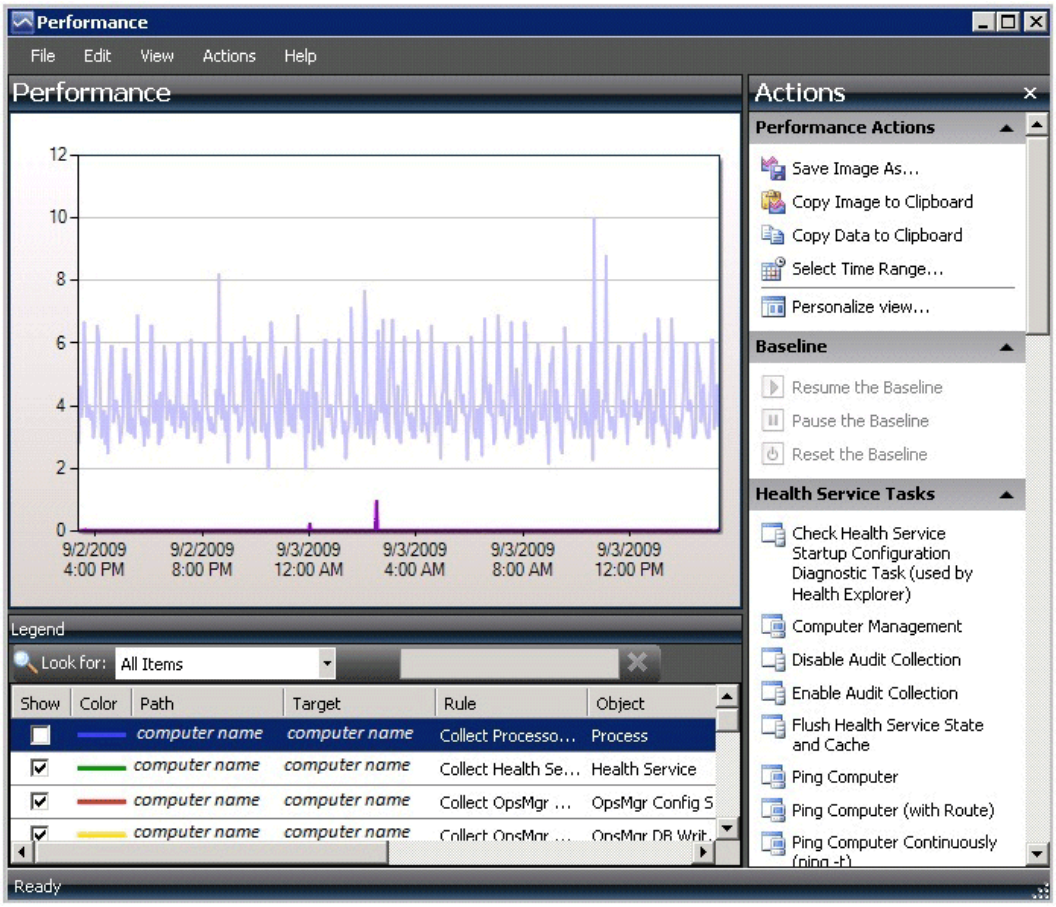
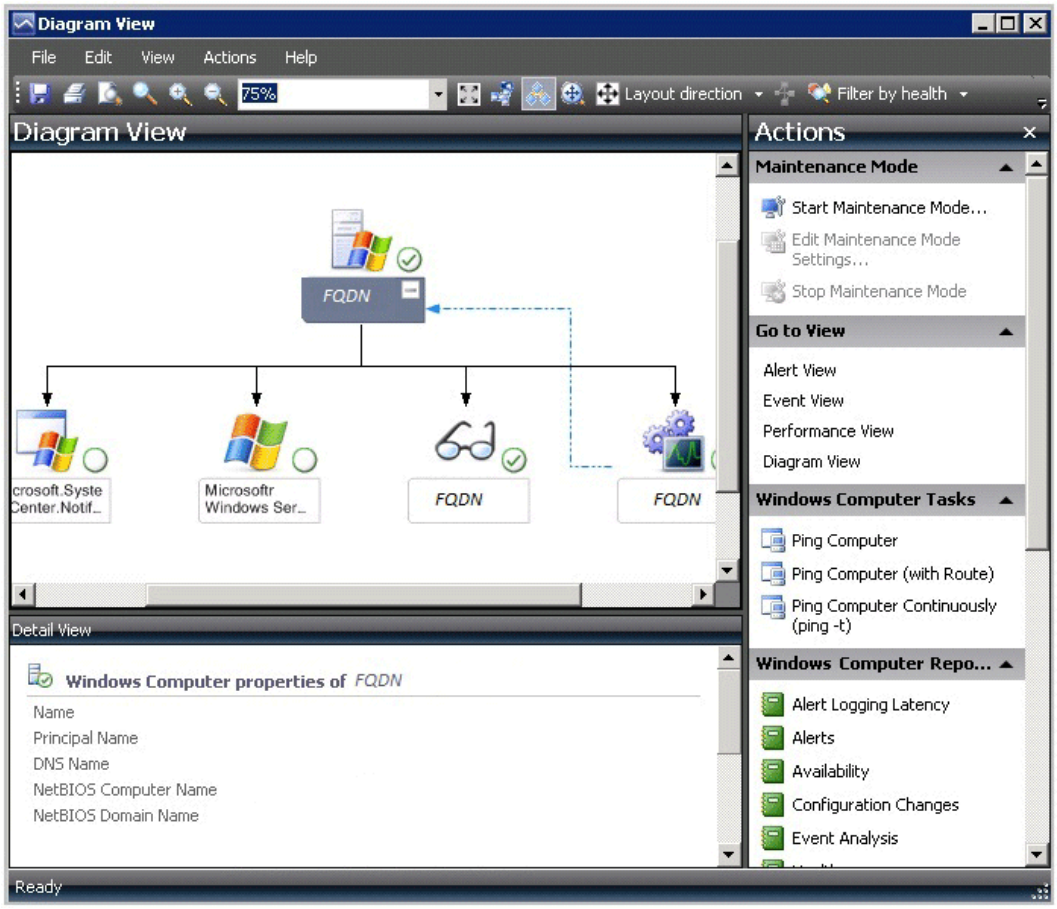


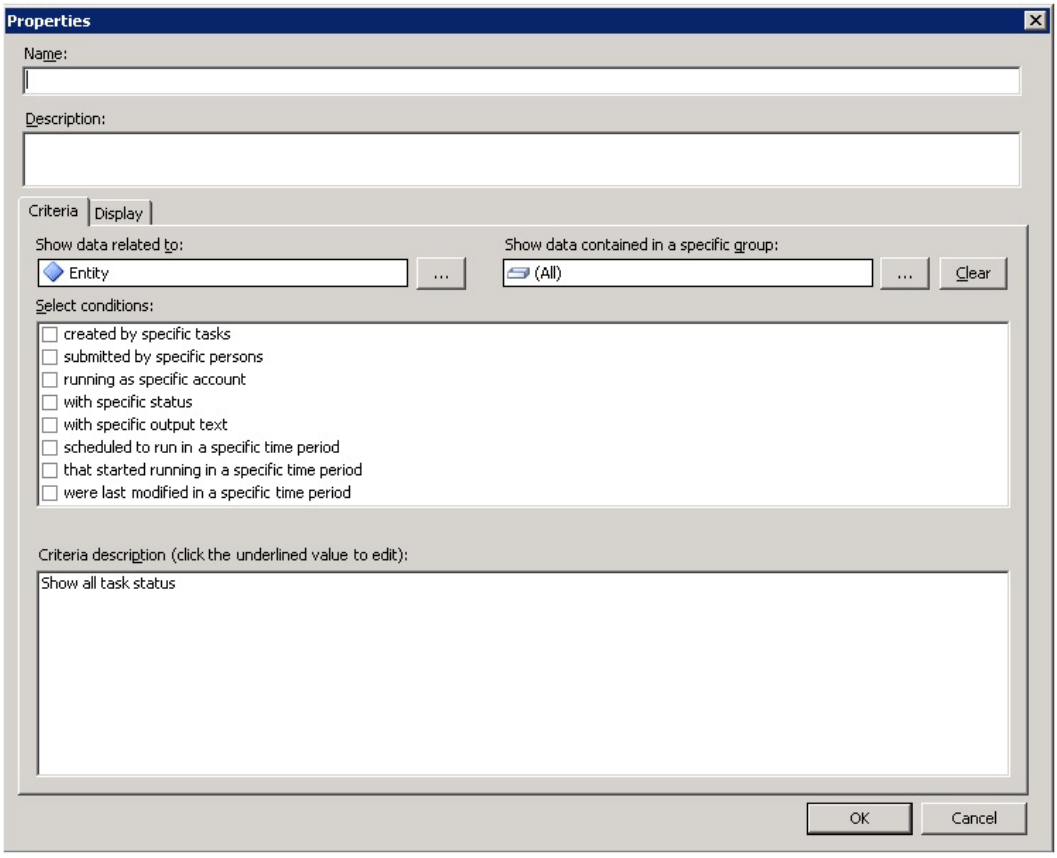
Diagram View Type

The Diagram view displays a graphical view of a set of managed objects and how they relate to one another. For information on creating a diagram view, see How to Create a Diagram View.



Task Status View Type

The task status view displays tasks that meet criteria specified in the properties, such as only those tasks that apply to certain object types. For information on creating a task status view, see How to Create a Task Status View.



Note

Users that are members of the Read-only Operator role cannot view or run any tasks. For this reason, no tasks appear in a task status view that is opened by a Read-only Operator.

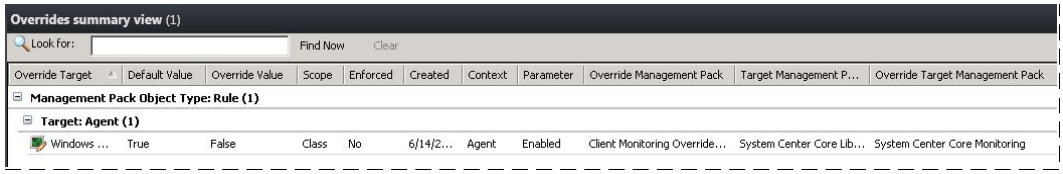
Web Page View Type

The Web page view displays a Web page in a separate window in the Operations console. For information on creating a Web page view, see How to Create a Web Page View.

Overrides Summary View Type

You can only create an overrides summary view in My Workspace.

You can view all rule and monitor overrides in the overrides summary view. The overrides summary view can be used for both sealed and unsealed management packs. You can customize this view by grouping items by multiple column headers. For information on creating an overrides summary view, see How to Create an Overrides Summary View.

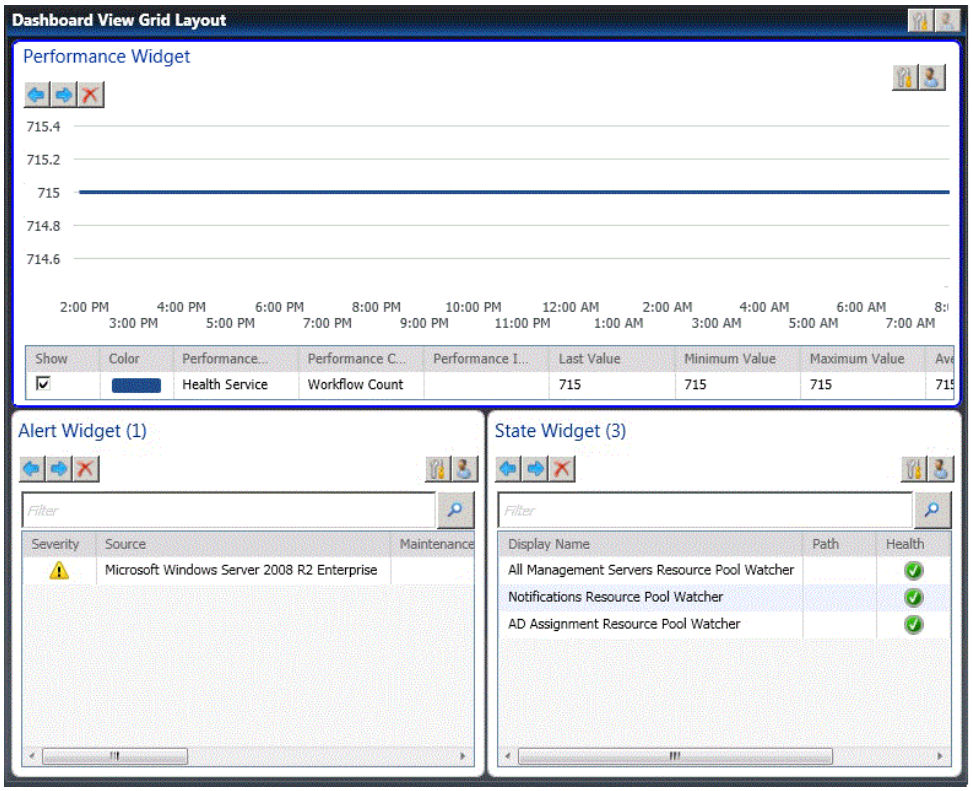


Dashboard View Type

The dashboard view allows you to present multiple types of data in a single view.

Security

When a dashboard view uses data from the data warehouse database, operators might be able to view data that they would not otherwise have access to in views that use data from the operational database.



For information on creating a dashboard view, see How to Create a Dashboard View.

See Also

Using Views in Operations Manager

Creating Views in Operations Manager

How to Personalize a View in Operations Manager

Guidance for Scoping and Targeting Views

Standard Views in Operations Manager

Several views are created by default when System Center 2012 – Operations Manager is installed. Management packs also contain views. When a management pack is imported, a folder that contains the views that are defined in the management pack is created in the Monitoring workspace.

The following table describes the views and folders of the views available when Operations Manager is installed. For views added by a management pack, see the management pack guide for information.

View or View Folder	Description
Active Alerts	This view shows all alerts that are active (not closed). In this view, select an alert to view its details, such as the rule or monitor that generated the alert and the managed object that has the problem. Double-click an alert to open the properties of the alert. Select an alert and click Health Explorer in the Tasks pane to open Health Explorer in the context of this alert. When appropriate, you can close the alert from this view by clicking **Close Alert** in the **Tasks** pane. For more information, see: • Viewing Alert Details • Using Health Explorer to Investigate Problems • Impact of Closing an Alert • How to Close an Alert Generated by a Monitor
Discovered Inventory	This view shows all objects that have been discovered and their states. Click **Change Target Type** in the **Tasks** pane to filter the discovered inventory list to a single type of object. The target type determines the type of information that will be displayed in the details pane for a selected object. For example, if you change the target type to Health Service, Detail View displays information about the health service for the selected object, such as port and action account identity. If you change the target type to Computer, Detail View displays computer information such as name and asset status. Select an object and click Health Explorer in the Tasks pane to open Health Explorer in the context of this object. When the state of an object in Discovered Inventory is **Not monitored**, that means…

View or View Folder	Description
	For more information, see Using Health Explorer to Investigate Problems.
Distributed Applications	This view shows all monitoring objects created by the Distributed Application Designer in your management group and their states. Select an object and click Health Explorer in the Tasks pane to open Health Explorer in the context of this object. For more information, see Using Health Explorer to Investigate Problems.
Task Status	This view shows the output from tasks that you have executed in the console. The **Task Status** view shows when a task is completed, finished, and the user who executed this specific task.
Unix/Linux Servers	This view shows the state of the following aspects of discovered UNIX and Linux computers: • Overall state of the computer • State of the agent on the computer, if an agent is installed • State of the management server role, if the computer is a management server • State of the operating system To see information that is collected for a computer, select the computer **Name** field for a specific computer. You can click **Properties** in the **Tasks** pane to display all of the information that is collected. To open other views for a computer, right-click the computer, select **Open**, and click a view to open. For example, to view a computer's performance, select the **Performance** option. Using the Performance view, you may filter to a set of counters to display by using the **Look for** option in the **Details** pane. Select a computer and click Health Explorer in the Tasks pane to open Health Explorer in the context of this computer. For more information, see Using Health

View or View Folder	Description
	Explorer to Investigate Problems.
Windows Computers	This view shows the state of the following aspects of discovered Windows computers: • Overall state of the computer • State of the agent on the computer, if an agent is installed • State of the management server role, if the computer is a management server • State of the Windows operating system To see information that is collected for a computer, select the computer **Name** field for a specific computer. You can click **Properties** in the **Tasks** pane to display all of the information that is collected. To open other views for a computer, right-click the computer, select **Open**, and click a view to open. For example, to view a computer's performance, select the **Performance** option. Using the Performance view, you may filter to a set of counters to display by using the **Look for** option in the **Details** pane. Select a computer and click Health Explorer in the Tasks pane to open Health Explorer in the context of this computer. For more information, see Using Health Explorer to Investigate Problems.
Agentless Exception Monitoring (folder)	Agentless Exception Monitoring (AEM) is used to aggregate, view, and report on error reports that are sent by the Windows Error Reporting service. The Agentless Exception Monitoring folder contains four state views and one event view, specific to data gathered by AEM. • **Application View** • **Crash Listener View** • **Error Events** • **Error Group View** • **System Error Group View**
Data Warehouse (folder)	The data warehouse is the database that stores

View or View Folder	Description
	operations data which is used by Reporting Server to build reports.The Data Warehouse folder contains views to help you monitor the state and performance of the data warehouse. • **Active Alerts** • **All Event View** • **Collection Performance** • **Collection Servers** • **Synchronizaton Performance**
Microsoft Audit Collection Services (folder)	Audit Collection Services (ACS) collects records generated by an audit policy. The ACS collector receives and processes events from ACS forwarders and then sends this data to the ACS database. The service that runs on ACS forwarders is included in the Operations Manager agent. The Microsoft Audit Collection Services folder contains views specific to ACS operations. • The ACS **Collector** folder contains an event view, a state vew, and multiple performance views. • The ACS **Fowarder** folder contains an event view and a state vew.
Network Monitoring (folder)	The Network Monitoring folder contains an alert view that is scoped to discovered network devices, state views for each type of network device, and a Network Summary Dashboard view. For more information, see Viewing Network Devices and Data in Operations Manager. The Network Monitoring folder also contains views specific to network discovery and performance.
Operations Manager (folder)	One of the views in the Operations Manager folder is a diagram of the management group. You can click an item in the diagram to view details about the object. The Operations Manager folder contains numerous views, and organized as follows:

View or View Folder	Description
	• **Activated APM Agent Details** • **Agent Details** • **Management Configuration Service** • **Management Data Access** • **Management Group Details** • **Management Packs and Workflows** • **Management Server** • **Notification**
Synthetic Transaction (folder)	The Synthetic Transaction folder contains state views for OLE DB data sources and TCP port checks.
Web Application Transaction Monitoring (folder)	The Web Application Transaction Monitoring folder contains a state view of monitored Web applications.
Windows Service and Process Monitoring (folder)	The Windows Service and Process Monitoring folder contains state views for Windows services and processes.

See Also

Using Views in Operations Manager

Creating Views in Operations Manager

How to Personalize a View in Operations Manager

Guidance for Scoping and Targeting Views

Creating Views in Operations Manager

System Center 2012 – Operations Manager views display information that meets specific criteria. When you select a view, a query is sent to the Operations Manager database and the results of the query are displayed in the results pane. You can use the standard views created when Operations Manager is installed, views provided by management packs, or create your own custom views.

You must have the rights of the Author role to create a view in the Monitoring workspace. If you are an operator, you can create a view in My Workspace. The procedures below create views in My Workspace, however the same procedures apply to creating a view in the Monitoring workspace.

For information on selecting the objects, classes, or groups for a view, see Guidance for Scoping and Targeting Views.

This topic contains the following procedures:

- How to Create an Alert View
- How to Create an Event View
- How to Create a State View
- How to Create a Performance View
- How to Create a Diagram View
- How to Create a Task Status View
- How to Create a Web Page View
- How to Create a Dashboard View
- How to Create an Overrides Summary View

How to Create an Alert View

You can create a custom alert view that shows only those alerts that you want to see. For example, if you need to track the status of UNIX-based or Linux-based computers, you can create a view that shows only critical alerts generated by those computers.

To create an alert view

1. In the Operations console, click **My Workspace**.
2. Right-click the folder where you want to store the view and point to **New**, and click **Alert View**.
3. In the **Properties** dialog box of the alert view, type a name and a description for the view. (The description is optional.)
4. Set the criteria to identify the alerts to display:
   a. Narrow the pool of possible alerts by identifying a class or group for alerts. For example, to create an alert view for UNIX-based or Linux-based computers, select **Unix Computer** in the **Show data related to** list. For more information, see Guidance for Scoping and Targeting Views.
   b. Select the conditions that define the content of the view. There are a number of different conditions that you can choose, from severity or priority to alerts that include text in specific fields. For example, for the UNIX-based or Linux-based computers alert view, select **of a specific severity** in the **Select conditions** list.
   c. Refine the criteria description by clicking the underlined text in the **Criteria description** box.

      For the UNIX-based or Linux-based computers alert view, click **specific**. In the **Alert Type** window, select **Critical**, and then click **OK**.

      Note
      You can add multiple criteria to refine the view to fit your needs.

5. Customize the appearance of the alert view on the **Display** tab. You can specify the columns to display, the sort order for the columns, and the manner in which items are grouped.
6. Click **OK** to create the view.

How to Create an Event View

An event view can only display events that are collected by a management pack. Operations Manager does not collect all events.

To create an event view

1. In the Operations console, click **My Workspace**.
2. Right-click the folder where you want to store the view, point to **New**, and then click **Event View**.
3. In the **Properties** dialog box of the event view, type a name and a description for the view. (The description is optional.)
4. Set the criteria to identify the events to display:
   a. Narrow the pool of possible events by identifying a class or group for events. For example, to create an event view for UNIX-based computers, select **Unix Computer** in the **Show data related to** list. For more information, see Guidance for Scoping and Targeting Views.
   b. Select the conditions that define the content of the view. There are a number of different conditions that you can choose. For example, for the UNIX-based computers event view, select **with specific severity level** in the **Select conditions** list.

      Note
      When you select **generated by specific rules**, only event collection rules can be selected. If you do not see the rule that you want to select when you click **specific**, ensure that the category of the rule you want is **Event Collection**.

   c. Refine the criteria description by clicking the underlined text in the **Criteria description** box.

      For the UNIX-based computers event view, click **specific**. In the **Event Type** window, select **Audit Failure**, and then click **OK**.

   Note
   You can add multiple criteria to refine the view to fit your needs.
5. Customize the appearance of the event view on the **Display** tab. You can specify the columns to display, the sort order for the columns, and the manner in which items are grouped.
6. Click **OK** to create the view.

How to Create a State View

The state view in Operations Manager is like most other view types in that you use the **Criteria** tab in the **Properties** dialog box of the view to define which objects you want shown in your view. You then use the **Display** tab to customize how the data looks in your view. Each section of the **Criteria** tab adds an additional filter to your view.

Note

When a state view is displayed, you might find that multiple objects are listed by the same name. For example, a Windows-based computer object and management server object might have the same computer name. The Windows-based computer object and the management server object will be listed on their own row in the state view and thus, the same computer name will be listed twice. This is expected behavior.

To create a state view

1. Right-click the folder where you want to store the view, point to **New**, and then click **State View**.
2. In the **Properties** dialog box of the event view, type a name and a description for the view. (The description is optional.)
3. On the **Criteria** tab, click the ellipses (**…**) next to the **Show data related to** box. The **Select a Target Type** dialog box displays a list of the object types available in your management group. Click to select the object type of the objects that you want to view, and then click **OK**. For more information, see Guidance for Scoping and Targeting Views.

   The object type you select is listed in the **Show data related to** box. If you want to narrow the focus of the view, you can also click the ellipses (**…**) next to **Show data contained in a specific group**. Click a group to filter the objects shown in your view, and then click **OK**.

   Note

   If you do not see the object type that you want, click **View all targets** and then type a word or phrase in **Find** to filter the displayed list.
4. Use the checkboxes provided to select individual criteria to apply additional filters to the objects that you want to display in your view. You might need to further define the criteria in the **Criteria description** box.
5. Click the **Display** tab. By default, all columns in your state view display. Click to deselect one or more columns that you do not want to display. Choose how you want to sort the objects in your view in **Sort columns by**.
6. Click **OK** to create the view.

How to Create a Performance View

Performance views use data stored in the operational database. A performance view can only display performance counters that are collected by a management pack. Operations Manager does not collect all performance counters.

To create a performance view

1. In the Operations console, click **My Workspace**.
2. Right-click the folder where you want to store the view, point to **New**, and then click **Performance View**.
3. In the **Properties** dialog box of the performance view, type a name and a description for the view. (The description is optional.)
4. Set the criteria to identify the performance data to display:
   a. Identify a class or group for performance data. For example, to create a performance view for UNIX-based computers, select **Unix Computer** in the **Show data related to** list. For more information, see Guidance for Scoping and Targeting Views.
   b. Select the conditions that define the content of the view. There are a number of different conditions that you can choose. For the UNIX-based computers performance view, select **collected by specific rules** in the **Select conditions** list.
   c. Refine the criteria description by clicking the underlined text in the **Criteria description** box.

      For the **collected by specific rules** condition, click **specific**. In the **Select rules** window, select a performance collection rule, and then click **OK**.

   Note
   You can add multiple criteria to refine the view to fit your needs.
5. Customize the appearance of the alert view on the **Display** tab. You can specify the chart type to display, the period of time that the chart should cover, and the display options for the X axis and Y axis.
6. Click **OK** to create the view.

How to Create a Diagram View

In Operations Manager, a diagram view uses a template to control the layout of the information in the diagram. You can choose from an existing template or create your own template. If you choose to create your own template, you configure the layout of the view while you are creating the view.

To create a diagram view

1. In the Operations console, click **My Workspace**.
2. Right-click the folder where you want to store the view, point to **New**, and click **Diagram View**.

3. In the **Properties** dialog box of the diagram view, type a name and a description for the view. (The description is optional.)
4. Click **Browse**. In the **Select Object** dialog box, click the group for the type of objects that you want to include in your diagram view, and then click **OK**. For more information, see Guidance for Scoping and Targeting Views.
5. Click **Create your own template** to design a layout for your diagram view.
6. If you want to accept the default settings for the diagram view, click **Create**. If you want to change the default settings, continue with this procedure.
7. On the **Diagram Properties** tab, type a number in **Levels to show** to display the number of related classes and subclasses that you want in your view. This number includes the top-level class. In **Layout Direction**, click the drop-down arrow to view a list of display options for the objects in your view. **North South** displays the objects in a vertical arrangement, and **East West** displays the objects side by side.
8. Click the **Object Properties** tab. Click **Boxes** if you want to delineate your related object types and child object types by containing them in a box. You can also adjust the **Nodes Per Row** setting to define how many of your related object types are listed before beginning another row.
9. On the **Line Properties** tab, choose the format for the lines of the boxes in your diagram by using the **Containment Line** settings. Choose the format for objects that are not grouped by boxes using the **Non Containment Line** settings. Click **Create**.

How to Create a Task Status View

The task status view in Operations Manager is like most other view types in that you use the **Criteria** tab in the **Properties** dialog box of the view to define which objects you want shown in your view. You then use the **Display** tab to customize how the data looks in your view. Each section of the **Criteria** tab adds an additional filter to your view.

To create a task status view

1. In the Operations console, click **My Workspace**.
2. Right-click the folder where you want to store the view, point to **New**, and then click **Task Status View**.
3. In the **Properties** dialog box of the task status view, type a name and a description for the view. (The description is optional.)
4. On the **Criteria** tab, click the ellipses (**…**) next to the **Show data related to** box. The **Select a Target Type** dialog box displays a list of the object types available in your management group. Click to select the object type that most specifically describes the objects that you want to view, and then click **OK**. For more information, see Guidance for Scoping and Targeting Views.

   The object type you select is listed in the **Show data related to** box. If you want to narrow the focus of the view, you can also click the ellipses (**…**) next to **Show data contained in a specific group**. Click a group to filter the objects shown in your view, and

then click **OK**.

Note
If you do not see the object type that you want, click **View all targets** and then type a word or phrase in **Find** to filter the displayed list.

5. Use the check boxes provided to select individual criteria to apply additional filters to the objects that you want to display in your view. You might need to further define the criteria in the **Criteria description** box.
6. Click the **Display** tab. By default, all columns in your state view display. Click to deselect one or more columns that you do not want to display. Choose how you want to sort the objects in your view in **Sort columns by**.
7. Click **OK** to create the view.

How to Create a Web Page View

You can create a view that displays a specific web page. For example, you can create a web page view that points to http://social.technet.microsoft.com/Forums/en-US/category/systemcenteroperationsmanager, which makes the community forums for Operations Manager available to you within the Operations console. You can interact with the web pages displayed in a web page view, just as you can in an internet browser.

To create a web page view

1. In the Operations console, click **My Workspace**.
2. Right-click the folder where you want to store the view, point to **New**, and then click **Web Page View**.
3. Enter a name and description for the view. (The description is optional.)
4. In the **Target website** field, enter the URI for the web page to be displayed in the view. You can specify an Internet or intranet address.

   Note
   The web view will only display the specified web page on computers that have access to that web page. For example, if you create a web page view that links to the System Center page on Microsoft.com, an Operations console on a computer that does not have Internet access will not display the correct web page in that web page view.
5. Click **OK**.

How to Create a Dashboard View

You can create dashboard views in the Operations Manager web console as well as the Operations console.

Security

When a dashboard view uses data from the data warehouse database, operators might be able to view data that they would not otherwise have access to in views that use data from the operational database.

You can use dashboard views to present multiple types of data in a single view. You select either a flow layout, which consists of multiple columns, or a grid layout, which consists of multiple cells. In the grid layout, you also specify the layout of the cells.

If you create a dashboard view that uses a flow layout, you can change the number of columns afterward. If you create a dashboard view that uses a grid layout, you can change the layout afterward but you cannot change the number of cells.

For both layouts, after you create the dashboard view, you add widgets which will display specific types of data.

Note

A column or cell in a dashboard view can contain a widget or another dashboard view.

Operations Manager contains the following widgets:

- State
- Performance
- Alert

Additional widgets may be provided by management packs.

Widgets in a dashboard view can display data for a particular target class or group of objects. To support the dashboard view that you are going to create, you should first create a group containing a set of computers or objects to include in the displayed data.

Note

When you create a dashboard view that includes a widget that displays data for a target class that contains instances (a non-singleton class), that dashboard view cannot be imported into other management groups.

You can also create a service level dashboard view to track data for service level objectives that you create. For more information, see Creating a Service Level Dashboard.

To create a dashboard view

1. In the Operations console, click **My Workspace**.
2. Right-click the folder where you want to store the view, point to **New**, and click **Dashboard View**.
3. In the New Instance Wizard, on the **Template** page, click either **Flow Layout** or **Grid Layout**, and then click **Next**.
4. On the **General Properties** page, enter a name for the dashboard view. The description is optional. Click **Next**.
5. For a grid layout, on the **Select Layout** page, choose the number of cells to display and the layout template for the cells. The layout templates change based on the number of cells selected. Click **Next**.

For a flow layout, on the **Specify the flow layout column count** page, select the number of columns to display. Click **Next**.

6. Review the settings on the **Summary** page, and then click **Create**.
7. Click **Close**.

The dashboard view that you created is displayed. Next, you configure the columns or cells in the dashboard view.

To add widgets to a dashboard view

1. In a cell or column of a dashboard view, click **Click to add widget**.
2. In the New Instance Wizard, on the **Template** page, select from the available templates. The wizard pages for the Flow Layout and Grid Layout templates are the same as in the new dashboard view procedure. The following steps provide instructions for the other widget templates.

   Alert Widget:

   a. On the **General Properties** page, enter a name for the widget. The description is optional. Click **Next**.
   b. On the **Specify the Scope** page, select a group or object, and then click **Next**. For more information, see Guidance for Scoping and Targeting Views.
   c. On the **Specify the Criteria** page, use the severity, priority, and resolution state checkboxes to select the criteria for data to be displayed, and then click **Next**.
   d. On the **Display** page, select the columns you want displayed. You can also configure the sort order and how to group the data. Click **Next**.
   e. Review the settings on the **Summary** page, and then click **Create**.
   f. Click **Close**.

   Performance Widget:

   a. On the **General Properties** page, enter a name for the widget. The description is optional. Click **Next**.
   b. On the **Specify the Scope and Counters** page, select a group or object. For more information, see Guidance for Scoping and Targeting Views.
   c. On the **Specify the Scope and Counters** page, click **Add**.
   d. In the **Select performance counters** dialog box, use the **Object**, **Counter**, and **Instance** dropdown menus to filter the performance counters listed in **Available Items**. Select performance counters from the **Available Items** list, click **Add**, and then click **OK**.

      Note
      The performance counters available are scoped to the group or object you selected in **Select a group or object**.

   e. Click **Next**.
   f. On the **Time Range** page, select the time range for the data, and click **Next**.
   g. On the **Specify the Chart Preferences** page, select the items you want displayed in

the performance chart. You can configure order of the items by using the up and down arrows. For the vertical axis, you can select Automatic or configure the minimum and maximum values manually. Cilck **Next**.

h. Review the settings on the **Summary** page, and then click **Create**.

i. Click **Close**.

State Widget:

a. On the **General Properties** page, enter a name for the widget. The description is optional. Click **Next**.

b. On the **Specify the Scope** page, click **Add**.

c. In the **Add Groups or Objects** window, click the groups or objects in **Available items** and click **Add**, and then click **OK**.

d. In **Select a class to scope the members of the specific groups**, you can change the selected class. (Object is selected by default.) Click **Next**.

e. On the **Specify the Criteria** page, use the health state checkboxes to select the criteria for data to be displayed, and then click **Next**.

Note

You can also select to display only objects in maintenance mode.

f. On the **Display** page, select the columns you want displayed. You can also configure the sort order and how to group the data. Click **Next**.

g. Review the settings on the **Summary** page, and then click **Create**.

How to Create an Overrides Summary View

You can only create an overrides summary view in My Workspace.

You can view all rule and monitor overrides in an overrides summary view. The overrides summary view can be used for both sealed and unsealed management packs.

To create an overrides summary view

1. In the Operations console, click **My Workspace**.
2. Right-click the folder where you want to store the view, point to **New**, and then click **Overrides Summary Vieew**.
3. In the **Properties** dialog box of the overrides summary view, type a name and description for the view. (The description is optional.)
4. Set the criteria to identify the performance data to display:
   a. Identify a class or group for performance data. For example, to create an overrides summary view for all System Center agents, select **Agent** in the **Show data related to** list. For more information, see Guidance for Scoping and Targeting Views.
   b. Select the conditions that define the content of the view.
   c. Refine the criteria description by clicking the underlined text in the **Criteria description** box.

Note

You can add multiple criteria to refine the view to fit your needs.

5. Customize the appearance of the alert view on the **Display** tab.
6. Click **OK** to create the view.

See Also

Using Views in Operations Manager

Standard Views in Operations Manager

How to Personalize a View in Operations Manager

Guidance for Scoping and Targeting Views

How to Personalize a View in Operations Manager

In System Center 2012 – Operations Manager, views are contained in management packs. If a view is contained in a sealed management pack, you can open the properties of the view but you cannot save any changes to it. However, you can change the display options of the view and then save it as a personalized view.

Note

Personalized views are only visible to the user who personalized the view.

To personalize a view

1. In the Operations console, click **Monitoring**.
2. In the **Monitoring** workspace, right-click the view that you want to personalize and then click **Personalize view**. The **Personalize view** dialog box displays with the default settings of the view.
3. In **Columns to display**, click to place a check next to the property that you want to display in your view. You can also click to remove any checkmarks set by the original view. In the **Sort columns by** box, click the drop-down arrow to choose a property by which you want to sort the monitored objects in your view, and then click **OK**.

   Note

   In a state view, the option to sort by groups is not available. This option is available in other view types, such as the alert view and event view.

To restore view defaults

1. In the Operations console, click **Monitoring**.

2. In the **Monitoring** workspace, right-click the personalized view
3. Click **Reset to Default**, and then click **OK**.

See Also

Using Views in Operations Manager

Standard Views in Operations Manager

Creating Views in Operations Manager

Guidance for Scoping and Targeting Views

Guidance for Scoping and Targeting Views

In System Center 2012 – Operations Manager, you can use groups to limit a view in the Operations console, making it easier to find the specific information you need. You can change the scope for any existing view (other than dashboard views) to a specific group; however, this change only applies to the user who makes it and does not persist when the console is restarted.

For persistent management, you can create views that are scoped to a specific group. You can also scope the following widgets in a dashboard view:

- Alert
- Instance Details
- Performance
- State

For example, after you create a group of objects, you can create a dashboard view in which each widget is targeted to the group, providing a single view for important information for the members of the group.

After you create views for the group, you can create a user role that is scoped to the group and limited to the views for that group, and then assign users to that user role. This enables the individuals with that user role to monitor the objects they are concerned with, while limiting them to information that only pertains to those objects.

See Also

Using Views in Operations Manager

Standard Views in Operations Manager

Creating Views in Operations Manager

How to Personalize a View in Operations Manager

Using SharePoint to View Operations Manager Data

System Center 2012 – Operations Manager includes a SharePoint Web Part that displays selected dashboards from the web console. A configured Web Part allows you to see at a glance the availability and performance metrics for applications in your environment.

The Operations Manager Web Part is particularly useful for providing current status views to individuals in your organization who are not Operations Manager users. Use the following procedures, as applicable, to set up dashboards on a SharePoint page.

How to Deploy the Operations Manager Web Part

Before you can add the Operations Manager Web Part to a SharePoint page, the Web Part must be deployed to the SharePoint site.

How to Configure the Web Part to Connect to a Web Console

After you deploy the Operations Manager Web Part, you configure it to connect to a specific web console.

How to Add the Operations Manager Web Part to a SharePoint Page

After the Operations Manager Web Part is deployed to a SharePoint site, you can add the Web Part to a SharePoint page.

How to Configure the Web Part to Use Shared Credentials

To configure the Operations Manager Web Part so that those who are not Operations Manager users can view it, you must configure the Web Part to use shared credentials.

How to Add Additional Environments to the Web Part

When you deploy the Operations Manager Web Part, you configure it to connect to a Web Console Server or *environment*. You can add additional environments to a Web Part, which will enable you to display dashboards from multiple management groups.

How to Uninstall the Operations Manager Web Part

You can uninstall the Operations Manager Web Part from all sites and web applications in the farm or from a specific site or web application.

How to Deploy the Operations Manager Web Part

The following are the prerequisites for deploying the Operations Manager web part:

- The Operations Manager web console must be installed on a management server.
- The SharePoint farm must be running SharePoint Server 2010 Standard, SharePoint Server 2010 Enterprise, or SharePoint Foundation 2010.

  Note
  If the SharePoint farm is running SharePoint Foundation 2010, you can only deploy the web part in the same domain as the web console and you cannot use shared credentials.
- You must have SharePoint administrator permissions for the SharePoint farm; specifically, you must have permissions to perform the following tasks:
  - Run the SharePoint PowerShell client
  - Start and stop the SPAdminV4 and SPTimerV4 services
  - Run the Add-SPSolution and Install-SPSolution cmdlets for the farm, and run the Enable-SPFeature cmdlet for all sites on the farm

The web part is a solution file named Microsoft.EnterpriseManagement.SharePointIntegration.wsp. To deploy the web part, you run a script named install-OperationsManager-DashboardViewer.ps1. This script is located in the Operations Manager installation folder under Setup\amd64\SharePoint.

Note
You can get more information on the scripts included with Operations Manager by using the command shell and the get-help cmdlet. For example: **get-help install-OperationsManager-DashboardViewer.ps1**.

Using the install-OperationsManager-DashboardViewer.ps1 script, you can deploy the web part to all sites and web applications in the farm or to a specific site or web application.

To deploy the Operations Manager web part

1. Copy the install-OperationsManager-DashboardViewer.ps1 file and the Microsoft.Enterprisemanagement.Sharepointintegration.wsp file from the Operations Manager installation folder under Setup\amd64\SharePoint to a location that the SharePoint 2010 Management Shell can access.
2. Open the SharePoint 2010 Management Shell and navigate to the directory where you saved the install-OperationsManager-DashboardViewer.ps1 file.
3. In the SharePoint 2010 Management Shell, type the following command, and then press **Enter**.

   .\install-OperationsManager-DashboardViewer.ps1 –solutionPath *<directory for Microsoft.EnterpriseManagement.SharePointIntegration.wsp>* **-url** *<optional, for installing to a specific portal address or website>*

   Here is an example that deploys the web part to a specific portal address. In this example

you are copying the files to “C:\Program Files\System Center Operations Manager 2012\”.

.\install-OperationsManager-DashboardViewer.ps1 “C:\Program Files\System Center Operations Manager 2012\” http://localhost:4096

If an error occurs when you run the script, you must disable the RemoteSigned default code-signing execution policy for the SharePoint 2010 Management Shell. To allow the install-OperationsManager-DashboardViewer.ps1 script to run, type the following command, and then press **enter**:

Set-ExecutionPolicy Unrestricted

You will see some confirmation messages, select **Y** to confirm, and then run the script.

4. Verify that the web part is deployed and activated by performing the following steps:
   a. Open the site http://localhost.
   b. In the **Site Actions** dropdown menu, click **Site Settings**.
   c. In the **Site Collection Administration** section, click **Site collection features**.
   d. Locate **Operations Manager Dashboard Web Part**.
      - If the button to the right says **Activate**, then the feature was not automatically activated during deployment. To activate the web part, click the **Activate** button.
      - If the button to the right says **Deactivate**, no steps are required. The Operations Manager Dashboard web part can now be inserted into site pages.
5. If you disabled the RemoteSigned default code-signing execution policy to run the install-OperationsManager-DashboardViewer.ps1 script, you should re-enable it after the script runs. Type the following command and then press **enter**:

   Set-ExecutionPolicy Restricted

   You will see some confirmation messages, select **Y** to confirm.

How to Configure the Web Part to Connect to a Web Console

After the web part is deployed and activated, you must configure the web part to connect to a web console or *environment*. You can add more environments at any time. Use the following procedure to configure the environment for a web part.

To configure the environment for a web part by using the user interface

1. On the SharePoint central administration site, in the **Site Actions** dropdown menu, click **View All Site Content**.
2. In **Lists**, click **Operations Manager Web Console Environments**.
3. Click **Add new item**.
4. In the **Name** field, enter a unique name.
5. In the **HostURI** field, enter the URI to a server hosting the Operations Manager web

console. For example: **http://ServerName/OperationsManager/**

6. Click **Save**.

How to Add the Operations Manager Web Part to a SharePoint Page

After you deploy the Operations Manager web part to a SharePoint site, you can add the web part to pages. When you add the web part, you configure it to display a specific dashboard view. For the configuration, you will need the URI for the dashboard view that you want displayed.

To obtain the URI, open the web console and navigate to the desired dashboard view. The address bar will display an address such as the following:

http://localhost/OperationsManager/#/dashboard%7Btype=Microsoft.SystemCenter.Visualization.Library!Visualization.SlaDashboardViewInstanceDaily%7D

The following procedure creates a SharePoint page with the Operations Manager Dashboard Viewer web part that can only be accessed by users who have an Operations Manager user role, such as Operator or Administrator. To configure the Operations Manager Dashboard Viewer web part so that those who are not Operations Manager users can view it, perform the following steps and then see the procedure **How to Configure the Web Part to Use Shared Credentials**.

To add the web part to a page

1. Open an Internet browser, and then navigate to the SharePoint server.
2. In the **Site Actions** dropdown menu, click **New Page**.
3. Enter a name for the page, and then click **Create**.
4. The new page opens with editing tools available. Below **Editing Tools**, click **Insert**.
5. On the **Insert** toolbar, click **Web Part**.
6. In **Categories**, click **Microsoft System Center**.
7. In **Web Parts**, click **Operations Manager Dashboard Viewer Web Part**, and then click **Add**.
8. Click the arrow in the top right of the web part, and then click **Edit web part**.
9. Select the web console server in the **Dashboard Server** field, and enter the URI for the dashboard in the **Dashboard Parameters** field, and then click **OK**.
10. On the menu bar, click **Page**.
11. Click **Save & Close**.

Note

After you correctly set up a dashboard web part in SharePoint, you might receive an error message saying “ticket has expired”. This is because there is a very narrow time-out for an override ticket (by default, 5 seconds). If the time on the server running SharePoint and the Web console server differ by more than this value, the connection fails. This is a likely situation if the computers are in different domains and are using a different time

source. You can increase the time-out on the SharePoint Server in the web console list, but this would make the server more vulnerable to attack. The best solution is to synchronize the time between the server running SharePoint and the web console server.

How to Configure the Web Part to Use Shared Credentials

To configure the Operations Manager Dashboard Viewer web part so that those who are not Operations Manager users can view it, perform the following procedures. In the first procedure, you configure credentials by creating a Target Application ID in SharePoint. Next, you configure the web part environment.

Note

Operations Manager provides two scripts in the setup\SharePoint directory to allow users to add and update the SharePoint web environment keys from the web config file: add-OperationsManager-WebConsole-Environment.ps1 and update-OperationsManager-WebConsole-Environment.ps1. These scripts strip the encryptionAlgorithm and encryptionValidationAlgorithm for the override ticket from the web config file and add or update it in the sharepoint environment. This allows you to automate the creation and rotation of keys. Procedures for using these scripts are in this section.

Note

You cannot configure shared credentials in SharePoint Foundation 2010.

To create a Target Application ID

1. In SharePoint Central Administration, in the **Application Management** section, click **Manage service applications**.
2. Double-click **Secure Store Service**.
3. Click **New**.
4. On the **Application settings** page, enter a Target Application ID, a display name, and an email contact address. The Target Application ID is a unique text string that is used by the Secure Store Service application to identify this target application. The display name is displayed in the user interface. The contact can be any legitimate email address and does not have to be the identity of an administrator of the Secure Store Service application. In **Target Application Type**, select **Group**. Click **Next**.
5. On the **Add Field** page, accept the default of **Windows User Name** and **Windows Password**, and click **Next**.
6. In **Target Application Administrators**, enter a domain account, and click **OK**.
7. Click the dropdown arrow to the right of the name of the Target Application ID that you created, and click **Set Credentials**.
8. In the **Windows User Name** field, enter the user name of the account you want the web part to use. Enter the password for the account and confirm the password, and then click

OK.

To configure the Web Part environment to use shared credentials

1. On the server hosting the Web console, in the installation folder for the Operations Manager web console, locate the Web.config file. The default installation path is C:\Program Files\System Center 2012\Operations Manager\WebConsole\WebHost.
2. Open Web.config in a text editor.
3. Locate the <encryption> section.
4. Locate the OverrideTicketEncryptionKey entry. In the following example, the first bold value is the encryption algorithm key and the second bold value is the encryption validation algorithm key:

   Example: <key name="OverrideTicketEncryptionKey" algorithm="3DES" value="**92799B26F0BF54EE76A40CFECDB29868927D2DA4D7E57EBD**"> <validation algorithm="HMACSHA1" value="**7526BAC9FC9562835A3872A3DC12CB8B**"/>
5. Copy both keys and close Web.config.
6. On the SharePoint site, in the **Site Actions** dropdown menu, click **View All Site Content**.
7. In **Lists**, click **Operations Manager Web Console Environments** .
8. Click the web part that you want to configure, and then click **Edit Item**.
9. In the **TargetApplicationID** field, enter the Target Application ID that you created in the previous procedure.
10. In the **Encryption Algorithm Key** field, enter the encryption algorithm key that you copied from Web.config.
11. In the **Encryption Validation Algorithm Key** field, enter the encryption validation algorithm key that you copied from Web.config.
12. Click **Save**.

Repeat this procedure for each Operations Manager environment.

To configure the environment for a Web Part by using a script

1. Copy the add-OperationsManager-WebConsole-Environment.ps1 file, which is in the Operations Manager installation folder under Setup\amd64\SharePoint, to the SharePoint server.
2. Open Operations Manager Shell.
3. Run add-OperationsManager-WebConsole-Environment.ps1 using the following parameters:

   -title *the name of the dashboard view*

   -webconsoleUNC "*path to the web.config file, not including filename*"

   Note
   The web.config file is found under Program Files\System Center 2012\Operations Manager\WebConsole\WebHost on the computer running the

web console.

-targetApplicationID *the Target Application ID*

How to Add Additional Environments to the Web Part

Adding new environments to the Web Part enables you to display dashboards from multiple management groups.

To add environments to the Web Part

1. On the SharePoint site, in the **Site Actions** dropdown menu, click **View All Site Content**.
2. In **Lists**, click **Operations Manager Web Consoles**.
3. Click **Add new item**.
4. In the **Name** field, enter a unique name.
5. In the **HostURI** field, enter the URI to a server hosting the Operations Manager web console. For example: **http://localhost/OperationsManager/**
6. Click **Save**.

To add environments to a Web Part by using a script

1. Copy the update-OperationsManager-WebConsole-Environment.ps1 file, which is in the Operations Manager installation folder under Setup\amd64\SharePoint, to the SharePoint server.
2. Open Operations Manager Shell.
3. Run update-OperationsManager-WebConsole-Environment.ps1 using the following parameters:

   -title *the name of the dashboard view*

   -webconsoleUNC "*path to the web.config file, not including filename*"

   Note
   The web.config file is found under Program Files\System Center 2012\Operations Manager\WebConsole\WebHost on the computer running the web console.

   -targetApplicationID *the Target Application ID*

How to Uninstall the Operations Manager Web Part

As with deploying the Operations Manager Web Part, you can uninstall the Web Part from all sites and web applications in the farm or from a specific site or web application. The Web Part

can be uninstalled by using a script or retracted by using the SharePoint 2010 Central Administration site.

To uninstall the Web Part by using a Script

1. Copy the install-OperationsManager-DashboardViewer.ps1 file to a location that the SharePoint 2010 Management Shell can access.
2. Open the SharePoint 2010 Management Shell and navigate to the directory where you saved the install-OperationsManager-DashboardViewer.ps1 file.
3. In the SharePoint 2010 Management Shell, type the following command, and then press **Enter**.

   .\uninstall-OperationsManager-DashboardViewer.ps1 –solutionPath *<directory for Microsoft.EnterpriseManagement.SharePointIntegration.wsp>* **-url** *<optional, for uninstalling from a specific portal address or website>*

   Example that uninstalls the Web Part from a specific portal address:

   .\uninstall-OperationsManager-DashboardViewer.ps1 "C:\Program Files\System Center Operations Manager 2012\" http://localhost:4096

   If an error occurs when you run the script, you must disable the RemoteSigned default code-signing execution policy for the SharePoint 2010 Management Shell. To allow the install-OperationsManager-DashboardViewer.ps1 script to run, type this command, and then press **enter**:

   Set-ExecutionPolicy Unrestricted

   You will see some confirmation messages, select **Y** to confirm, and then run the script.
4. If you disabled the RemoteSigned default code-signing execution policy to run the install-OperationsManager-DashboardViewer.ps1 script, you should re-enable it after the script runs. Type this command, and then press **enter**:

   Set-ExecutionPolicy Restricted

   You will see some confirmation messages, select **Y** to confirm.

To retract the Web Part by using SharePoint Central Administration

1. Open the SharePoint 2010 Central Administration site.
2. Click **System Settings**.
3. Click **Manage Farm Solutions**.
4. Right-click the Microsoft.EnterpriseManagement.SharePointIntegration.wsp file, and then click **Retract**.

See Also

Using the Operations Manager Consoles

Finding Data and Objects in the Operations Manager Consoles

Using Views in Operations Manager
Not Monitored and Gray Agents
Subscribing to Alert Notifications
Using Reports in Operations Manager

Subscribing to Alert Notifications

In System Center 2012 – Operations Manager, when an alert is generated, Operations Manager can notify designated individuals by email, instant message (IM), or text message (SMS). Notifications can also run commands automatically when an alert is raised on a monitored system.

A notification requires the following elements:

- A Run As account that provides credentials to the Notification Account Run As profile.
- A notification channel which defines the format for the notification and the method by which the notification is sent.
- A notification subscriber which defines the recipients and the schedule for sending notifications to the subscriber.
- A notification subscription which defines the criteria for sending a notification, the channel to be used, and the subscribers to receive the notification.

An Operations Manager administrator must configure the Run As account for notifications and define the notification channels. An Operations Manager administrator, advanced operator, or operator can create a subscriber and a subscription.

Subscribing to Alert Notifications topics

- How to Create and Configure the Notification Action Account
- How to Enable an Email Notification Channel
- How to Enable an Instant Message Notification Channel
- How to Enable a Text Message (SMS) Notification Channel
- How to Enable a Command Notification Channel
- How to Create Notification Subscribers
- How to Create Notification Subscriptions
- How to Customize Message Content for Notifications
- How to Subscribe to Notifications from an Alert
- How to Create Subscriptions Using Classes and Groups
- How to Specify Which Alerts Generate Notifications (Conditions)
- Sending Notifications for Specific Computers and Specific Alerts to Specific Teams

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Getting Information from Operations Manager
- Using the Operations Manager Consoles
- Finding Data and Objects in the Operations Manager Consoles
- Using Views in Operations Manager
- Using SharePoint to View Operations Manager Data
- Using Reports in Operations Manager

How to Create and Configure the Notification Action Account

In System Center 2012 – Operations Manager, when an alert is generated, Operations Manager can notify designated individuals by email, instant message (IM), or text message (SMS). The Notification Account Run As profile is used to send notifications. For notifications to work correctly, you must create a Run As account that provides the credentials for sending notifications and associate the Run As account to the Notification Account profile.

To create and configure the notification action account

1. Log on to the computer with a user account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. In the **Administration** workspace, right-click **Security**, and then click **Create Run As Account**. Use the Create Run As Account Wizard to create an account to use as the Notification action account, which is used to send the notifications.
4. On the **Introduction** page, click **Next**.
5. On the **General Properties** page, select **Windows** in the **Run As Account type** list, and then in **Display name**, type **Notification action account**. Click **Next**.
6. On the **Credentials** page, type the information for the user name, password, and domain of the user account that to be used for notifications. Click **Next**.
7. Select the **More secure** distribution security option. For more information on this option, see Distribution and Targeting for Run As Accounts and Profiles.
8. Click **Create**.
9. In the navigation pane, click **Accounts** under **Run As Configuration**.
10. In the details pane, right-click **Notification action account**, and then click **Properties**.
11. On the **Distribution** tab, click **Add**.
12. In the **Computer Search** window, click **Search** to display a name of available computers.

13. Select the server or servers to distribute the credentials to, click **Add**, and then click **OK** to close the search window.
14. Click **OK** to close the properties window.
15. In the navigation pane, click **Profiles** under **Run As Configuration**.
16. Right-click **Notification Account** and click **Properties**, which will open the **Run As Profile Wizard**.
17. On the **Introduction** page, click **Next**.
18. On the **General Properties** page, click **Next**.
19. On the **Run As Accounts** page, click **Add**.
20. In the **Add a Run As Account** window, in the **Run As account** dropdown menu, select the Run As account that you created earlier in this procedure. Accept the default of **All targeted objects** and then click **OK**.
21. Click **Save**. When the association is completed, click **Close** to close the wizard.

See Also

How to Enable an Email Notification Channel

How to Enable an Instant Message Notification Channel

How to Enable a Text Message (SMS) Notification Channel

How to Enable a Command Notification Channel

How to Create Notification Subscribers

How to Create Notification Subscriptions

How to Customize Message Content for Notifications

How to Subscribe to Notifications from an Alert

How to Create Subscriptions Using Classes and Groups

How to Specify Which Alerts Generate Notifications (Conditions)

Sending Notifications for Specific Computers and Specific Alerts to Specific Teams

How to Enable an Email Notification Channel

To configure alert notifications for System Center 2012 – Operations Manager, your first task is to enable a notification channel. This topic describes how to configure a channel that will send alert notifications to subscribers by using email.

Before you begin, gather the following information:

- SMTP server information
  - Fully qualified domain name (FQDN).
  - Port number for the SMTP server.

    - Authentication method for the SMTP server. You have two choices: anonymous or Windows Integrated.
- Return email address. This address is used for all email notifications on this channel and will receive any replies to notifications.
- Email subject and body text that you want subscribers to receive. For more information, see How to Customize Message Content for Notifications.

To enable an email notification channel

1. Log on to the computer with a user account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. In the navigation pane, under **Notifications**, right-click **Channels**. Click **New channel** and then click **E-mail (SMTP)**.
4. Type a name for the channel, such as **SMTP channel** and optionally provide a description. Click **Next**.
5. In the **SMTP servers** area, click **Add**.
6. In the **Add SMTP Server** dialog box, type the fully qualified domain name (FQDN) of a Simple Mail Transfer Protocol (SMTP) server, type the port number, select the authentication method used by the SMTP server, and then click **OK**.

   Note
   You can add one or more additional servers to act as backup servers. If the primary SMTP server is unavailable, notifications are sent through the secondary server.
7. Type the **Return Address** that should appear on email notifications, and then in the **Retry interval** list, select the number of minutes to wait before trying to resend a notification to the primary SMTP server. Click **Next**.
8. In the **Default e-mail notification format** area, specify the **E-mail subject** and **E-mail message** text or leave the default selections, select the **Importance** level that you want the emails sent with, and then specify the **Encoding** type. You can click the right arrow next to the **E-mail subject** and **E-mail message** boxes for a full list of available variables. For more information, see How to Customize Message Content for Notifications.
9. Click **Finish**, and then click **Close**.

Next task: How to Create and Configure the Notification Action Account

See Also

How to Enable an Instant Message Notification Channel

How to Enable a Text Message (SMS) Notification Channel

How to Enable a Command Notification Channel

How to Create Notification Subscribers

How to Create Notification Subscriptions
Subscribing to Alert Notifications
How to Create and Configure the Notification Action Account
How to Customize Message Content for Notifications
How to Subscribe to Notifications from an Alert
How to Create Subscriptions Using Classes and Groups
How to Specify Which Alerts Generate Notifications (Conditions)
Sending Notifications for Specific Computers and Specific Alerts to Specific Teams

How to Enable an Instant Message Notification Channel

To configure alert notifications for System Center 2012 – Operations Manager, your first task is to enable a notification channel. This topic describes how to configure a channel that will send alert notifications to subscribers by using an instant message.

Before you begin, gather the following information from your instant message server (Live Communications Server):

- Fully qualified domain name (FQDN).
- Protocol used to send messages. You have two choices: TCP or Transport Layer Security (TLS).
- Port used for instant messages. The default is 5060.
- Encoding used by the instant message server and notification subscribers. The default is UTF-8.
- Return address to be used for the instant messages.

To enable an instant message notification channel

1. Log on to the computer with a user account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. In the navigation pane, under **Notifications**, right-click **Channels**. Click **New channel**, and then click **Instant Message (IM)**.
4. Type a name for the channel, such as **IM channel** and optionally provide a description. Click **Next**.
5. In the **IM server** box, type the FQDN of an instant messaging server.
6. Type the **Return Address** that should appear on instant message notifications. Preface the address with **sip:**. In the **Protocol option** list, select either TCP or TLS as the protocol used to send the instant messages. In the **Authentication method** list, select either NTLM or Kerberos as the authentication method for users. In the **IM port** box, the

default instant messaging port of 5060 is entered. Type the port number used to send instant messages.

Note
The return address should be a dedicated address that is used only for Operations Manager notifications.

7. Click **Next**.
8. In the **Default instant messaging notification format** area, in the **IM message** box, specify the text that is sent to notification subscribers. The **IM message** box contains a default message that includes text and variables. You can edit the default message or delete it and replace it with another message. You can click the right arrow next to the **IM message** box for a full list of available variables. For more information, see How to Customize Message Content for Notifications.
9. In the **Encoding** box, select the text format that your IM server and notification subscribers use for transmission. By default, Unicode (UTF-8) is used.
10. Click **Finish** and then click **Close**.

Next task: How to Create and Configure the Notification Action Account

See Also

How to Enable an Email Notification Channel

How to Enable a Text Message (SMS) Notification Channel

How to Enable a Command Notification Channel

How to Create Notification Subscribers

How to Create Notification Subscriptions

Subscribing to Alert Notifications

How to Create and Configure the Notification Action Account

How to Customize Message Content for Notifications

How to Subscribe to Notifications from an Alert

How to Create Subscriptions Using Classes and Groups

How to Specify Which Alerts Generate Notifications (Conditions)

Sending Notifications for Specific Computers and Specific Alerts to Specific Teams

How to Enable a Text Message (SMS) Notification Channel

To configure alert notifications for System Center 2012 – Operations Manager, your first task is to enable a notification channel. This topic describes how to configure a channel that will send alert notifications to subscribers by using a Short Message Service (SMS) or text message.

Note

The modem used for SMS must support SMS Protocol Data Unit (PDU) mode.

To enable an SMS notification channel

1. Log on to the computer with a user account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. In the navigation pane, under **Notifications**, right-click **Channels**. Click **New channel** and then click **Text message (SMS)**.
4. Type a name for the channel, such as **SMS channel** and optionally provide a description. Click **Next**.
5. In the **Text message** box, specify the text that is sent to SMS notification subscribers. The **Text message** box contains a default message that includes text and variables. You can edit the default message or delete it and replace it with another message. You can click the right arrow next to the **Text message** box for a full list of available variables. For more information, see How to Customize Message Content for Notifications.
6. In the **Encoding** box, select the text format for the SMS messages.
7. Click **Finish**, and then click **Close**.

Next task: How to Create and Configure the Notification Action Account

See Also

How to Enable an Instant Message Notification Channel

How to Enable an Email Notification Channel

How to Enable a Command Notification Channel

How to Create Notification Subscribers

How to Create Notification Subscriptions

Subscribing to Alert Notifications

How to Create and Configure the Notification Action Account

How to Customize Message Content for Notifications

How to Subscribe to Notifications from an Alert

How to Create Subscriptions Using Classes and Groups

How to Specify Which Alerts Generate Notifications (Conditions)

Sending Notifications for Specific Computers and Specific Alerts to Specific Teams

How to Enable a Command Notification Channel

To configure alert notifications for System Center 2012 – Operations Manager, your first task is to enable a notification channel. This topic describes how to configure a channel that runs an executable program automatically in response to an alert.

To create a command notification channel, you need the following information:

- Full path of the command file.
- Command line parameters.
- The startup folder for the command, which is the path of the program you want to run.

Important
Unlike the other notification channels, the command notification channel will run its command by using Local System, rather than the Notification Action Account.

To enable a command notification

1. Log on to the computer with a user account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. In the navigation pane, under **Notifications**, right-click **Channels**. Click **New channel** and then click **Command**.
4. Type a unique name for this command channel in the **Notification command channel name** box and a brief description in the **Description** box. Click **Next**.
5. Type the path to the executable file that you want to run in the **Full path to command file** box. For example, “%systemroot%\cmd.exe” or “c:\winnt\system32\cscript.exe”. Type any parameters that you want to run with this command in **Command line parameters** box. Type the directory for this command in the **Startup folder for the command line** box.
6. Click **Finish**, and then click **Close**.

After you have enabled the command notification channel, do the following:

- Create a notification subscriber that has the command channel selected in the subscriber address. For more information, see How to Create Notification Subscribers.
- Create a new subscription and select only the subscriber created for this command. For more information, see How to Create Notification Subscriptions.

See Also

How to Enable an Instant Message Notification Channel

How to Enable a Text Message (SMS) Notification Channel

How to Enable an Email Notification Channel

How to Create Notification Subscribers
How to Create Notification Subscriptions
Subscribing to Alert Notifications
How to Create and Configure the Notification Action Account
How to Customize Message Content for Notifications
How to Subscribe to Notifications from an Alert
How to Create Subscriptions Using Classes and Groups
How to Specify Which Alerts Generate Notifications (Conditions)
Sending Notifications for Specific Computers and Specific Alerts to Specific Teams

How to Create Notification Subscribers

In System Center 2012 – Operations Manager, when an alert is generated, Operations Manager can notify designated individuals by email, instant message (IM), or text message (SMS). Notifications can also run commands automatically when an alert is raised on a monitored system. A notification requires a channel, a subscriber, and a subscription.

These procedures explain how to create subscribers for notifications. A notification subscriber defines when to send notifications and the addresses to which the notifications should be sent. A subscriber can be an individual user account or a distribution list.

Notification channels must be enabled before you create subscribers. After a subscriber is created, you create a notification subscription that defines the format of the notification message and any filters such as age or severity of the alert.

To create a notification subscriber as an administrator

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. Under **Notifications**, right-click **Subscribers,** and click **New subscriber**.
4. On the **Description** page, type a display name for this subscriber.
5. On the **Schedule Notifications** page, click **Always send notifications**, or **Notify only during the specified times** and specify when notifications should be sent to this subscriber. The options available allow you to:
   - Limit notifications to a specific range of dates.
   - Specify that notifications are sent only during certain hours or except for certain hours.
   - Specify that notifications will be sent only on certain days of the week.
   - Set a time zone to be used for the subscriber.

   Note

The settings on the **Schedule Notifications** page apply globally to the subscriber. You can also specify unique schedule settings for each address that you add to the subscriber, in the following steps. For example, you can add one email address that receives the notifications during business hours and add a second email address that receives the notifications outside of business hours.

6. On the **Subscriber Addresses** page, click **Add** to add subscriber addresses to the notification.
7. On the **Describe the Subscriber Address** page, enter a name to identify the subscriber address, and then click **Next**.
8. On the **Provide the Channel and Delivery Address** page, perform the following steps:
   a. In **Channel Type**, select between email, instant message, text message, or command for the method of notification.
   b. If you select command for channel type, in **Command Channel**, select the name of a command channel. The command channel must be created before you create the subscriber. Skip the next step, because no delivery address is specified for a command channel.
   c. In **Delivery address for the selected channel**, enter the address to which the notification should be sent.
   d. Click **Next**.
9. On the **Schedule Notifications** page, click **Always send notifications**, or **Notify only during the specified times** and click **Add** to create a date range, and then click **Next**.
10. Click **Add** to define another subscriber address. Otherwise, click **Finish**, and then click **Close**.
11. The new subscriber displays in the **Subscribers** pane.

Next task: How to Create Notification Subscriptions

To create a notification subscriber as an operator

1. Log on to the computer with an account that is a member of the Operations Manager Operators or Advanced Operators role.
2. In the Operations console, click **Tools** in the top menu bar, and then click **My Subscriber Information**.
3. The **Description** page displays the name you are logged in as and cannot be changed. Click **Next**.
4. On the **Schedule Notifications** page, click **Always send notifications**, or **Notify only during the specified times** and click **Add** to create a date range, and then click **Next**.
5. On the **Subscriber Addresses** page, click **Add** to add subscriber addresses to the notification.
6. On the **Describe the Subscriber Address** page, enter a name to identify the subscriber address, and then click **Next**.
7. On the **Provide the Channel and Delivery Address** page, perform the following steps:
   a. In **Channel Type**, select between email, instant message, text message, or

command for the method of notification.

b. If you select command for channel type, in **Command Channel**, select the name of a command channel. The command channel must be created before you create the subscriber. Skip the next step, because no delivery address is specified for a command channel.

c. In **Delivery address for the selected channel**, enter the address to which the notification should be sent.

d. Click **Next**.

8. On the **Schedule Notifications** page, click **Always send notifications**, or **Notify only during the specified times** and click **Add** to create a date range, and then click **Next**.
9. Click **Add** to define another subscriber address. Otherwise, click **Finish**, and then click **Close**.

Next task: How to Create Notification Subscriptions

See Also

How to Enable an Instant Message Notification Channel

How to Enable a Text Message (SMS) Notification Channel

How to Enable a Command Notification Channel

How to Enable an Email Notification Channel

How to Create Notification Subscriptions

Subscribing to Alert Notifications

How to Create and Configure the Notification Action Account

How to Customize Message Content for Notifications

How to Subscribe to Notifications from an Alert

How to Create Subscriptions Using Classes and Groups

How to Specify Which Alerts Generate Notifications (Conditions)

Sending Notifications for Specific Computers and Specific Alerts to Specific Teams

How to Create Notification Subscriptions

In System Center 2012 – Operations Manager, when an alert is generated, Operations Manager can notify designated individuals by email, instant message (IM), or text message (SMS). Notifications can also run commands automatically when an alert is raised on a monitored system. A notification requires a channel, a subscriber, and a subscription.

These procedures explain how to configure a notification subscription. A subscription defines the criteria for a notification, such as when a critical alert is generated. A subscription also defines the channel to be used for the notification and the subscribers to receive the notification.

Notification channels and subscribers must be configured before you create a subscription.

To create a notification subscription as an administrator

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. In the **Administration** workspace, expand **Notifications**, right-click **Subscriptions,** and then click **New subscription**. The Notification Subscription Wizard starts.
4. On the **Description** page, in **Subscription name,** type a descriptive name for the subscription, type a short description, and then click **Next**.
5. On the **Subscription Criteria** page, you can set conditions that will determine when notifications will be sent to specified subscribers. If you do not set conditions, notifications will be sent for all alerts. Click **Next**.

   Note
   You will also receive notifications when an alert is updated.
6. On the **Subscribers** page, click **Add** to add subscribers who are already defined, or click **New** to add new subscribers. For more information on defining subscribers, see How to Create Notification Subscriptions.
7. Click **Next**.
8. On the **Channels** page, click **Add** to add a channel that is already defined, or click **New** to add a new channel. For more information on defining channels, see How to Enable an Email Notification Channel, How to Enable an Instant Message Notification Channel, How to Enable a Text Message (SMS) Notification Channel, and How to Enable a Command Notification Channel.
9. In the **Alert aging** section on the **Channels** page, select to send notifications without delay or set a value in minutes that notification should be delayed unless conditions remain unchanged, and then click **Next**.
10. Review the settings on the **Summary** page, click **Finish**, and then click **Close**.

To create a notification subscription as an operator

1. Log on to the computer with an account that is a member of the Operations Manager Operators or Advanced Operators role.
2. In the Operations console, click **Tools** in the top menu bar, and then click **My Subscriptions**.
3. In the **Notification Subscriptions** window, click **New**.
4. On the **Description** page, in **Subscription name,** type a descriptive name for the subscription, type a short description, and then click **Next**.
5. On the **Subscription Criteria** page, you can set conditions that will determine when notifications will be sent to specified subscribers. If you do not set conditions, notifications will be sent for all alerts. Click **Next**.

   Note

You will also receive notifications when an alert is updated.

6. On the **Subscribers** page, click **Add** to add subscribers who are already defined, or select a subscriber in the **Selected subscribers** box and click **Edit** to change the settings for this subscription. For more information on defining subscribers, see How to Create Notification Subscriptions.
7. Click **Next**.
8. On the **Channels** page, click **Add** to add a channel that is already defined, or click **New** to create a customized copy of an existing channel. For more information on defining channels, see How to Enable an Email Notification Channel, How to Enable an Instant Message Notification Channel, How to Enable a Text Message (SMS) Notification Channel, and How to Enable a Command Notification Channel.
9. In the **Alert aging** section on the **Channels** page, select to send notifications without delay or set a value in minutes that notification should be delayed unless conditions remain unchanged, and then click **Next**.
10. Review the settings on the **Summary** page, click **Finish**, and then click **Close**.

See Also

How to Enable an Instant Message Notification Channel

How to Enable a Text Message (SMS) Notification Channel

How to Enable a Command Notification Channel

How to Create Notification Subscribers

How to Enable an Email Notification Channel

Subscribing to Alert Notifications

How to Create and Configure the Notification Action Account

How to Customize Message Content for Notifications

How to Subscribe to Notifications from an Alert

How to Create Subscriptions Using Classes and Groups

How to Specify Which Alerts Generate Notifications (Conditions)

Sending Notifications for Specific Computers and Specific Alerts to Specific Teams

How to Customize Message Content for Notifications

In System Center 2012 – Operations Manager, you can customize the format that will be used for messages that notify you of alerts. The format of an alert notification is determined by the channel by which the notification is sent. Each channel type has a default format, as shown in the following examples.

Note

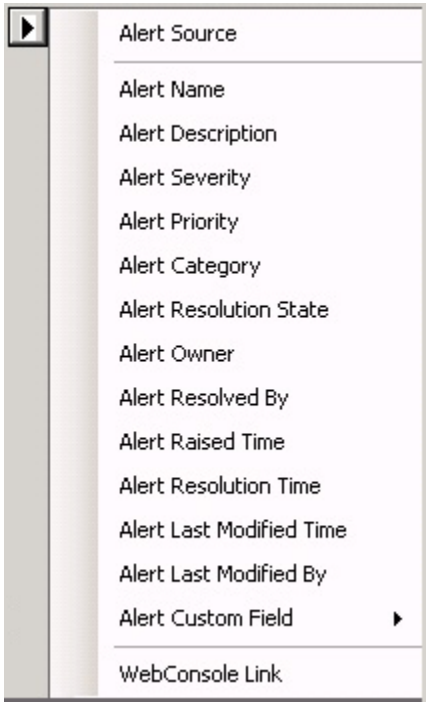
The command channel type is not mentioned because it generates a command rather than a notification message.

Channel type	Default notification format
Email	**Subject**: Alert: *alert name* Resolution state: *new or closed* Alert: Source: Path: Last modified by: Last modified time: Alert description: Alert view link: Notification subscription ID generating this message:
Instant message (IM)	Alert: *alert name* Path: *path to managed entity* Resolution state: *new or closed* Last modified by:
SMS (text message)	Alert: *alert name* Resolution state: *new or closed*

You can change the format on the **Format** page of the channel type wizard when you create the channel or after the channel is created. The procedure is the same for all three channel types.

To configure notification format

1. On the **Format** page of the channel type wizard, in the message box for the channel type (or subject box for the email channel), delete any information from the default format that you do not want to include.
2. Position your cursor in the location of the box where you want to add information.
3. Type any non-variable text that you want in the message.
4. Click the button to the right of the box to display the information you can add to the subject or message for notifications, as shown in the following illustration.



5. Click any item in that list to add the corresponding variable to the notification message. For example, if you click **Alert Severity**, the following variable will be added to the box:

   $Data[Default='Not Present']/Context/DataItem/Severity$

   Note
   When a default value for a parameter is included, such as [Default=’Not Present’] in the preceding example, it indicates the text to provide when the alert does not contain data for that parameter.

6. When you are done, click **Finish**. All notification messages that use the same channel will be formatted the same way.

Customizing a Channel for a Subscription

When you create a subscription, you can copy an existing channel that you can customize for that subscription.

To customize a channel for a subscription

1. In the **Notification Subscription Wizard**, on the **Channels** page, click **New**, and then click **Create Customized Copy**.
2. In the **Channel Search** window, use **Filter by** and **Search** to locate the channel you want to copy. Select the channel in **Available channels**, click **Add**, and then click **OK**.
3. The notification channel wizard for the selected channel opens. You can change the name, description, settings, and message format on the corresponding wizard pages. As

a best practice, change the name of the channel to distinguish it from the original channel. Click **Finish** when you are done making changes.

See Also

How to Enable an Instant Message Notification Channel

How to Enable a Text Message (SMS) Notification Channel

How to Enable a Command Notification Channel

How to Create Notification Subscribers

How to Create Notification Subscriptions

Subscribing to Alert Notifications

How to Create and Configure the Notification Action Account

How to Enable an Email Notification Channel

How to Subscribe to Notifications from an Alert

How to Create Subscriptions Using Classes and Groups

How to Specify Which Alerts Generate Notifications (Conditions)

Sending Notifications for Specific Computers and Specific Alerts to Specific Teams

How to Subscribe to Notifications from an Alert

In System Center 2012 – Operations Manager, when an alert is generated, Operations Manager can notify designated individuals by email, instant message (IM), or text message (SMS). Notifications can also run commands automatically when an alert is raised on a monitored system. A notification requires a channel, a subscriber, and a subscription.

You can create a notification subscription from an alert to ensure that you are notified if the alert is sent again. You can either create a new subscription or add the alert to an existing subscription. In the following procedure, you create a new subscription.

Note

You must have configured a notification channel and notification subscriber to perform this procedure.

To create a notification subscription from an alert

1. In the **Alerts** view, right-click the alert, click **Notification subscription**, and then click **Create**.
2. The text boxes for the name and description for the subscription are pre-populated with information from the alert. Click **Next**.

3. The text boxes for the conditions and criteria for when the notification is sent are pre-populated with default values from the alert. Click **Next**.
4. Click **Add or Remove** to select the notification subscriber that the notifications should be sent to.
5. Click **Search** to display all available subscribers.
6. Double-click the subscriber you want to use, and then click **OK**.
7. Click **Next**.
8. Click **Add or Remove** to select the notification channel to use.
9. Click **Search** to display all available channels.
10. Double-click the channel you want to use, and then click **OK**.
11. Click **Next**, and then click **Finish**.
12. Click **Close**.

See Also

How to Enable an Instant Message Notification Channel

How to Enable a Text Message (SMS) Notification Channel

How to Enable a Command Notification Channel

How to Create Notification Subscribers

How to Create Notification Subscriptions

Subscribing to Alert Notifications

How to Create and Configure the Notification Action Account

How to Customize Message Content for Notifications

How to Enable an Email Notification Channel

How to Create Subscriptions Using Classes and Groups

How to Specify Which Alerts Generate Notifications (Conditions)

Sending Notifications for Specific Computers and Specific Alerts to Specific Teams

How to Create Subscriptions Using Classes and Groups

In System Center 2012 – Operations Manager, when an alert is generated, Operations Manager can notify designated individuals. These notifications have three parts:

- A channel, which can be email, instant message (IM), or text message (SMS). Notifications can also run commands automatically when an alert is raised on a monitored system.
- A subscriber, which defines the recipients and the schedule for sending notifications to the subscriber.

- A subscription, which defines the criteria for sending a notification, the channel to be used, and the subscribers to receive the notification.

You can use classes and groups to configure the subscription. Two of the conditions for alerts that you can select for a subscription are:

- Raised by any instance in a specific group.
- Raised by any instance in a specific class.

You can select multiple groups or classes when you set the value for either condition.

Note
Operations Manager does not support using “not equal to” or “not a member of” for notification subscriptions.

Groups

Groups are logical collections of objects, such as Windows-based computers, hard disks, or instances of Microsoft SQL Server. Some groups are created by Operations Manager, such as the Operations Manager Agent Managed Computer Group and the All Windows Computers group. You can create groups to meet your specific monitoring needs, such as all Windows computers in a specific organizational unit (OU). For more information on creating groups, see **How to Create Groups in Operations Manager 2012**.

Groups can have explicit or dynamic membership. Suppose you wanted to create a subscription that would send notifications for alerts generated by five specific servers to one person and notifications for alerts generated by a different five servers to a second person. You could create two groups and explicitly assign each server to one of the groups, and then create a subscription that would send notifications for each group to the appropriate person.

When you select a specific group as a condition for an alert notification, notifications are sent for alerts raised by any member of the specified group.

Classes

A class represents a kind of object, and every object in Operations Manager is considered an instance of a particular class. All instances of a class share a common set of properties. Each object has its own values for these properties which are determined when the object is discovered. Most management packs define a set of classes that describe the different components that make up the application that is being monitored and to the relationships between those classes.

Every class in Operations Manager has a base class. A class has all the properties of its base class and potentially adds more. All of the classes from the different management packs installed in your management group can be arranged in a tree with each class positioned under its base class. If you start at any class, and then walk up the tree following its base class, and then the base class of that class, and so on, you eventually reach the **Object** class which is the root of the System Center class library.

When you select a specific class as a condition for an alert notification, notifications are sent for alerts raised by any instance of the specified class.

Examples

Example 1: To send notifications of alerts for UNIX computers to your UNIX administrator, you create a subscription using the condition **Raised by any instance in a specific group**, select the **UNIX/Linux Computer Group** as the value for the condition, and select the UNIX administrator as the subscriber.

Example 2: To send notifications of alerts for the UNIX operating system to your UNIX administrator, you create a subscription using the condition **Raised by any instance in a specific class**, select the **UNIX/Linux Operating System** as the value for the condition, and select the UNIX administrator as the subscriber.

In the first example, the UNIX administrator would be notified of alerts raised by the operating system on a UNIX computer, as well as any other alerts that are raised by a UNIX computer. In the second example, the notifications would only be sent when the alert was raised by the UNIX operating system.

See Also

How to Enable an Instant Message Notification Channel

How to Enable a Text Message (SMS) Notification Channel

How to Enable a Command Notification Channel

How to Create Notification Subscribers

How to Create Notification Subscriptions

Subscribing to Alert Notifications

How to Create and Configure the Notification Action Account

How to Customize Message Content for Notifications

How to Subscribe to Notifications from an Alert

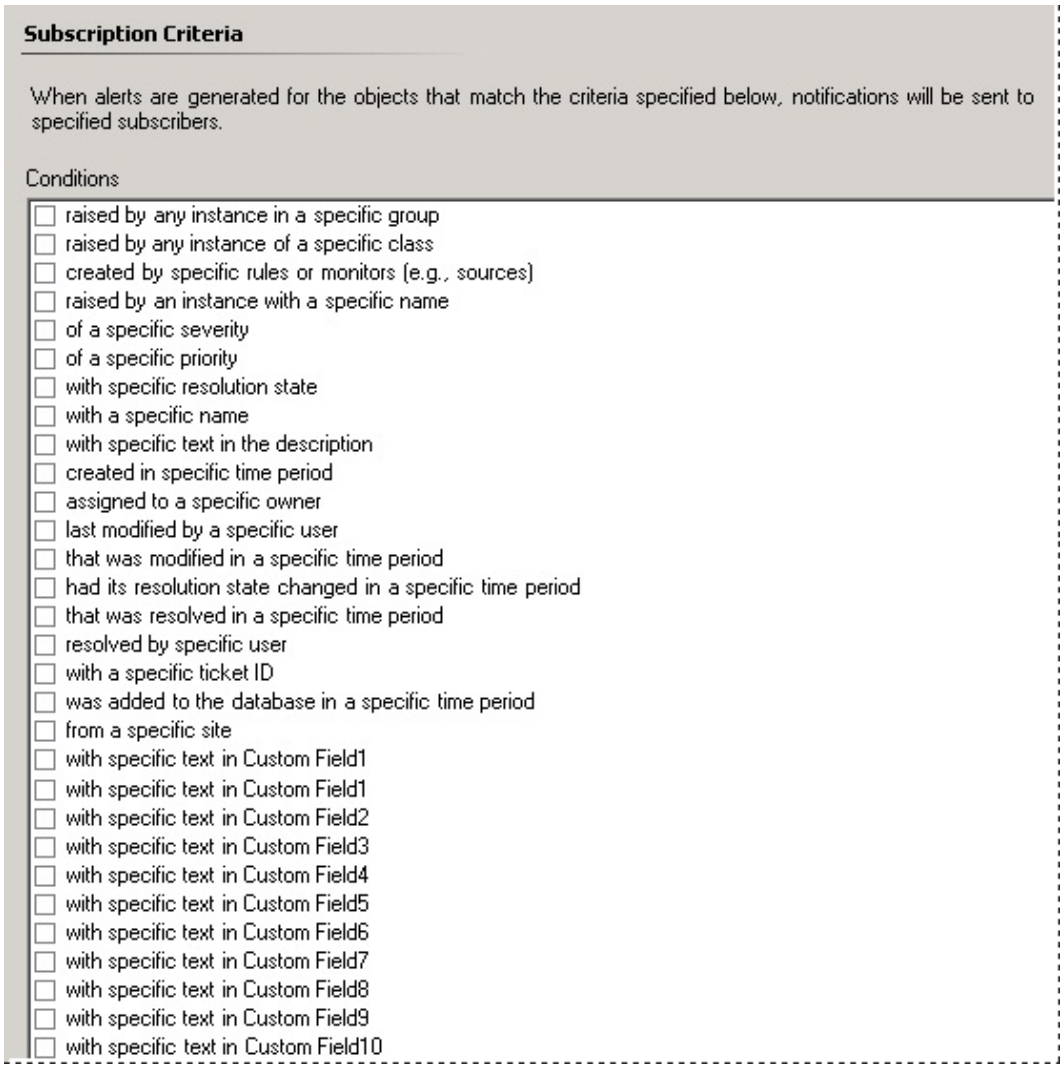
How to Enable an Email Notification Channel

How to Specify Which Alerts Generate Notifications (Conditions)

Sending Notifications for Specific Computers and Specific Alerts to Specific Teams

How to Specify Which Alerts Generate Notifications (Conditions)

When you create a subscription to be notified of Operations Manager alerts, you must specify the criteria or conditions that determine the alerts that will generate a notification. The following illustration shows the conditions you can choose from.



When you select a condition, it is added to the **Criteria description**. In the **Criteria description** box, the word **specific** is blue and underlined, and is a placeholder for the value for the condition. Click **specific** to set the value for that condition.

For example, for the condition of **a specific severity**, click **specific**, and then select from the available values: **Information**, **Warning**, and **Critical**.

When you create a notification subscription from an alert that has been generated, the conditions for the subscription are configured automatically with values from the specific alert.

See Also

How to Enable an Instant Message Notification Channel

How to Enable a Text Message (SMS) Notification Channel

How to Enable a Command Notification Channel

How to Create Notification Subscribers
How to Create Notification Subscriptions
Subscribing to Alert Notifications
How to Create and Configure the Notification Action Account
How to Customize Message Content for Notifications
How to Subscribe to Notifications from an Alert
How to Create Subscriptions Using Classes and Groups
How to Enable an Email Notification Channel
Sending Notifications for Specific Computers and Specific Alerts to Specific Teams

Sending Notifications for Specific Computers and Specific Alerts to Specific Teams

In System Center 2012 – Operations Manager, when an alert is generated, Operations Manager can notify designated individuals. These notifications have three parts:

- A channel, which can be email, instant message (IM), or text message (SMS). Notifications can also run commands automatically when an alert is raised on a monitored system.
- A subscriber, which defines the recipients and the schedule for sending notifications to the subscriber.
- A subscription, which defines the criteria for sending a notification, the channel to be used, and the subscribers to receive the notification.

You can use the combination of subscriber and subscription to tailor which alerts are sent to individuals or teams.

For example, suppose you have a team that wants to be notified of any problems on specific test lab servers that the team owns. To configure notifications for this situation, you would:

1. Create a notification subscriber that uses the addresses for the individual team members or the address of a distribution list that contains the team members.
2. Create a group that contains the test lab servers that the team wants to monitor.
3. Create a subscription that sends notifications of alerts to the notification subscriber from step 1 for alerts raised by any member of the group from step 2.

See Also

How to Enable an Instant Message Notification Channel

How to Enable a Text Message (SMS) Notification Channel

How to Enable a Command Notification Channel

How to Create Notification Subscribers

How to Create Notification Subscriptions

Subscribing to Alert Notifications

How to Create and Configure the Notification Action Account

How to Customize Message Content for Notifications

How to Subscribe to Notifications from an Alert

How to Create Subscriptions Using Classes and Groups

How to Specify Which Alerts Generate Notifications (Conditions)

How to Enable an Email Notification Channel

Using Reports in Operations Manager

For a description of the differences between dashboard views and reports, see this System Center Operations Manager blog post.

Using Reports in Operations Manager topics

- Operations Manager Reports Library
- How to Create Reports in Operations Manager
- How to Save a Report
- How to Run a Report
- Scheduling Reports
- How to Export a Report
- How to Troubleshoot Reports that Return No Data

Operations Manager Reports Library

System Center 2012 – Operations Manager provides the reports described in the following tables. For more information on a report, in the **Reporting** workspace, click the report and view the **Report Details**. For information on reports that are provided by other management packs, see the respective management pack guides.

Note
When you first install Operations Manager, it may take several minutes for all report libraries to appear in **Reporting**.

Microsoft Generic Report Library

Report	Description
Alert Logging Latency	This report helps to isolate issues in monitoring with Operations Manager by showing the

Report	Description
	logging latency of an alert for selected objects over time.
Alerts	This report shows alerts raised during the selected report duration and for given filter parameters for selected objects.
Availability	This report shows the time in state for selected objects during the selected report duration. Time in state is summarized by default as per the objects' availability monitors.
Configuration Changes	This report shows the changes in configuration for selected objects over time.
Custom Configuration	This report shows configuration data filtered by all entered parameters.
Custom Event	This report shows event data filtered by all selected parameters.
Event Analysis	This report shows a table of events and a count by server filtered by all entered parameters.
Health	This report shows the time in state for selected objects during the selected report duration. Time in state is summarized by default as per the objects' overall entity health.
Most Common Alerts	This report shows the most common alerts raised during the selected report duration and for given filter parameters for selected objects.
Most Common Events	This report shows the most common events raised during the selected report duration and for given filter parameters for selected objects.
Overrides	This report shows overrides configured in or applied to selected management packs over time.
Performance	This report shows selected objects and performance counter values graphically over time.
Performance Detail	This report shows selected objects and performance counter values graphically over time.

Report	Description
Performance Top Instances	This report shows the top or bottom “N” instances for selected objects and a specific performance counter rule.
Performance Top Objects	This report shows the top or bottom “N” objects for selected objects and a specific performance counter rule.

Client Monitoring Views Library

Report	Description
Top N Applications	This report shows the top “N” applications based on their crash count and provides details for each application.
Top N Applications Growth and Resolution	This report shows the top “N” applications based on their growth percentile computed against two specified time intervals.
Top N Error Groups	This report shows the top “N” error groups based on their crash count.
Top N Error Groups Growth and Resolution	This report shows the top “N” error groups based on their growth percentile computed against two specified time intervals.

Microsoft Data Warehouse Reports

Report	Description
Data Warehouse Availability	This report shows the availability of the data warehouse components based on the monitor "Data Warehouse Connectivity and Processes State".
Data Warehouse Events	This report shows data warehouse-related events to help determine data warehouse health.
Data Warehouse Properties	This report shows data warehouse properties and grooming settings.

Microsoft ODR Report Library

Report	Description
Alerts Per Day	This report shows the number of alerts generated per day from each rule or monitor that alerted within the report period (by default one week).
Instance Space	This report shows the number of instances of each class (for example, Exchange Servers) that are created in your management group.
Management Group	This report shows the operating system version used in the Operations Manager infrastructure (management servers).
Management Packs	This report shows the versions of each management pack that is installed in your environment. It also summarizes all the overrides you have defined in your environment, as well as custom rules and monitors you have authored.
Most Common Alerts	This report shows the most common alerts generated within the report period (by default one week). It also shows this data by management pack.

System Center Core Monitoring Reports

Report	Description
Agent Counts by Date, Management Group and Version	This report shows detail information for agent accounts during specified time interval.
Agents by Health State	This report shows lists of agents organized by health state.
Data Volume by Management Pack	This report shows the volume of data generated by management packs. The purpose of this report is to provide insight into which management packs are driving the data volumes in your environment so that you can establish baselines and identify opportunities for tuning. From this report, you can obtain more specific details per management pack by clicking one of the counts cells in the table at

Report	Description
	the top of the report to open the Data Volume by Workflow and Instance report for the management packs.
Data Volume by Workflow and Instance	This report shows the volume of data generated, organized by workflows (discoveries, rules, monitors, etc.), as well as by instances.

Microsoft Service Level Report Library

Report	Description
Service Level Tracking Summary Report	This reports shows whether the configured Service Level Objectives (SLOs) met their respective goals, for selected service levels.

Web Application Availability Monitoring Solutions Library

Report	Description
Test Availability	This report shows availability reported by an individual test over time.
Test Performance	This report shows selected objects and performance counter values over time to relate how well a web application has performed.
Web Application Availability	This report shows how available the web application was. The web application availability is the rollup of all tests defined in your web application.

Application Monitoring Reports

Report	Description
Application Failure Analysis	This report provides detailed failure analysis for a selected application.
Application Performance Analysis	This report provides detailed performance analysis for a selected application
Application Status	This report provides daily, weekly and monthly application status summaries.

Report	Description
Problems Distribution Analysis	This report shows the distribution of performance, connectivity, security and code problems across all monitored applications, highlighting the applications that are most problematic.
Summary Failure Analysis	This report provides a breakdown of problems by application.
Summary Performance Analysis	This report provides a breakdown of performance violations by application.
Summary User Analysis	This report highlights the application users who experience most of the problems.
(Client Side Monitoring) Application AJAX Calls Analysis	This report provides detailed failure analysis for a selected application.
(Client Side Monitoring) Application Analysis	This report provides an overview of activity, performance and exception statistics for a selected application.
(Client Side Monitoring) Application Status	This report provides daily, weekly and monthly application status summaries.
(Client Side Monitoring) Client Latency Distribution	This report provides an analysis of client side performance in relation to network latency.
(Client Side Monitoring) Load Time Analysis Based on Subnet	This report provides an analysis of client side performance based on client subnets.
(Client Side Monitoring) Summary Performance Analysis	This report provides an analysis of performance violations by application.
(Client Side Monitoring) Summary Size Analysis	This report provides an analysis of content size across multiple applications and shows the correlation between content size and load time.
(Client Side Monitoring) Summary User Analysis	This report highlights the application users who experience most of the problems.
(Problem Analysis Reports) Application Activity Breakdown	This report shows application activity trends for a selected period in relation to an application's activity during a previous period and average application activity.
(Problem Analysis Reports) Application Daily Activity	This report shows application activity trends for a selected day in relation to an application's

Report	Description
	activity during a previous period and average application activity.
(Problem Analysis Reports) Application Failure Breakdown by Functionality	This report shows the list of application requests that experience most of the problems.
(Problem Analysis Reports) Application Failure Breakdown by Resources	This report provides failure analysis for distributed applications based on the application components and external resource dependencies.
(Problem Analysis Reports) Application Heavy Resources Analysis	This report provides performance analysis for distributed applications based on the application components and external resource dependencies.
(Problem Analysis Reports) Application Slow Request Analysis	This report shows the breakdown of application performance violations based on application requests.
(Problem Analysis Reports) Day of Week Utilization	This report shows application activity trends and application resource utilization trends for a selected period.
(Problem Analysis Reports) Hour of Day Utilization	This report shows application activity trends and application resource utilization trends for a selected period.
(Problem Analysis Reports) Utilization Trend	This report shows application activity trends and application resource utilization trends for a selected period.
(Resource Utilization Analysis) Application CPU Utilization Analysis	This reports highlights applications that have the heaviest CPU utilization and provides a breakdown of CPU utilization based on the servers which host the application.
(Resource Utilization Analysis) Application IO Utilization Analysis	This reports highlights applications that have the heaviest IO utilization and provides a breakdown of IO utilization based on the servers which host each application.
(Resource Utilization Analysis) Application Memory Utilization Analysis	This reports highlights applications that have the heaviest memory utilization and provides a breakdown of memory utilization based on the servers which host each application.

Report	Description
(Resource Utilization Analysis) Application Request Utilization Analysis	This report provides an analysis of application based on the volume of processed requests.
(Resource Utilization Analysis) Computer Application Load Analysis	This report provides an analysis of servers based on the volume of processed requests.
(Resource Utilization Analysis) Computer CPU Utilization Analysis	This reports highlights servers that have the heaviest CPU utilization and provides a breakdown of CPU utilization based on the monitored applications running on each server.
(Resource Utilization Analysis) Computer IO Utilization Analysis	This reports highlights servers that have the heaviest IO utilization and provides a breakdown of IO utilization by monitored applications running on each server.
(Resource Utilization Analysis) Computer Memory Utilization Analysis	This reports highlights servers that have the heaviest memory utilization and provides a breakdown of memory utilization based on the monitored applications running on each server.

See Also

Using Reports in Operations Manager

How to Create Reports in Operations Manager

How to Save a Report

How to Run a Report

Scheduling Reports

How to Export a Report

How to Troubleshoot Reports that Return No Data

How to Create Reports in Operations Manager

- How to Create an Alert Logging Latency Report
- How to Create an Alerts Report
- How to Create an Availability Report
- How to Create a Configuration Changes Report
- How to Create an Event Analysis Report

- How to Create an Operational Data Report

How to Create an Alert Logging Latency Report

The following procedure is an example of how you create an alert logging latency report for a managed computer. An alert logging latency report shows you how much time it took from when an alert was generated until it was written into the Operations Manager database. An alert is not displayed in the Operations console until after it is written into the Operations Manager database. Alert latency can be a function of network delays in your environment.

This information is useful when considering service level agreements (SLA). You might not want to commit to an SLA of 2 minutes if alerts take longer than that to get written into the Operations Manager database.

Note
Operations Manager Reporting must be installed before you can run an alert logging latency report.

To create an alert logging latency report

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Monitoring**.
3. In the **Monitoring** workspace, expand **Monitoring** and then click **Windows Computers**.
4. In the **Windows Computers** pane, click a row with a Health Service instance.
5. In the **Tasks** pane, under **Report Tasks**, click **Alert Logging Latency**.
6. In the **Parameter Area**, click the down arrow in the **From** box and then click **Yesterday**.

   Note
   You can further specify the timeframe for the report in the additional options in the **Parameter Area**.
7. Click the down arrow on the **Threshold** list, and select the latency threshold you want to measure.
8. Click the down arrow on the **Aggregation Type** list, and click the value you want for this report.
9. Click **Run** to display the **Alert Logging Latency Report**.
10. Click **Close** to close the report.

How to Create an Alerts Report

An alerts report summarizes alerts that have occurred on a managed entity. The following procedure is an example of how you create an alerts report for a managed computer. The procedure presented here is applicable to creating other types of alerts reports. In this example procedure, you generate a report for the previous 24-hour period.

Note
Operations Manager Reporting must be installed before you can run an alerts report.

To create an alerts report

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Monitoring**.
3. In the **Monitoring** workspace, expand **Monitoring**, and then click **Wndows Computers**.
4. In the **Windows Computers** pane, click a row with a Health Service instance.
5. In the **Tasks** pane, under **Report Tasks**, click **Alerts**.
6. In the **Reporting Parameter** area, click the down arrow in the **From** box and then click **Yesterday**.

   Note
   You can further specify the timeframe for the report in the additional options in the **Reporting Parameter** area.
7. Click **Run** to display the **Alert Report**.
8. Click **Close** to close the report.

How to Create an Availability Report

The following procedure is an example of how you create an availability report for a managed computer. The procedure presented here is applicable to creating other types of availability reports. In this example procedure, you generate a report for the entire week.

Note
Operations Manager Reporting must be installed before you can run an Availability report.

The availability report provides the following information about the selected computers:

- **Down** – computer state is critical (red)
- **Up** – computer state is healthy (green)
- **Yellow** – computer state is warning (yellow)

- **Unmonitored** – computer or monitor did not exist during reporting period
- **Monitor disabled** – monitor has been disabled, such as by using an override
- **Monitoring unavailable** – the System Center Management Health service monitoring the computer is unavailable
- **Planned/unplanned maintenance** – computer is in maintenance mode; overrides all other states

To create an availability report

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Monitoring**.
3. In the **Monitoring** workspace, expand **Monitoring**, and then click **Windows Computers**.
4. In the **Windows Computers** pane, click the row, or rows, that represent the computer for which you want to run an availability report.
5. In the **Tasks** pane, under **Report Tasks**, click **Availability**.
6. In the **Report** view, in the **Parameter** area, click the down arrow in the **From** box, point to **This week**, and then click **Sunday**.
7. Click the down arrow in the **To** box, point to **This week** and then click **Saturday**.
8. Click **Use business hours**.

   Note
   You can further specify the timeframe for the report in the additional options in the **Parameter** area.
9. When you have specified the timeframe for the report, click **Run** to display the Availability Report.
10. For a more detailed report, such as a report showing a graph for every day, click the horizontal bar graph under **Availability Tracker**.
11. In the tool bar, click **View**, point to **Go To**, and then click **Back to Parent Report** to return to the original report.
12. Click **Close** to close the report.

How to Create a Configuration Changes Report

System Center 2012 – Operations Manager monitors parameters of objects that are defined in management packs. You can create a Configuration Changes report listing changes that have occurred to monitored parameters. You should expect a delay of at least 2 minutes from the time when a change is made until it is reflected in a Configuration Changes report. In the following

example procedure, you will make a change to the Heartbeat Interval setting and then create a Configuration Changes report to view the result.

To report configuration changes

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. Click **Settings**.
4. Under **Agent**, double-click **Heartbeat** .
5. Change the agent Heartbeat Interval from its default value of 60 seconds to 120 seconds, and click **OK**.
6. In the Operations console, click **Monitoring**.
7. In the **Monitoring** workspace, expand **Monitoring**, and then click **Windows Computers**.
8. In the **Windows Computers** pane, click a row containing a Health Service instance.
9. In the **Tasks** pane, under **Report Tasks**, click **Configuration Changes**.
10. In the **Reporting Parameter** area, click the down arrow in the **From** box, and then click **Yesterday**.

    Note
    You can further specify the timeframe for the report in the additional options in the Reporting Parameter area.
11. In the **Reporting Parameter** area, under **Monitoring Object**, click **Add**.
12. In the **Add Object** dialog box, in the **Object Name** list, click the down arrow and then click **Begins with**.
13. In the **Object name** text box, type the computer name for the computer you selected in step 5, and then click **Search**.
14. In the **Available items** list, click the computer with the **Type** of **Health Service**, click **Add**, and then click **OK**.
15. In the **Reporting Parameter** area, in the **Monitoring Object** list, click the entry that is not of the type **Health Service**, and then click **Remove**.
16. Click **Run** to display the **Configuration Changes Report**.
17. Click **Close** to close the report.

How to Create an Event Analysis Report

Use the following procedure to create an event analysis report.

To create an event analysis report

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Monitoring**.
3. In the **Monitoring** workspace, expand **Monitoring**, and then click **Windows Computers**.
4. In the **Windows Computers** pane, click a row containing a Health Service instance.
5. In the **Tasks** pane, under **Report Tasks**, click **Event Analysis**.
6. In the **Reporting Parameter** area, click the down arrow in the **From** box, and then click **Yesterday**.

   Note
   You can further specify the timeframe for the report in the additional options in the Reporting Parameter area.
7. In the **Reporting Parameter** area, under **Monitoring Object**, click **Add**.
8. In the **Add Object** dialog box, in the **Object Name** list, click the down arrow, and then click **Begins with**.
9. In the **Object name** text box, type the computer name for the computer you selected in step 4, and then click **Search**.
10. In the **Available items** list, click the computer with the **Type** of **Health Service**, click **Add**, and then click **OK**.
11. In the **Reporting Parameter** area, in the **Monitoring Object** list, click the entry that is not of the type **Health Service**, and then click **Remove**.
12. Click **Run** to display the **Event Analysis Report**.
13. Click **Close** to close the report.

How to Create an Operational Data Report

The Microsoft Customer Experience Improvement Program (CEIP) collects information about how you use Microsoft programs and about some of the issues you might encounter. Microsoft uses this information to improve the products and features you use most often and to help solve issues. Participation in the program is strictly voluntary.

During setup of Operations Manager Reporting, on the **Operational Data Reports** page, you had the option to join CEIP. If you elected to join CEIP, Operations Manager Reporting collects information about your installation and sends reports to Microsoft on a weekly basis. You can view the contents of these Operational Data Reports by creating a Microsoft ODR Report.

To create a Microsoft ODR Report

1. Log on to the computer with an account that is a member of the Operations Manager Report Operators role.
2. In the Operations console, click **Reporting**.

3. In the **Reporting** workspace, expand **Reporting**, and then click **Microsoft ODR Report Library**.
4. In the **Reports** pane, right-click one of the reports (for example, **Management Packs**), and then click **Open**.
5. In the **Report** view, in the **Parameter** area, click the down arrow in the **From** box, point to **This week**, and then click **Sunday**.
6. Click the down arrow in the **To** box, point to **This week**, and then click **Saturday**.
7. Click **Run** to display the ODR Report.
8. Click **Close** to close the report.

How to Save a Report

When you run a report, you can save the report to **Favorite Reports** or you can save a report into an existing management pack. A report saved to **Favorite Reports** is only visible to you. Saving a report to a management pack is useful if you need to share with report users a report that uses a specific set of parameters.

The following steps outline the procedure for saving a report to a management pack:

1. Run a report (from the generic report library or from a management pack, such as the SQL Server management pack). Specify the parameters you want to for the report and click **Run**.
2. When the report renders, validate that it contains the information you need.
3. On the **File** menu, click **Save to management pack**.
4. Follow the instructions in the wizard to save the report.

After the wizard completes, the management pack is saved to Operations Manager and then later deployed to the report server and is made available for all report operators.

Note

Be aware of the following when saving reports:

- Reports can be saved to a management pack from **Favorite Reports**.
- Reports cannot be saved to a management pack from authored reports.

  Management packs can be exported and imported into other management groups and the reports will work only when these management groups share the same data warehouse.

  Only users with administrator authorization can save reports to management packs.

See Also

Using Reports in Operations Manager

How to Create Reports in Operations Manager

Operations Manager Reports Library
How to Run a Report
Scheduling Reports
Operations Manager Reports Library
How to Troubleshoot Reports that Return No Data

How to Run a Report

Use the following procedure to run a report from the Reporting workspace. In this example, you will run an availability report.

To run a report from the Reporting pane

1. Log on to the computer with an account that is a member of the Operations Manager Report Operators role.
2. In the Operations console, click **Reporting**.
3. In the **Reporting** workspace, expand **Reporting** and then click **Microsoft Generic Report Library**.
4. In the **Reports** pane, right-click one of the reports (for example, **Availability**) and then click **Open**.
5. In the **Report** view, in the **Parameter** area, click the down arrow in the **From** box, point to **This week**, and then click **Sunday**.
6. Click the down arrow in the **To** box, point to **This week** and then click **Saturday**.
7. Click **Use business hours**.

   Note
   You can further specify the timeframe for the report in the additional options in the **Parameter** area.
8. Click **Add Object**.
9. In the **Add Object** dialog box, in the **Object Name** text box, type the computer name for a computer that you want to report availability, and then click **Search**.
10. In the **Available items** list, click the computer you want to run a report for, click **Add**, and then click **OK**.
11. Click **Run** to display the Availability Report.
12. For a more detailed report, such as a report showing a graph for every day, click the horizontal bar graph under **Availability Tracker**.
13. In the toolbar, click **View**, point to **Go To**, and then click **Back to Parent Report** to return to the original report.
14. Click **Close** to close the report.

See Also

Using Reports in Operations Manager

How to Create Reports in Operations Manager

How to Save a Report

Operations Manager Reports Library

Scheduling Reports

Operations Manager Reports Library

How to Troubleshoot Reports that Return No Data

Scheduling Reports

System Center 2012 – Operations Manager enables you to schedule report delivery for reports that you have created and saved. Scheduled reports can be sent by email to specified individuals and groups. Scheduled reports can also be delivered to the cache in the SQL Server Report Server and thereby shorten the time required to retrieve a report.

Scheduling Reports topics

- How to Create a Report Schedule
- How to Email Scheduled Reports
- How to Schedule the Delivery of a Report to the SQL Report Server Cache
- How to Cancel a Scheduled Report
- How to Edit a Scheduled Report

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Getting Information from Operations Manager
- Using Reports in Operations Manager
- Operations Manager Reports Library
- How to Create Reports in Operations Manager
- How to Save a Report
- How to Run a Report
- How to Export a Report
- How to Troubleshoot Reports that Return No Data

How to Create a Report Schedule

Use the following procedure to create a schedule to save a report. Make sure that you have created an Availability report and saved it as a favorite before using this procedure. For more information about creating an Availability report, see How to Create an Availability Report and for more information about saving a report as a favorite, see How to Save a Report.

To create a report schedule

1. Log on to the computer with an account that is a member of the Operations Manager Report Operators role.
2. In the Operations console, click **Reporting**.
3. In the **Reporting** workspace, click **Favorite Reports**.
4. In the **Favorite Reports** pane, right-click the Availability report you saved as a favorite, and then click **Schedule**.
5. In the **Subscribe to a Report Wizard**, on the **Delivery Settings** page, do the following:
   a. Type a description in the **Description** text box.
   b. Click the down arrow in the **Delivery method** list, and then click **Report Server File Share**.

      Note
      If you want to manage and distribute reports securely, you could deliver reports to Microsoft Windows SharePoint Services, which offers digital rights management. Consult your network security administrator.

   c. Type a file name for the report in the **File name** text box.
   d. Type a file path for the report in the **Path** text box.

      Note
      Report scheduling supports Universal Naming Convention (UNC) file names and must not end in a backslash.

   e. Click the down arrow in the **Render Format** list, and then click the file format you want for the report.
   f. Type a user name in the **User name** text box, and then type a password in the **Password** text box.

      Note
      The credentials must have Write user rights on the file share.

   g. Click the down arrow in the **Write mode** list, select the Write mode you want for subsequent files, and then click **Next**.
6. In the **Subscribe to a Report Wizard**, on the **Subscription Schedule** page, do the following:
   a. Select one of the **Generate the report** options.
   b. Type a start date and start time for the reports to be generated in **The Subscription**

is effective beginning list. You can also enter the date when this subscription will end in **The subscription expires on** list, and then click **Next**.

7. In the **Subscribe to a Report Wizard**, on the **Parameters** page, specify a span of time for the report in the **From** and **To** lists.
8. Make any other changes you need for this report, and then click **Finish**.

See Also

Scheduling Reports

How to Edit a Scheduled Report

How to Email Scheduled Reports

How to Schedule the Delivery of a Report to the SQL Report Server Cache

How to Cancel a Scheduled Report

How to Email Scheduled Reports

Before you can schedule a report for email delivery, you must configure the email settings in the Report Server using the Reporting Server Configuration Manager.

The example in this procedure uses an availability report that you have already created and saved as a favorite. For more information about creating an availability report, see How to Create an Availability Report. For more information about saving a report as a favorite, see How to Save a Report.

To configure email settings in the SQL Server Report Server

1. On the Windows desktop, click **Start**, point to **Programs**, point to **Microsoft SQL Server 2008**, point to **Configuration Tools**, and then click **Reporting Services Configuration**.
2. In **Reporting Services Configuration Manager**, in the **Report Server Installation Instance Selection** dialog box, click **Connect**.
3. In the navigation pane, click **E-mail Settings**.
4. In the **E-mail Settings** pane, enter the following:
   - An email address for use as the sender address in the **Sender Address** text box.
   - The address of the SMTP server that will be used to send the email messages in the **SMTP Server** text box.
5. Click **Apply**, and then click **Exit**.

To email scheduled reports

1. Log on to the computer with an account that is a member of the Operations Manager Report Operators role.

2. In the Operations console, click **Reporting**.
3. In the **Reporting** workspace, click **Favorite Reports**.
4. In the **Favorite Reports** pane, right-click the Availability report you saved as a favorite, and then click **Schedule**.
5. In the Subscribe to a Report Wizard, on the **Delivery Settings** page, do the following:
   - Type a description in the **Description** text box.
   - Click the down arrow in the **Delivery method** list, and then click **Report Server E-Mail**.
   - Type an email address of the destination inbox to receive reports in the **To** text box. You can also type email addresses in the **Cc**, **Bcc**, and the **Reply To** text boxes.
   - Click the down arrow in the **Render Format** list, and then click the file format you want for the report.
   - Click the down arrow in the **Priority** list, and then select the appropriate priority.
   - Type a subject for the email in the **Subject** text box.
   - Click **Next**.
6. On the **Subscription Schedule** page, do the following:
   - Select one of the **Generate the report** options.
   - Type a start date and start time for the reports to be generated in **The Subscription is effective beginning** list. You can also enter the date when this subscription will end in **The subscription expires on** list, and then click **Next**.
7. On the **Parameters** page, specify a span of time for the report in the **From** and **To** lists, make any other changes you need for this report, and then click **Finish**.

See Also

Scheduling Reports

How to Create a Report Schedule

How to Edit a Scheduled Report

How to Schedule the Delivery of a Report to the SQL Report Server Cache

How to Cancel a Scheduled Report

How to Schedule the Delivery of a Report to the SQL Report Server Cache

You can create a schedule for sending reports to the cache in the SQL Server Report Server and thereby shorten the time required to retrieve a report if the report is large or accessed frequently. For more information about report caching, see Caching Reports (SSRS).

The example in this procedure uses an availability report that you have already created and saved as a favorite. For more information about creating an availability report, see How to Create

an Availability Report. For more information about saving a report as a favorite, see How to Save a Report.

To schedule the delivery of a report to the SQL Report Server Cache

1. Log on to the computer with an account that is a member of the Operations Manager Report Operators role.
2. In the Operations console, click **Reporting**.
3. In the **Reporting** workspace, click **Favorite Reports**.
4. In the **Favorite Reports** pane, right-click the availability report you saved as a favorite, and then click **Schedule**.
5. In the **Subscribe to a Report Wizard**, on the **Delivery Settings** page, do the following:
   a. Type a description in the **Description** text box.
   b. Click the down arrow in the **Delivery method** list, and then click **Null Delivery Provider**.
   c. Click **Next**.
6. On the **Subscription Schedule** page, do the following:
   a. Select one of the **Generate the report** options.
   b. Type a start date and start time for the reports to be generated in **The Subscription is effective beginning** list. You can also enter the date when this subscription will end in **The subscription will end** list, and then click **Next**.
7. On the **Parameters** page, specify a span of time for the report in the **From** and **To** lists, make any other changes you need for this report, and then click **Finish**.

See Also

Scheduling Reports

How to Create a Report Schedule

How to Email Scheduled Reports

How to Edit a Scheduled Report

How to Cancel a Scheduled Report

How to Cancel a Scheduled Report

Use the following procedure to cancel scheduled reports.

To cancel a scheduled report

1. Log on to the computer with an account that is a member of the Operations Manager Report Operators role.
2. In the Operations console, click **Reporting**.

3. In the **Reporting** workspace, click **Scheduled Reports**.
4. In the **Scheduled Reports** pane, right-click the scheduled report you want to cancel, and then click **Cancel Schedule**.
5. In the **System Center Operations Manager** dialog box, click **OK** to confirm the deletion of your schedule or click **No** to keep your schedule.

See Also

Scheduling Reports

How to Create a Report Schedule

How to Email Scheduled Reports

How to Schedule the Delivery of a Report to the SQL Report Server Cache

How to Edit a Scheduled Report

How to Edit a Scheduled Report

Use the following procedure to edit settings for scheduled reports from the **Reporting** pane in System Center 2012 – Operations Manager.

To edit a scheduled report

1. Log on to the computer with an account that is a member of the Operations Manager Report Operators role.
2. In the Operations console, click **Reporting**.
3. In the **Reporting** workspace, click **Scheduled Reports**.
4. In the **Scheduled Reports** pane, right-click the scheduled report you want to edit, and then click **Edit Schedule**.
5. In the **Subscribe to a Report Wizard**, on the **Delivery Settings** page, if you select the **Windows File Share** as a **Delivery method**, you must type the password in the **Password** text box before you can make any other changes.
6. Type any other changes you need on the **Delivery Settings** page, and then click **Next**.
7. Type any changes you need to make on the **Subscription Schedule** page, and then click **Next**.
8. Type any changes you need to make on the **Report Parameters** page, and then click **Finish.**

See Also

Scheduling Reports

How to Create a Report Schedule

How to Email Scheduled Reports

How to Schedule the Delivery of a Report to the SQL Report Server Cache

How to Cancel a Scheduled Report

How to Export a Report

After a report has been created, you can export the report into one of several formats.

Note

Operations Manager Reporting must be installed before you can run a report.

If you want to manage and distribute reports securely, you can export reports to Microsoft Windows SharePoint Services, which offers digital rights management. Consult your network security administrator.

To export a report

1. After a report has been run, in the toolbar, click the **File** menu, point to **Export**, and then click the format you want to export the file to.
2. In the **Save As** dialog box, select the folder where you want to save the report, and then click **Save**.

See Also

Using Reports in Operations Manager

How to Create Reports in Operations Manager

How to Save a Report

How to Run a Report

Scheduling Reports

Operations Manager Reports Library

How to Troubleshoot Reports that Return No Data

How to Troubleshoot Reports that Return No Data

When running a Performance Report or Configuration Data Report, data might not be displayed. Use the following procedures to evaluate if any data has been collected for the report and how to find the proper parameters to use for the report. For this example, it is assumed that the Windows Server 2003 Operating System Management Pack has been imported.

Ensure that all appropriate overrides in a particular management pack have been enabled. For example, the Windows Server Operating System Management Pack does not discover physical disk partitions, only logical disk partitions.

If you want to monitor physical disk drives, you can do so by enabling the Object Discovery feature for the Windows Server 2003 physical disk or Windows 2000 Server physical disk objects. Additionally, the Microsoft Windows Server 2003 Operating System Management Pack can monitor individual instances of processors or all instances of processors together. By default, the health of the processors will be monitored as a total of all instances. If you want to monitor individual processor instances, you can do so by enabling the Object Discoveries for Windows Server 2003 Processor objects. See the appropriate management pack guide for more information about any override that you might need to enable. The two examples listed are from the Windows Server Operating System Management Pack.

After any applicable overrides have been enabled, you would use the following two procedures. In the first procedure, you will troubleshoot an instance when no data is displayed in a performance data report by using My Workspace to see if the required data has been collected in the Operations Manager database.

In the second procedure, you will troubleshoot an instance when no data is displayed in a configuration data report. In this example, it is assumed that the Operating System Configuration report returns no data.

To troubleshoot no data in a performance report

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click **Reporting**.
3. In the Reporting workspace, expand **Reporting**, and then click **Windows Server 2003 Operating System**.
4. In the Windows Server 2003 Operating System Reports pane, click **Disk Performance Analysis**.
5. In the Report Details pane, a list of the performance counters available in this report is displayed. Keep in mind one of the counters, for example, **LogicalDisk\Disk Bytes/sec_Total**.
6. In the Operations console, click **My Workspace**.
7. In My Workspace, right-click **My Workspace**, point to **New**, and then click **Performance View**.
8. In the **Properties** dialog box, in the **Name** field, type a name for this view (for this example use **Test**).
9. In the **Criteria** tab, click **with a specific counter name**.
10. In **Criteria description** field, click **specific**.
11. In the **Counter Name** dialog box, type the name of the counter you noted in step 5, for example **Disk Bytes/sec**, and then click **OK**.
12. In the **Properties** dialog box, click **OK**.

13. In the Test results pane, in **Legend** area, click one or more of the **Show** check boxes.
    - If data appears in the **Test** pane, that data is available in the Operations Manager database and should be available for the report.
    - If no data appears, click the **Authoring** button. In Authoring, expand **Authoring**, expand **Management Pack Objects**, and then click **Rules**. Look in the **Enabled by default** column for any rules that are not enabled. If they are not enabled, use overrides to enable the rule that you need for your report.

    Note
    Some performance data collection rules in the Exchange Management Packs store data in only the Reporting data warehouse and cannot be verified with this procedure.
14. In the **Legend** area, examine the **Target** column and verify that the text in the **Target** column matches what is listed in the **Object** column in the Parameter Area of the report. If the value listed in the **Target** column is different, use the value listed in **Target** column in the report and run the report again.

    Note
    When searching for the name of an object in a report, you might find that the name of the hosting computer is listed only in the **Object path** column in the Parameter Area. If you want to locate multiple specific objects, you can create a dynamic group containing the correct types of objects and run the report with this new group. For more information about creating groups, see **How to Create Groups in Operations Manager**.

To troubleshoot no data in a configuration data report

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click **My Workspace**.
3. In My Workspace, right-click **My Workspace**, point to **New**, and then click **State View**.
4. In the **Properties** dialog box, in the **Name** field, type a name for this view (for this example use **Test1**).
5. On the **Criteria** tab, click the ellipses (**…**) next to the **Show data related to** box.
6. In the **Select a Target Type** dialog box, click **View all Targets**.
7. In the **Find** box, type **Windows Operating System**.
8. In the **Target** column, click **Windows Operating System**, and then click **OK**.
9. In the **Properties** dialog box, examine the contents in the list with the check boxes contain the data that you wanted to run a report against (for example, Build Number), and then click **OK**.
10. In the Test1 results pane, examine the content in the **Name** column. The values listed in the **Name** column are the correct object names you need to search for when searching for objects for the report.

Note

When searching for the name of an object in a report, you might find that the name of the hosting computer is listed only in the **Object path** in the Parameter Area. In this instance, you need to create a dynamic group containing the correct types of objects and run the report with this new group. For more information about creating groups, see **How to Create Groups in Operations Manager**.

See Also

Using Reports in Operations Manager

How to Create Reports in Operations Manager

How to Save a Report

How to Run a Report

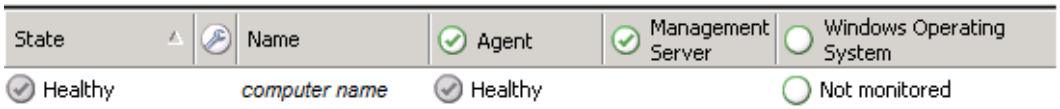
Scheduling Reports

How to Export a Report

Operations Manager Reports Library

Not Monitored and Gray Agents

In System Center 2012 – Operations Manager, you may see discovered objects in the Operations console displayed as not monitored or gray, as shown in the following illustration.



The state view in the previous illustration contrasts two “unknown” states.

- The agent is shown as healthy, but the indicator is gray.
- The operating system is shown as not monitored.

The gray icon indicates that the health service watcher on the management server that is watching the health service on the monitored computer is not receiving heartbeats from the agent anymore. The health service watcher had received heartbeats previously and the state was reported as healthy. This also means that the management servers are no longer receiving any information from the agent.

The not monitored icon indicates that there are no monitors for the object. In the previous illustration, the view tells you that there are no monitors for the operating system on this computer. In this case, this is because the management packs for the Windows Server operating systems have not been imported in this management group.

What to do for a gray state

Some of the common reasons for a gray state are:

- Heartbeat failure
- Health service is not running
- Incorrect configuration
- System workflows failure
- Operational or data warehouse database performance
- Management server or gateway server performance
- Network or authentication issues

The **Show Gray Agent Connectivity Data** task will help you identify why an agent is gray.

To check a gray agent for connectivity

1. Open the Operations console and click **Monitoring**.
2. Navigate to the Operations Manager\Agent Details\Agent Health State view.
3. In **Agent State from Health Service Watcher**, click the agent you want to check connectivity for.
4. In the **Tasks** pane, select the task **Show Gray Agent Connectivity Data**.
5. The **Run Task – Show Gray Agent Connectivity Data** dialog box appears. Click **Run**.
6. The Task Status dialog box appears. When the task is completed, you can click **Copy Text** or **Copy HTML** and paste the task output in the appropriate tool for further review.

   The task output will identify the following information:

   - The last time a heartbeat was received from the agent.
   - Whether the System Center Management Health service is running on the agent.
   - Whether the agent responds to ping.
   - The last time the configuration on the agent was updated.
   - Possible reasons that the agent is unavailable.
   - The management server that the agent reports to.

For information on troubleshooting, see the Knowledge Base article Troubleshooting gray agent state. Although the article was written for Operations Manager 2007, the troubleshooting steps will also be helpful for System Center 2012 – Operations Manager.

What to do for a not monitored state

When an object shows as not monitored, check whether the appropriate management pack for monitoring the object is imported. Ensure that the appropriate monitors are enabled.

Sometimes restarting the System Center Management Health service on the agent-managed computer can resolve the issue. You can also try placing the object in maintenance mode for several minutes. For more information, see How to Suspend Monitoring Temporarily by Using Maintenance Mode.

Next, check the DNS configuration for the computer, both FQDN and DNS suffix.

An agent can also show as not monitored because the new agent has the same NetBIOS name as a previously installed agent. When the agent is deleted from Operations Manager, the grooming of the deleted agent is occurs after two days. Therefore, the agent is not immediately groomed out of the database completely. To work around this limitation, wait three days after deleting the agent to install the new agent.

For more ideas for troubleshooting, see the blog post Getting headaches trying to figure out why you are seeing the 'Not Monitored' state for Management Servers or Agents?.

See Also

Using the Operations Manager Consoles

Finding Data and Objects in the Operations Manager Consoles

Using Views in Operations Manager

Using SharePoint to View Operations Manager Data

Subscribing to Alert Notifications

Using Reports in Operations Manager

How to View All Rules and Monitors Running on an Agent-Managed Computer

Administrators for System Center 2012 – Operations Manager sometimes want to know which rules and monitors are running on a computer. This is simple to do with the **Show Running Rules and Monitors for this Health Service** task.

To view all rules and monitors running on a computer

1. Open the Operations console and click **Monitoring**.
2. For an agent-managed computer, navigate to the Operations Manager\Agent Details\Agent Health State view. For a management server, navigate to Operations Manager\Management Server\Management Servers State view.
3. Click the agent you want to see rules and monitors for.
4. In the **Tasks** pane, select the task **Show Running Rules and Monitors for this Health Service**.
5. The **Run Task – Show Running Rules and Monitors for this Health Service** dialog box appears. Click **Run**.
6. The Task Status dialog box appears. When the task is completed, you can click **Copy Text** or **Copy HTML** and paste the task output in the appropriate tool for further review.

See Also

How Heartbeats Work in Operations Manager

Resolving Heartbeat Alerts

Viewing Active Alerts

Viewing Alert Details

Examining Properties of Alerts, Rules, and Monitors

Impact of Closing an Alert

How to Close an Alert Generated by a Monitor

How to Reset Health

Identifying the Computer Experiencing a Problem

Using Health Explorer to Investigate Problems

Using Event View to Investigate Problems

Investigating Alert Storms

How an Alert is Produced

How to Set Alert Resolution States

How to Configure Automatic Alert Resolution

Diagnostic and Recovery Tasks

Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

Using the Visio 2010 Add-in and SharePoint 2010 Visio Services Data Provider

The Visio 2010 Add-in for System Center 2012 – Operations Manager combines the strengths of two applications widely used in enterprise IT to simplify the creation of customized dashboards that show the health of an environment. The Visio Add-in lets you create diagrams that show objects by geography on a map, by location in a data center or building, by role in a logical view of an application, or by topology for complex distributed applications such as Microsoft Exchange Server or technologies such as Active Directory Domain Services.

The SharePoint 2010 Visio Services Data Provider for System Center 2012 – Operations Manager enables you to take the customized dashboards you create with the Visio 2010 Add-in and include them in SharePoint 2010 Web sites. These Web-based dashboards are updated and provide access to instant status information through the familiar SharePoint browser-based experience.

The Visio 2010 Add-in and SharePoint 2010 Visio Services Data Provider have the following features:

- Distributed applications exported from Operations Manager as Visio documents automatically show live health state information on the exported objects when opened in Microsoft Office Visio.
- You can easily create new Visio documents and link shapes to any managed object (such as a computer, database, Web site, or perspective) to show the current health state.
- You can automatically link entire existing Visio documents to the computer and to network devices managed by Operations Manager by matching computer names or IP addresses.
- Health states can be automatically refreshed in Visio documents. You can use this option along with Visio's full-screen view to create dashboard views suitable for use as a summary display in a data center control room.
- Predefined data graphics enable you to switch from Operations Manager health icons to the shape color for health state.
- Health states can be automatically refreshed in published Visio documents that are hosted in SharePoint 2010 document libraries, when the Visio Services data provider for System Center 2012 – Operations Manager is installed and configured on the SharePoint 2010 server farm.

The following topics provide information about how to install, configure, and use the Visio Add-in and the SharePoint 2010 Visio Services Data Provider.

- Install the Visio 2010 Add-in
- Install the Visio Services Data Provider
- Grant Visio Services with Read-Only Operator Permissions
- Configure the Operations Manager Data Source in Visio 2010
- View an Operations Manager Distributed Application Diagram in Visio 2010
- Add Links to Operations Manager to a New or Existing Visio 2010 Document
- Build a simple monitoring dashboard using the Visio Web Part
- Publish a Visio diagram to SharePoint 2010
- Change the Way Health State is Represented in Visio 2010
- Troubleshooting the Visio 2010 Add-in

Install the Visio 2010 Add-in

The Visio 2010 Add-in for System Center 2012 – Operations Manager has the following prerequisites:

- System Center 2012 – Operations Manager Operations or Authoring console.

  You can download the Authoring console from the Microsoft Download Center (http://go.microsoft.com/fwlink/?LinkID=136356).
- Microsoft Office Visio 2010 Professional or Premium.
- The Microsoft .NET Framework 3.5 SP1 (http://go.microsoft.com/fwlink/?LinkID=131605).

When you run the Setup program for the Visio Add-in, your system is checked against these requirements. If your system does not meet the requirements, a link is provided so that you can download the missing software.

Note
If you have previously installed the Vision 2007 version of the Add-in on this computer, uninstall it before installing the Visio 2010 Add-in.

Note
If you previously installed the Visio Add-in with System Center Operations Manager 2007 R2, and upgraded to System Center 2012 – Operations Manager, you must uninstall it prior to installing the System Center 2012 – Operations Manager version.

To install the Visio 2010 Add-in

1. In Windows Explorer, navigate to the directory where you downloaded the Add-in and then double-click **OpsMgrAddinSetup.msi**. This is the installation file for the client.
2. Click **Next** on the Welcome page of the installation wizard.
3. Read the license agreement, select **I Agree**, and then click **Next**.
4. Specify the installation location, and then click **Next**.
5. Click **Next** to start the installation.
6. Click **Close** when the installation is complete.

The next time you start Visio, you are asked if you want to install the Visio Add-in. Click **Install**. When the installation is complete, the Operations Manager command is available in the Visio ribbon.

Install the Visio Services Data Provider

The Visio Services Data Provider for System Center 2012 – Operations Manager leverages SharePoint 2010's Visio Services to enable Visio diagrams to show live health state from Operations Manager in SharePoint.

The Visio Services Data Provider for System Center 2012 – Operations Manager has the following prerequisites:

- System Center 2012 – Operations Manager, Operations or Authoring console
- SharePoint 2010 Enterprise
- The Microsoft .NET Framework 3.5 SP1

Note
You must install SharePoint Server 2010 in a farm environment versus standalone (on a single server with a built-in database by using the default settings) so that Visio Services can be configured to run as a domain account with Operations Manager access. For

more information about installing SharePoint Server 2010 on a single server farm, see Deploy a single server with SQL Server (SharePoint Server 2010). For more information about installing SharePoint Server 2010 on a multiple server farm, see Multiple servers for a three-tier farm (SharePoint Server 2010).

To install the Visio Services data provider

1. In Windows Explorer, navigate to the directory where you downloaded the Add-in and then double-click **the OpsMgrDataModuleSetup.msi**.
2. Read the license agreement, select **I Agree**, and then click **Next**.
3. Specify the installation location, and then click **Next**.

   By default, files are extracted to the C:\Program Files\ directory. You can change this to any location.

   Note
   The .msi program does not install or deploy the data provider to the SharePoint servers in the server farm. This program simply extracts the SharePoint deployment package to a location specified by the SharePoint administrator.
4. Open the SharePoint 2010 Management Shell as an administrator.
5. Run the following command:

   ```
   .\InstallOpsMgrDataModule.ps1
   ```

   Note
   The SharePoint 2010 Administration service must be running prior to running `.\InstallOpsMgrDataModule.ps1`

   The `InstallOpsMgrDataModule` cmdlet installs the deployment package to the solution store for the server farm and then deploys the data module to each of the SharePoint servers in the server farm.
6. After the cmdlet has completed, you can verify that the package was successfully deployed by running the `get-spsolution` cmdlet. You should see “True” in the Deployed column next to the opsmgrdatamodule.wsp entry.
7. Start SharePoint Central Administration to verify that the data provider is listed as a Trusted Data Provider for Visio Services.

Grant Visio Services with Read-Only Operator Permissions

In order for Visio Services to refresh the diagrams that are published and connected to Operations Manager data, the Visio Services service application must be configured with credentials that have access to the management server. This is because the Visio Services

service application is executing the data provider that is responsible for returning the updated dataset from the management server.

The easiest way to configure this is to make the account that Visio Services is running as a Read-Only Operator on the management server.

If you need to determine the account that is configured for Visio Services, use SharePoint's Central Administration:

1. Open the Central Administration site.
2. In the **Security** section, click **Configure Service Accounts**.
3. In the list of Service Accounts, select Service Application Pool – SharePoint Web Services Default.

   The account is listed in the **Select an account for this component** field.

To grant the Visio Services account Read-Only Operator access to the management server

1. In the Operations console, open the Administration view.
2. In the Administration pane, expand **Administration**, expand **Security**, and then click **User Roles**.
3. In the User Roles pane, right-click **Read-Only Operator**, and then click **Properties**.
4. In the **Operations Manager Read-Only Operators – User Role Properties** dialog box, on the **General Properties** page, click **Add**.
5. On the **Select User or Groups** page, enter the account that is configured for Service Application Pool, and then click **OK**.
6. Click **Apply**, and then click **OK** to close the **Operations Manager Read-Only Operators -User Role Properties** dialog box.

Configure the Operations Manager Data Source in Visio 2010

Before Visio 2010 can interact with System Center 2012 – Operations Manager, you need to configure Operations Manager as a data source for your Visio document. You also need to configure the Operations Manager web console address to enable opening the Health Explorer or Alert view directly from Visio. You need to configure these items for each Visio document you create.

Note

This latest version of the Visio 2010 Add-in also functions with Operations Manager 2007 R2. If installing this version with Operations Manager 2007 R2, ensure that credentials and access are configured to communicate with the root management server (RMS).

To configure the Operations Manager data source and web console address in Visio

1. Open a new drawing in Visio.
2. Click **Operations Manager** in the ribbon, and then click **Configure**.
3. In the **Name** field, type the name of the management server.
4. In the **Address** field, type the address for the web console. This is the console that is used to launch the Health Explorer and Alert view from Visio.

   If you do not know the address, and you have Operations Manager administrator privileges, click **Look up web console address**. If you do not know the address, and you are not an Operations Manager administrator, contact the administrator for the address, and then type it in the **Address** field.
5. If you want to receive regular updates of state information from the management server, select **Automatically refresh data**, and then specify a refresh interval in seconds.
6. Click **OK**.

View an Operations Manager Distributed Application Diagram in Visio 2010

When you export a distributed application from the System Center 2012 – Operations Manager Operations console and then open it in Microsoft Visio 2010 with the Visio Add-in for System Center 2012 – Operations Manager, the diagram in the Visio document contains information about the health state of each object. This information is provided through a connection to Operations Manager.

To view a distributed application as a Visio diagram

1. In the Operations console, open your diagram.
2. On the toolbar, click the **To Visio** icon.
3. Open the folder in which you want to save the diagram, type a file name, and then click **Save**.
4. In Visio, open the exported diagram.

   Visio automatically contacts the management server.
5. If you are prompted, type the user credentials for the management server, and then click **OK**.

   When the diagram opens, the External Data window appears in the lower pane of Visio. This window contains detailed information about the objects in the diagram, including the health state and the last time the object state was refreshed in the diagram.

   You can drill into the status of any object by opening the Health Explorer in the

Operations Manager web console. To do this, right click the object and select **Health Explorer**. To see the alerts associated with this object, you can open the alerts view from within the Health Explorer. Before you can do this, make sure you have configured the address for the web console. See Configure the Operations Manager Data Source in Visio 2010 for more information.

Now that you have the initial diagram in Visio, you can customize it by adding new shapes. You can add links to Operations Manager components by dragging an object from the External Data window to an image or drawing in the diagram. The data is automatically linked to the image.

You can also change the way that the health state data is displayed on an object. Select the object, and then click a data graphic on the right side of Visio.

Add Links to Operations Manager to a New or Existing Visio 2010 Document

The Visio 2010 Add-in for System Center 2012 – Operations Manager lets you create a new Microsoft Office Visio document that you can link to Operations Manager objects. The Visio Add-in also lets you add live health state information to an existing Visio document.

To do this, you first specify the Operations Manager management server from which the Visio Add-in will get information about the managed objects and their health state. Then, you add the links by using one of the following methods:

- Link a single shape to a managed object. You can quickly link a few shapes to any object managed by Operations Manager.
- Add multiple links to the document and then associate these to Visio shapes later. This option works best for large documents that have many different types of managed object.
- Automatically link shapes in the document to computers and to network devices. This option uses a single wizard to automatically add health state information to large and complex network or topology diagrams.
- Insert a new shape that is linked to an Operations Manager object and that uses the Operations Manager icons.

Note

This latest version of the Visio 2010 Add-in also functions with Operations Manager 2007 R2. If installing this version with Operations Manager 2007 R2, ensure that credentials and access are configured to the RMS instead of the management server.

To link a single Visio shape to an object managed by Operations Manager

1. Click **Operations Manager** in the ribbon, and then click **Link Shape**.
2. Select the Operations Manager class of the object, such as **Windows Computer**, to

display a filtered list of available Operations Manager objects.

3. Select the object that you want to link to this shape, and then click **Link**.

The shape in the diagram now includes a state indicator in the upper-right corner of the image.

To add multiple links to objects managed by Operations Manager

1. Click **Operations Manager** in the ribbon, and then click **Add Data Links**.
2. Select the class for the shape, and then click **OK**.
3. Select the managed objects you want to link to this shape, and then click **Insert**.

   This adds the selected managed objects to the dataset in the Visio diagram, which can be viewed in the External Data window.
4. In the External Data window, select the object that you want to connect to a shape in the diagram or image.

   For example, if you want to add the management server for a geographic location to a map, select the management server.
5. Drag the object to the diagram or image and drop it onto the shape. This establishes the link between the shape and that managed object's record.

To automatically link multiple Visio shapes to Operations Manager managed computers and network devices

1. Open the Visio document.

   Ensure that each shape has defined shape data, such as the network name or IP address, or shape text (such as the IP address of the object).

   To view the shape data, right-click the shape, click **Data**, and then click **Shape Data**. This opens the Shape Data window for the selected shape.
2. Select all the shapes in the document.
3. Click **Operations Manager** in the ribbon, and then click **Reconcile Shapes**.
4. In the Automatically Link wizard, select **Selected shapes** or **All shapes in the document**, and then click **Next**.
5. Match the Visio shape property to the Operations Manager property. For example, match the Visio network name to the Operations Manager display name. The following Operations Manager classes are matched automatically:
   - Windows Computer (Microsoft.Windows.Computer)
   - Unix Computer (Microsoft.Unix.Computer)
   - SNMP Network Device (Microsoft.SystemCenter.NetworkDevice)

   Click **Next**.
6. Review the list of matches. Click to clear any objects you do not want to link, and then click **Next**.

   If more than one match is found, click **Select** to choose the object you want to link to. If no matches are found, click **Browse** to search for the object.

7. Review the list of links to define, and then click **Finish**.

The shapes are automatically connected to the managed objects they represent on the management server.

To insert a shape that is linked to an Operations Manager object

1. In your Visio diagram, click **Operations Manager** in the ribbon, and then click **Insert shape**.
2. Select the class of the object you want to insert. This filters the available objects to only those of the specified class. You can also search for a specific object.
3. Select the specific object, and then click **Insert**.

The new shape is added to the diagram. The shape icon matches those of other Operations Manager objects of the same class, and the shape data is populated with information from the management server.

Build a simple monitoring dashboard using the Visio Web Part

SharePoint 2010 Enterprise edition includes a Web part for Visio Services called the Visio Web Access Web Part. You can add this Web part to any SharePoint Web part page to build a dashboard that uses published Visio diagrams to provide visualizations.

To build a monitoring dashboard for your Visio diagram

1. In Internet Explorer, navigate to your SharePoint 2010 site.
2. Navigate to the Shared Documents document library.
3. Click **Site Actions** (above the ribbon), and then click **More Options**.
4. Select the Web Part page and click **Create**.
5. Type a name for the new page.
6. Under **Layout**, select **Header, Right Column, Body** from the list of available layout templates.
7. Click **Create** to create the new Web page.
8. Click the Body zone. You should see a new **Insert** tab on the ribbon.
9. On the **Insert** tab, click **Web Part**.
10. In the **Categories** list, click **Office Client Applications**, and then, in the **Web Parts** list, click **Visio Web Access**.
11. Click **Add**.

    The Visio Web Access Web Part is added to the Body zone of the Web part page.
12. Edit the properties of the Visio Web Access Web Part. In the **Web Part** toolbar, click **Edit**

Web Part.

13. Set the **Web Drawing URL** property. Click Browse and navigate to the document library where you published a Visio diagram. Select the published diagram and click **OK**.
14. Set the **Automatic Refresh** property to 1 minute (the minimum value supported). This enables the dashboard to automatically refresh the diagram with new data from the management server every 1 minute.
15. Clear the **Show Open in Visio** option in the Toolbar and User Interface section.
16. Click **OK** to apply the changes.

    You should now see the rendered Visio diagram in the browser.
17. Click **Stop Editing** to exit edit mode.

Your Web part should now display with the published diagram in the Visio Web Access Web part. Notice that the **Open in Visio** button (normally available by default) is no longer available in the Web part toolbar.

Publish a Visio diagram to SharePoint 2010

With the Visio 2010 Add-in installed on the client and the data provider installed on the SharePoint server, you can now publish diagrams that you have connected to Operations Manager data to a SharePoint document library to share them with others in your organization.

To publish a diagram to a SharePoint document library

1. From the **File** tab on the Visio 2010 ribbon, click **Save & Send**.
2. Click **Save to SharePoint**.
3. Click **Browse for a location** to specify where to save the diagram.
4. Under **File Types**, choose **Web Drawing (*.vdw)**.

   If you do not choose this option, the drawing will not be visible through a browser, only the client.
5. Click **Save As**.
6. Specify the name and location for the file. To browse to a SharePoint server, type the name of the SharePoint server in the address field and click **Go To**.
7. Click **Save**.

When the diagram is saved to a document library, you can simply browse to the document library in your browser and click the link to the document. The Visio diagram will open in your browser. With the data provider installed, the data will be refreshed directly from the management server.

Change the Way Health State is Represented in Visio 2010

By default, health state is depicted by using the System Center 2012 – Operations Manager health icons (such as the green check mark for a healthy state). You can customize the way that health state is shown by changing the data graphic associated with the object. For example, you can show the health state by filling the shape with red, yellow, green, or grey color to represent the three health states and to represent a managed object in maintenance mode.

To change the way that health state is represented

1. Select the shape or shapes that you want to change.
2. On the Data tab, click **Data Graphics**.
3. In the Data Graphics window, click the data graphic that you want to use. The Visio Add-in for System Center 2012 – Operations Manager includes two choices. The **SCOM IconSet** data graphic shows health state using icons as in Operations Manager. The **SCOM Color by Value** data graphic uses red, yellow, green, or grey color to represent the three health states and to represent a managed object in maintenance mode.

Troubleshooting the Visio 2010 Add-in

The following sections provide information about troubleshooting the Visio 2010 Add-in:

- Enabling trace logging on the data provider
- Known issues

Enable Trace Logging for the Server Data Module

Use the following steps to enable trace logging for the server data module installed on the SharePoint server.

1. Open the Microsoft.Office.Visio.Server.OperationsManager.dll configuration file in a text editor (such as Notepad).
2. Change the location for log files. Look for the following:

```
<configuration>
   <appSettings>
      <add key=”EnableLog” value=”True” />
      <add key=”LogPath” value=\\server\directory” />
   <appSettings>
</configuration>
```

For the LogPath parameter, change the value to the location where you want to save log files generated by the data provider.

3. Copy the configuration file to the directory on the GAC where the data module assembly is located.

The next time a diagram is refreshed, the configuration file is checked and log files are written to the location you specific.

Each refresh option is recorded in a separate log file. The name of the file reflects the user who attempted the refresh and the date and time the refresh was attempted (for example, “jdoe_3_25_2010_12-23-37_PM.log”). The log file contains the following:

- The name of the user that requested the refresh
- The date and time of the refresh
- The version of the assembly installed on the server
- The command string that was configured in the diagram before publishing to the server
- Details about the dataset to be refreshed, including table count, row count, and IDs for each row
- Any error conditions or exceptions that occur within the data module for each session

For successful refresh attempts, the log file also contains the XML version of the dataset returned to Visio Services for diagram refresh purposes.

Known issues with the Visio 2010 Add-in

You might see the following issues when you use the Visio Add-in for System Center 2012 – Operations Manager.

The font size of inserted shapes might appear too small

When you insert a new graphic by using the **Insert Shape** option, the font size for the shape text might appear too small. The size is determined by the default font size set for a template.

You can change the font size by selecting the shape and then choosing a different font size in the Visio toolbar.

Hyperlinks on sub-shapes are not available

Health Explorer and Alert View hyperlinks might not be available in Edit mode or Full Screen mode if you have grouped your shapes or added links to any shapes that were already contained within groups.

You receive a ConfigurationErrorsException error message

You might see the following error message:

```
System.Configuration.ConfigurationErrorsException: Configuration system failed to
initialize --->
```

```
System.Configuration.ConfigurationErrorsException: Unrecognized configuration section
userSettings.
   (C:\Documents and Settings\asttest\Local Settings\Application
Data\Microsoft_Corporation

\OpsMgrAddin.vsto_vstoloca_Path_logwdvddmizljsrbc2bvt5gtm5juzdix\12.0.6325.5000\user.conf
ig
   line 3)
.
.
.
```

To work around this problem, delete the configuration file identified at the top of the error message. For example, delete the following file:

\OpsMgrAddin.vsto_vstoloca_Path_logwdvddmizljsrbc2bvt5gtm5juzdix\12.0.6325.5000\user.config

You receive a MissingMethodException error message

You might see the following error message:

```
System.MissingMethodException: Method not found: 'System.Security.SecureString
System.Windows.Controls.PasswordBox.get_SecurePassword()'.
   at Microsoft.EnterpriseManagement.VisioAddin.EnterCredentials.get_Password()
   at
Microsoft.EnterpriseManagement.VisioAddin.SCOMHelpers.EnterCredentials(ManagementGroupCon
nectionSettings& connectSettings)
   at Microsoft.EnterpriseManagement.VisioAddin.Document.ConnectToManagementGroup()
   at Microsoft.EnterpriseManagement.VisioAddin.Document.AddDataLinkToShape()
```

To resolve this problem, install Microsoft .NET Framework 3.5 SP1, available from http://go.microsoft.com/fwlink/?LinkID=131605.

The state graphic is not displayed

The state graphic does not appear on a stencil even though you have linked the shape with the **Link Shape to Data** option.

Some stencils in Visio are not defined with a wrapping group. To resolve this problem, create a group for the shape, and then use the **Link Shape to Data** option again. To create a group, right-click the shape, and then click **Shape** and **Group**.

You see security warnings when you open a diagram

When you open a document that you previously linked to Operations Manager, you receive multiple security warnings.

This problem occurs because the status of the document components is set to refresh automatically. To suppress the warnings, select **Don't show this message again**.

You cannot re-install the Visio Add-in

If you delete the Operations Manager Add-in by using the Visio Trust Center, you cannot add it again later.

This behavior occurs by design in Visio. Before you can add the Operations Manager Add-in again, uninstall it by using Add/Remove Programs (or Programs and Features) in the Control Panel, and then reinstall it.

General Tasks in Operations Manager

General Tasks in Operations Manager topics

- Managing Alerts
- How to Suspend Monitoring Temporarily by Using Maintenance Mode
- Creating and Managing Groups
- Running Tasks in Operations Manager
- How to Create a Resource Pool
- Connecting Management Groups in Operations Manager
- Using Operations Manager Shell

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Initial Monitoring After Operations Manager Is Installed
- Managing Access in Operations Manager
- Operations Manager Monitoring Scenarios
- Getting Information from Operations Manager
- Maintenance of Operations Manager
- Operations Manager Report Authoring Guide

Managing Alerts

An alert is an indication of a significant event requiring attention. Rules and monitors can generate alerts. You can view alerts in the **Monitoring** workspace of the Operations console or web console.

Managing Alerts topics

- How Heartbeats Work in Operations Manager
- Resolving Heartbeat Alerts
- How an Alert is Produced
- Viewing Active Alerts
- Viewing Alert Details
- Examining Properties of Alerts, Rules, and Monitors
- Impact of Closing an Alert
- How to Close an Alert Generated by a Monitor
- How to Reset Health
- Identifying the Computer Experiencing a Problem
- Using Health Explorer to Investigate Problems
- Using Event View to Investigate Problems
- Investigating Alert Storms
- How to Set Alert Resolution States
- How to Configure Automatic Alert Resolution
- Diagnostic and Recovery Tasks

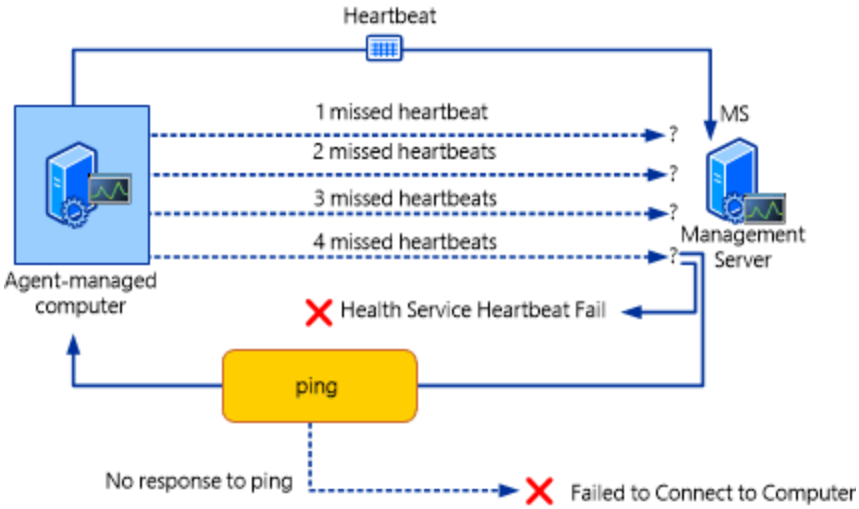
Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Subscribing to Alert Notifications
- General Tasks in Operations Manager
- How to Suspend Monitoring Temporarily by Using Maintenance Mode
- Creating and Managing Groups
- Running Tasks in Operations Manager
- How to Create a Resource Pool
- Connecting Management Groups in Operations Manager
- Operations Manager Report Authoring Guide

How Heartbeats Work in Operations Manager

System Center 2012 – Operations Manager uses *heartbeats* to monitor communication channels between an agent and the agent's primary management server. A heartbeat is a packet of data sent from the agent to the management server on a regular basis, by default every 60 seconds, using port 5723 (UDP).

When an agent fails to send a heartbeat 4 times, a **Health Service Heartbeat Failure** alert is generated and the management server attempts to contact the computer by using ping. If the computer does not respond to the ping, a **Failed to Connect to Computer** alert is generated. The following illustration shows this process.



When you see both alerts, you know the computer cannot be contacted by the management server. When you see only the heartbeat failure alert, you know the computer can be contacted but there is a problem with the agent. Both alerts are closed automatically when heartbeats resume.

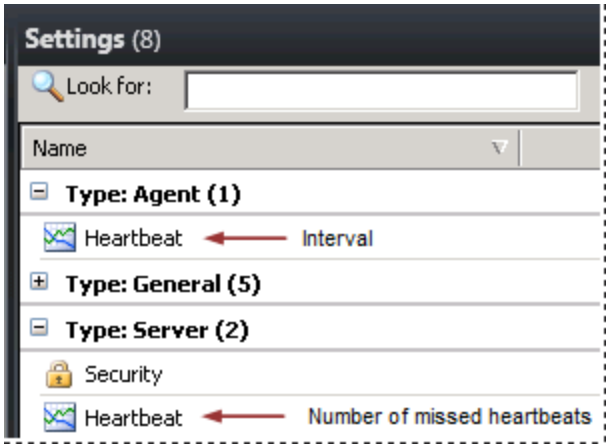
Note

By default, alerts for missed heartbeats and response to ping are disabled for client operating systems. To receive alerts for client operating systems, override the **Health Service Heartbeat Failure** and **Computer Not Reachable** monitors for the class **Windows Client Operating System** to set the **Generates Alert** parameter to **True**.

The health state for the agent-managed computer will change to critical (red) when the **Health Service Heartbeat Failure** alert is generated. To view details for the health state, right-click the computer in **Active Alerts**, point to **Open**, and click **Health Explorer**. The Availability node will

be expanded to display the critical item. Click **Health Service Heartbeat Failure**, and then click the **State Change Events** tab. You will see a list of state changes with the date and time of occurrence. Select any occurrence to display information in the **Details** pane. The health state will change to healthy (green) when heartbeats resume.

You can change the heartbeat interval for all agents and number of missed heartbeats for all management servers in **Settings** in the **Administration** workspace, as shown in the following illustration.



You can also override the global heartbeat interval for individual agents and the number of missed heartbeats for individual management servers by opening the properties for the computer in **Agent Managed** or **Management Servers** in the **Administration** workspace. For example, you might increase the heartbeat interval for a computer that has a slow connection to the network.

See Also

Resolving Heartbeat Alerts

How an Alert is Produced

Viewing Active Alerts

Viewing Alert Details

Examining Properties of Alerts, Rules, and Monitors

Impact of Closing an Alert

How to Close an Alert Generated by a Monitor

How to Reset Health

Identifying the Computer Experiencing a Problem

Using Health Explorer to Investigate Problems

Using Event View to Investigate Problems

Investigating Alert Storms

How to View All Rules and Monitors Running on an Agent-Managed Computer

How to Set Alert Resolution States
How to Configure Automatic Alert Resolution
Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)
Diagnostic and Recovery Tasks

Resolving Heartbeat Alerts

The Health Service sends a heartbeat to a management server to verify that the system is still responding. When a specified number of heartbeats fail to arrive, System Center 2012 – Operations Manager displays an alert.

This section shows how to investigate a Health Service Heartbeat Failure alert as an example. Different alerts have different causes and different resolutions.

If you want to walk through these procedures, you can cause this alert by disabling the System Center Management service on a test system.

To cause a Health Service Heartbeat Failure alert for testing

1. On a computer with an agent installed, open Control Panel.
2. Double-click **Administrative Tools**.
3. Double-click **Services**.
4. Right-click the **System Center Management** service, and then click **Stop**.

   Note
   Use this same procedure and select **Start** in step 4 when you are done testing.

How to Investigate Agent Heartbeat Issues

The **Monitoring** workspace displays active alerts. Looking at an alert provides information and tools to investigate with.

To investigate an active alert

1. Open the Operations console.
2. Click **Monitoring**.
3. Click **Active Alerts** to view the **Health Service Heartbeat Alert**.

   Note
   Depending on the heartbeat interval and the number of missing heartbeats, a few minutes might be required to see the alert.
4. Click the alert to highlight it and read the information in the **Alert Details** area. The **Alert Details** area provides information about the alert, including a description and knowledge about the cause and resolution.

How to Troubleshoot Agent Heartbeat Issues

Use the tasks in the **Tasks** pane to diagnose the cause of the alert. Different alerts have different tasks. For a Health Service Heartbeat Failure alert, the tasks deal with pinging the system and verifying or restarting the service.

To use the action tasks in troubleshooting

1. In the **Tasks** pane, under **Health Service Watcher Tasks**, click **Ping Computer**. The task opens a dialog box to display its progress.

   Note
   If the ping fails, use standard networking troubleshooting to figure out the issue with connectivity. Verify that the system is turned on.
2. Click **Close** to close the dialog box.
3. Under **Health Service Watcher Tasks**, click **Computer Management**. A **Computer Management** dialog box for the target system opens.
4. Click **Services and Applications** to expand it.
5. Click **Services** to display services.
6. Right-click the **System Center Management** service, and then click **Start**.

   Note
   After the connection with the agent is restored, the alert will be automatically resolved and the computer status will return to healthy.

These steps will fix the test failure created in this topic, as well as address a number of possible causes of a Health Service Heartbeat Failure. If an actual failure is not resolved by these steps, use standard troubleshooting techniques to figure out the cause of the issue. For instance, the alert displayed in **Active Alerts** shows how old the alert is. Check for events that happened at this time to see what might have caused an issue.

A sudden increase in the number of alerts is called an alert storm. An alert storm can be a symptom of massive changes of some kind within your management group, such as catastrophic failure of networks. An alert storm can also be a symptom of configuration issues within Operations Manager. A newly imported management pack starts monitoring immediately. If you have a large number of managed computers, an unforeseen configuration issue could cause a large increase in alerts.

See Also

How Heartbeats Work in Operations Manager

How an Alert is Produced

Viewing Active Alerts

Viewing Alert Details

Examining Properties of Alerts, Rules, and Monitors

Impact of Closing an Alert
How to Close an Alert Generated by a Monitor
How to Reset Health
Identifying the Computer Experiencing a Problem
Using Health Explorer to Investigate Problems
Using Event View to Investigate Problems
Investigating Alert Storms
How to View All Rules and Monitors Running on an Agent-Managed Computer
How to Set Alert Resolution States
How to Configure Automatic Alert Resolution
Diagnostic and Recovery Tasks
Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

How an Alert is Produced

In System Center 2012 – Operations Manager, an alert can be generated by a rule or a monitor. (For an explanation of rules and monitors, see What Is in an Operations Manager Management Pack?.) Some rules and monitors are configured to send an alert when specific conditions are met, such as a certain event occurring or an operation failing. Every rule and monitor does not generate an alert. When the default configuration of a monitor is to not send alerts, you can configure an override on the monitor to enable alerts. (For information about configuring overrides, see How to Override a Rule or Monitor.)

A monitor can be configured to generate an alert when health state changes to warning (yellow) or critical (red), or only when state changes to critical. For example, a monitor for free disk space detects that disk space on a computer is below the configured threshold. The monitor changes the health state to critical and sends a single alert. After the monitor has sent the alert, it will not generate future alerts so long as the health state does not change from critical to healthy (green). If, however, the health state is reset to healthy and then the disk space drops below the threshold again, another alert will be sent when the health state changes to critical.

If a monitor sends an alert for warning or critical, and the monitor sent an alert when the state changed to warning, it will only send a second alert when the stage changes from warning to critical if the first alert has been closed. If the alert that was sent when the state changed to warning remains open, no alert will be sent when the state changes from warning to critical.

The following illustration shows the state changes that can generate an alert.

State changes that can generate an alert

From	To	Alert
		No
		Yes, if first alert is closed
		Yes, if first alert is closed
		No
		Yes
		Yes

Most alerts generated by monitors will be automatically resolved when the health state returns to healthy. If a monitor is not configured to automatically resolve its alert, you can configure an override on the parameter **Auto-Resolve Alert** for the monitor.

Note

Rules cannot automatically resolve alerts.

Unlike monitors, rules can continue to send alerts as long as the condition that caused the alert persists or repeats. Depending on what the rule is checking for, a single issue could possibly generate a huge number of alerts. To prevent the noise of too many alerts, alert suppression can be enabled for a rule.

Note

Alert suppression can only be enabled when the rule is created. You cannot enable alert suppression by using an override.

When alert suppression is enabled for a rule, only the first alert is sent and further alerts are suppressed. A suppressed alert is not displayed in the Operations console. Operations Manager suppresses only duplicate alerts as defined by the alert suppression criteria. Fields stated in the suppression criteria must be identical for the alert to be considered a duplicate and suppressed. An alert must be created by the same rule and be unresolved to be considered a duplicate.

You can personalize the **Active Alerts** view to add the **Repeat Count** column. The repeat count for an alert with suppression enabled will be incremented for each suppressed alert. You can also view the repeat count in the properties for an alert.

Important

By default, all alerts that are generated by monitors and that use the same instance ID are suppressed, however nothing in the alert properties as viewed in a console will

indicate that suppression is enabled. Alerts that are generated by rules will also be suppressed by default if the rule definition in the management pack contains an empty Suppression Value tag, however nothing in the alert properties as viewed in a console will indicate that suppression is enabled. You will only be aware of the suppression if you view the **Repeat Count** column for the alert.

See Also

How Heartbeats Work in Operations Manager

Resolving Heartbeat Alerts

Viewing Active Alerts

Viewing Alert Details

Examining Properties of Alerts, Rules, and Monitors

Impact of Closing an Alert

How to Close an Alert Generated by a Monitor

How to Reset Health

Identifying the Computer Experiencing a Problem

Using Health Explorer to Investigate Problems

Using Event View to Investigate Problems

Investigating Alert Storms

How to View All Rules and Monitors Running on an Agent-Managed Computer

How to Set Alert Resolution States

How to Configure Automatic Alert Resolution

Diagnostic and Recovery Tasks

Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

Viewing Active Alerts

To view active alerts, open the Operations console and click **Monitoring**. The Monitoring Overview displays a summary of health states and alerts:

To view the actual alerts, click **Active Alerts** in the navigation pane.

Tip: If you are using the web console, you can filter the view of alerts by severity:

The list of alerts in the Results pane includes the severity, source, maintenance mode status, name, resolution state, and when the alert was created:

Severity	Source		Name	Resolution State	Created
Critical	*computer name*		*Alert name*	New	5/29/2009 1:17:10 PM

The following folders in the Monitoring workspace include a standard Active Alerts view scoped to the objects for that folder.

- Data Warehouse
- Network Monitoring
- Operations Manager
- Operations Manager\Agent Details
- Operations Manager\APM Agent Details
- Management Server
- Notification
- UNIX/Linux Servers

- Web Application Availability Monitoring

See Also

How Heartbeats Work in Operations Manager

Resolving Heartbeat Alerts

How an Alert is Produced

Viewing Alert Details

Examining Properties of Alerts, Rules, and Monitors

Impact of Closing an Alert

How to Close an Alert Generated by a Monitor

How to Reset Health

Identifying the Computer Experiencing a Problem

Using Health Explorer to Investigate Problems

Using Event View to Investigate Problems

Investigating Alert Storms

How to View All Rules and Monitors Running on an Agent-Managed Computer

How to Set Alert Resolution States

How to Configure Automatic Alert Resolution

Diagnostic and Recovery Tasks

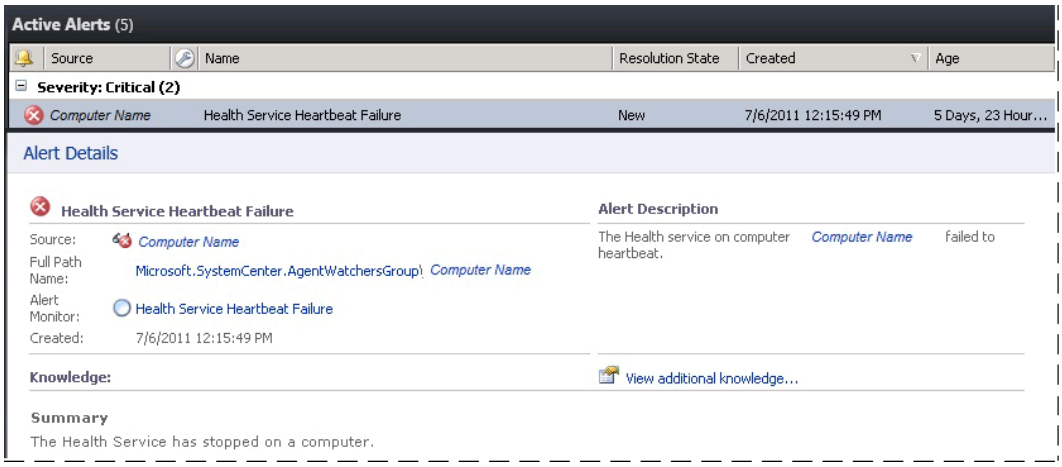
Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

Standard Views in Operations Manager

Viewing Alert Details

Alerts in System Center 2012 – Operations Manager include information to help you investigate and resolve the issues that caused the alerts.

To view the details for an alert, in the **Monitoring** workspace, click **Active Alerts**, and then click an alert in the results pane.



Tips

- Locate and investigate monitors in the **Warning** and **Error** states in the Health Explorer of the computer that was the source of the alert. (To open Health Explorer, right-click the alert, point to **Open**, and click **Health Explorer**.) If there are unhealthy monitors, they may correlate with the alert you are researching. Check out the **Context** pane of the **State Change Events** tab for possible additional clues to the root cause.
- Read all text in the alert properties. (Right-click the alert, and select **Properties**.) In particular, carefully review the **Alert Description** field on the **General** tab and the **Description** field on the **Alert Context** tab.
- Right-click the alert, and open the **Event** view. Sort the events by the **Level** column, and then locate the events with the **Error** and **Warning** event levels. Events may correlate with the alert you are investigating and provide insight to its resolution.

See Also

How Heartbeats Work in Operations Manager

Resolving Heartbeat Alerts

How an Alert is Produced

Viewing Active Alerts

Examining Properties of Alerts, Rules, and Monitors

Impact of Closing an Alert

How to Close an Alert Generated by a Monitor

How to Reset Health

Identifying the Computer Experiencing a Problem

Using Health Explorer to Investigate Problems

Using Event View to Investigate Problems

Investigating Alert Storms

How to View All Rules and Monitors Running on an Agent-Managed Computer

How to Set Alert Resolution States

How to Configure Automatic Alert Resolution

Diagnostic and Recovery Tasks

Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

Examining Properties of Alerts, Rules, and Monitors

The properties pages for alerts, rules, and monitors offer useful information and actions that you can take. The following tables explain what you can learn from properties for alerts, rules, and monitors and include tips on using the properties tabs.

Properties for Alerts

Tab	Description
General	The general tab contains key details about the alert, such as source (the monitored object on which the alert condition occurred), severity, priority, and repeat count (the number of times the alert condition has occurred). The alert description and status are also displayed on the general tab. You can assign an owner and ticket ID for an alert on the general tab. The rule or monitor that generated the alert is not displayed anywhere in the alert properties; for that information, see the alert details in the Operations console.
Product Knowledge	Product knowledge is information about the alert written by the author of the management pack that contains the alert. It should include information about the probable causes for the condition that caused the alert and guidance on resolving the condition.
Company Knowledge	Administrators can add knowledge to rules, monitors, and alerts to expand the troubleshooting information in the product knowledge to provide company-specific

Tab	Description
	information for operators.
History	You can add comments on the history tab that will be added to the alert history. This is useful for tracking actions related to the alert. Comments are limited to 85 characters. The alert history is specific to this occurrence of the alert, and is not contained in the same alert that is generated for another source or at another time. For notes that are useful for all occurrences of an alert, information should be added to the company knowledge tab.
Alert Context	Some alerts may display an alert context. The specific information provided in the alert context depends on the specific alert.
Custom Fields	Administrators can add information to any of the nine custom fields in an alert when an alert has been generated. The information added only applies to this unique alert. The custom fields can be searched on by using advanced search.

Properties for Rules

Tab	Description
General	The general tab provides the name and description of the rule, the management pack that it is contained in, the rule target, and whether the rule is enabled.
Configuration	The configuration tab provides information about the data source, condition, and responses configured for the rule. Unlike monitors which have alert configuration on an **Alerting** tab, alert configuration for a rule is on the **Configuration** tab, in **Responses**.
Product Knowledge	Product knowledge is information about the rule written by the author of the management pack

Tab	Description
	that contains the rule.
Company Knowledge	Administrators can add knowledge to rules, monitors, and alerts to expand the troubleshooting information in the product knowledge to provide company-specific information for operators.
Overrides	Administrators can apply overrides to the monitor on the overrides tab. Click **View summary** to view all overrides applied to the monitor.

Properties for Monitors

Tab	Description
General	The general tab provides the name and description of the monitor, the management pack that it is contained in, the parent monitor, and whether the monitor is enabled.
Health	The health tab tells you how health is defined for the monitor.
Alerting	The alerting tab provides information about an alert generated by the monitor. You can also see on thise tab whether alerts generated by this monitor are automatically resolved.
Diagnostic and Recovery	This tab lists any diagnostic or recovery tasks associated with this monitor. Administrators can add either type of task to the monitor on this tab.
Configuration	If there is a user interface for configuration of this monitor, it will be displayed on the configuration tab. If there is no user interface define, the XML that defines the configuration of this monitor is displayed.
Product Knowledge	Product knowledge is information about the monitor written by the author of the management pack that contains the monitor.

Tab	Description
Company Knowledge	Administrators can add knowledge to rules, monitors, and alerts to expand the troubleshooting information in the product knowledge to provide company-specific information for operators.
Overrides	Administrators can apply overrides to the monitor on the overrides tab. Click **View summary** to view all overrides applied to the monitor.

See Also

How Heartbeats Work in Operations Manager

Resolving Heartbeat Alerts

How an Alert is Produced

Viewing Active Alerts

Viewing Alert Details

Impact of Closing an Alert

How to Close an Alert Generated by a Monitor

How to Reset Health

Identifying the Computer Experiencing a Problem

Using Health Explorer to Investigate Problems

Using Event View to Investigate Problems

Investigating Alert Storms

How to View All Rules and Monitors Running on an Agent-Managed Computer

How to Set Alert Resolution States

How to Configure Automatic Alert Resolution

Diagnostic and Recovery Tasks

Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

Impact of Closing an Alert

In System Center 2012 – Operations Manager, an alert can be generated by a rule or a monitor. Alerts have two possible resolution states, by default: **New** and **Closed**. (Administrators can add

custom alert resolution states to a management group. For more information, see How to Set Alert Resolution States).

The impact of setting the alert resolution state to **Closed** depends on whether the alert was generated by a rule or a monitor. Click the alert to display the alert details. The details for an alert will either list **Alert Rule** or **Alert Monitor**.

If you close an alert that was generated by a rule and the issue continues or occurs again, another alert will be sent. Closing an alert that was generated by a rule when the issue is not fixed is not a problem, because the rule will generate another alert.

However, an alert that is generated by a monitor is sent only when the state for the monitor changes from healthy to some other state (warning or critical). If you close an alert that is generated by a monitor when the issue is not fixed, no other alerts will be sent.

For example, a monitor for free disk space detects that disk space on a computer is below the configured threshold. The monitor changes the health state to critical (red) and sends a single alert. After the monitor has sent the alert, it will not generate future alerts so long as the health state does not change from critical to healthy (green). If you close the alert while the object is in a warning or unhealthy state, the problem remains unresolved but no further alerts will be generated.

Generally, before you close an alert, you should verify that the issue is resolved. If the alert was generated by a monitor and the alert does not resolve automatically, check Health Explorer and the health state of the computer to ensure that the states have returned to healthy before you close the alert.

See Also

How Heartbeats Work in Operations Manager

Resolving Heartbeat Alerts

Viewing Active Alerts

Viewing Alert Details

Examining Properties of Alerts, Rules, and Monitors

How an Alert is Produced

How to Close an Alert Generated by a Monitor

How to Reset Health

Identifying the Computer Experiencing a Problem

Using Health Explorer to Investigate Problems

Using Event View to Investigate Problems

Investigating Alert Storms

How to View All Rules and Monitors Running on an Agent-Managed Computer

How to Set Alert Resolution States

How to Configure Automatic Alert Resolution

How to Close an Alert Generated by a Monitor

Monitors define the health states of objects. An object can have one of three health states: green (successful or healthy), yellow (warning), or red (critical or unhealthy). For example, a monitor for disk drive capacity might define green as less than 85 percent full, yellow as over 85 percent full, and red as over 90 percent full. A monitor can be configured to generate an alert when a state change occurs.

When you receive an alert, you can see in the alert details whether the alert was generated by a rule or a monitor. If the alert was generated by a monitor, as a best practice, you should allow the monitor to auto-resolve the alert when the health state returns to healthy. If you close the alert while the object is in a warning or unhealthy state, the problem remains unresolved but no further alerts will be generated.

If the monitor generates an alert when the health state changes to red and you do resolve the alert, you must also reset the health state for the monitor. If the monitor is not reset, the same condition that generated an alert can occur again but no alert will be generated because the health state has not changed.

To determine if an alert is resolved automatically

1. Select the alert, and then in the alert details, click the name of the alert monitor. The properties dialog box for the monitor opens.
2. In the monitor properties, click the **Alerting** tab to see if the option **Automatically resolve the alert when the monitor returns to a healthy state** is selected.

To close an alert that is generated by a monitor

1. Read the alert and examine its properties. Check the alert details to determine if the alert was generated by a monitor or a rule. Use the product knowledge for the alert to help determine the cause of the alert.
2. Troubleshoot the cause(s) of the alert and take the actions needed to resolve the problem.
3. When the problem is resolved, click **Source** in the alert details. This will open the **State** view for the object associated with the alert.
4. Right-click the object, point to **Open**, and then click **Health Explorer for** *object name*.
5. Select the monitor that generated the alert and click **Reset Health** on the toolbar. Close the Health Explorer and the **State** view.
6. Refresh the alerts view. If the alert is still listed, click the alert and then click **Close Alert**

in the Actions pane.

See Also

How Heartbeats Work in Operations Manager

Resolving Heartbeat Alerts

Viewing Active Alerts

Viewing Alert Details

Examining Properties of Alerts, Rules, and Monitors

Impact of Closing an Alert

How an Alert is Produced

How to Reset Health

Identifying the Computer Experiencing a Problem

Using Health Explorer to Investigate Problems

Using Event View to Investigate Problems

Investigating Alert Storms

How to View All Rules and Monitors Running on an Agent-Managed Computer

How to Set Alert Resolution States

How to Configure Automatic Alert Resolution

Diagnostic and Recovery Tasks

Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

How to Reset Health

Some monitors can set state to critical (red), warning (yellow), and healthy (green). Other monitors are only able to change state to critical or warning and cannot detect that state has returned to healthy. In that situation, the monitor must be reset manually. Administrators can check whether a monitor is type **Manual Reset** in the **Authoring** workspace.

Note
Only reset health for a monitor when you are sure that all issues have been resolved.

To reset health for a monitor

1. In the **Monitoring** workspace of the Operations console, right-click an alert, point to **Open**, and then click **Health Explorer**.
2. In **Health Explorer**, select a monitor, and on the toolbar, click **Reset Health**.

   Note
   You may also notice **Recalculate Health** on the toolbar. This function

reexamines the health state of a monitor or monitors; however, it only works with monitors that implement **On Demand Detection**. Most monitors do not implement **On Demand Detection**.

The following message displays: **Resetting the health of a monitor may take several minutes and will not be reflected in the Health Explorer immediately. The health state of some monitors cannot be reset and will not be updated as a result of this request. Do you wish to continue?**

3. If you are sure that you want to reset the monitor, click **Yes**.
4. Return to the Monitoring workspace, right-click the alert, point to **Set Resolution State**, and click **Closed**.

See Also

How Heartbeats Work in Operations Manager

Resolving Heartbeat Alerts

Viewing Active Alerts

Viewing Alert Details

Examining Properties of Alerts, Rules, and Monitors

Impact of Closing an Alert

How to Close an Alert Generated by a Monitor

How an Alert is Produced

Identifying the Computer Experiencing a Problem

Using Health Explorer to Investigate Problems

Using Event View to Investigate Problems

Investigating Alert Storms

How to View All Rules and Monitors Running on an Agent-Managed Computer

How to Set Alert Resolution States

How to Configure Automatic Alert Resolution

Diagnostic and Recovery Tasks

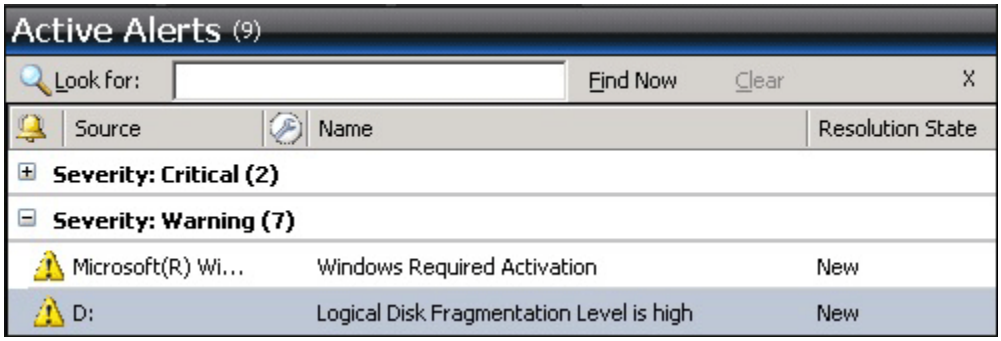
Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

Identifying the Computer Experiencing a Problem

This topic helps you answer questions such as “I see an alert that says logical disk defragmentation is high. Where is it high?”

To identify the computer experiencing a problem

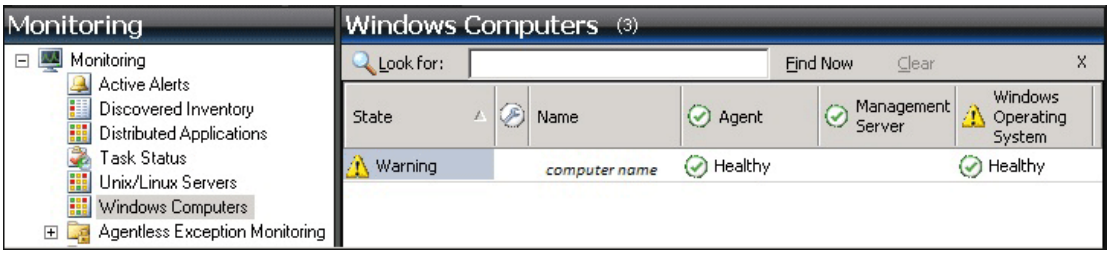
1. Click the alert.



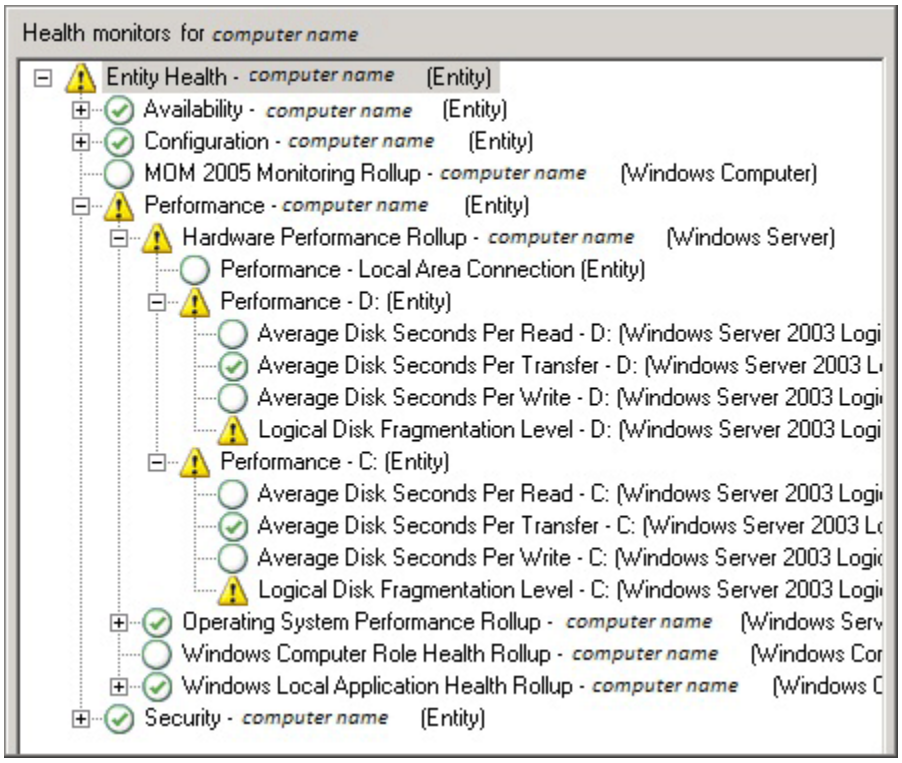
2. Look in the **Details** section for the **Path**.

Notice that this alert also includes the affected computer in the **Description**.

3. Click **Windows Computers** to view the state of the computer.



4. Right-click the computer, point to **Open**, and click **Health Explorer**:



In this illustration, you see that the logical disk fragmentation levels for C: and D: on this computer are in a warning state. Notice that the state rolls up to the **Performance** state for each disk, then to **Hardware Performance** for the computer, then to **Performance** for the computer, and finally to **Entity Health** for the computer.

See Also

[How Heartbeats Work in Operations Manager]

[Resolving Heartbeat Alerts]

[Viewing Active Alerts]

[Viewing Alert Details]

[Examining Properties of Alerts, Rules, and Monitors]

[Impact of Closing an Alert]

[How to Close an Alert Generated by a Monitor]

[How to Reset Health]

[How an Alert is Produced]

[Using Health Explorer to Investigate Problems]

[Using Event View to Investigate Problems]

[Investigating Alert Storms]

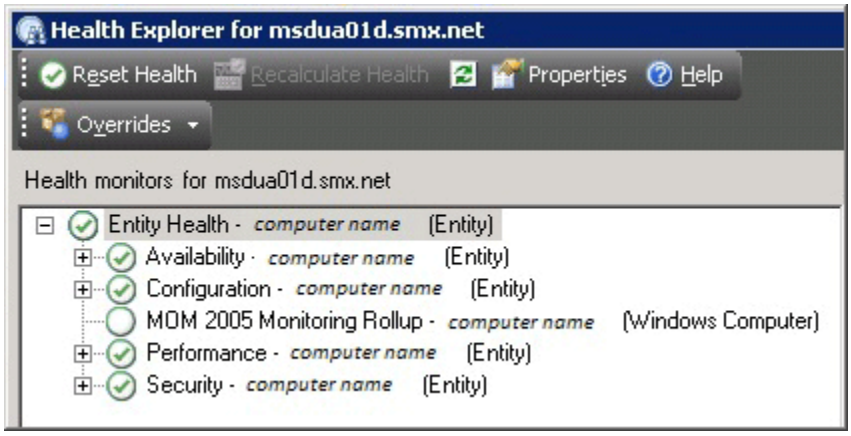
How to View All Rules and Monitors Running on an Agent-Managed Computer
How to Set Alert Resolution States
How to Configure Automatic Alert Resolution
Diagnostic and Recovery Tasks
Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

Using Health Explorer to Investigate Problems

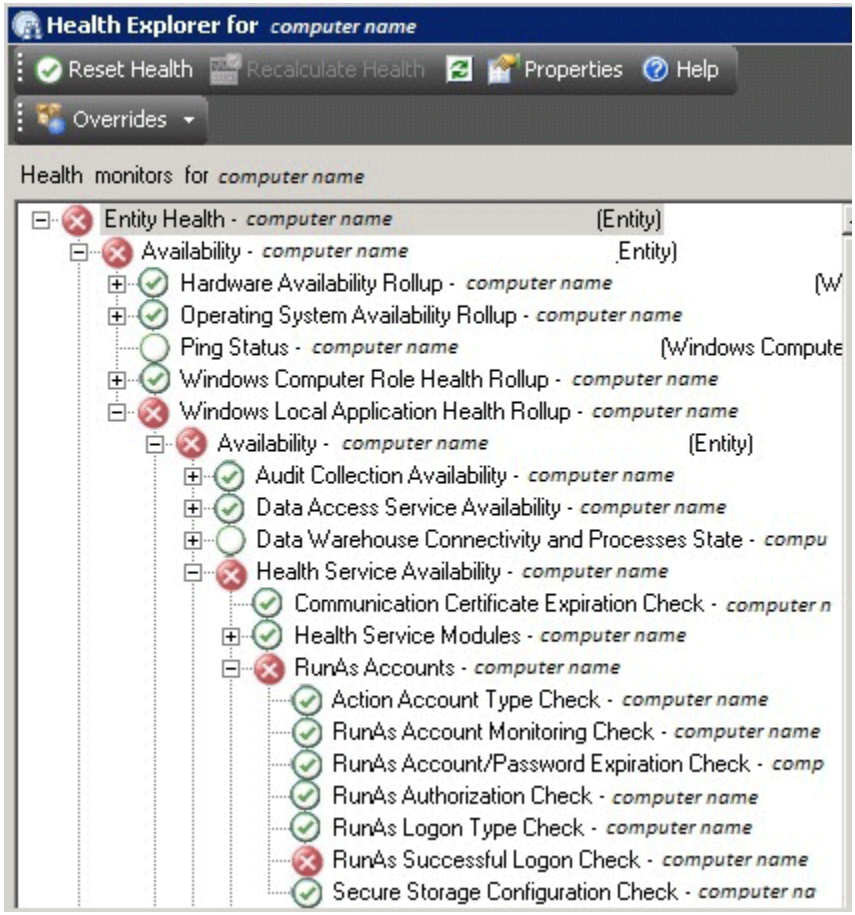
Use Health Explorer to find out which monitor is reacting and to review knowledge about the monitor and possible causes for actions related to it. In the **Active Alerts** view, click the alert to highlight it. The Health Explorer link under **Alert Actions** in the **Tasks** pane becomes active.

By default, when the Health Explorer window opens, all monitors in a failed state are expanded. If a monitor contains other monitors, as in the case of a roll-up monitor, Health Explorer shows all monitors in a hierarchical layout, displaying monitoring data for all dependent services and applications. To view more information about any dependent monitor, you can right-click that monitor, and then click **Monitor Properties** to open another Health Explorer window.

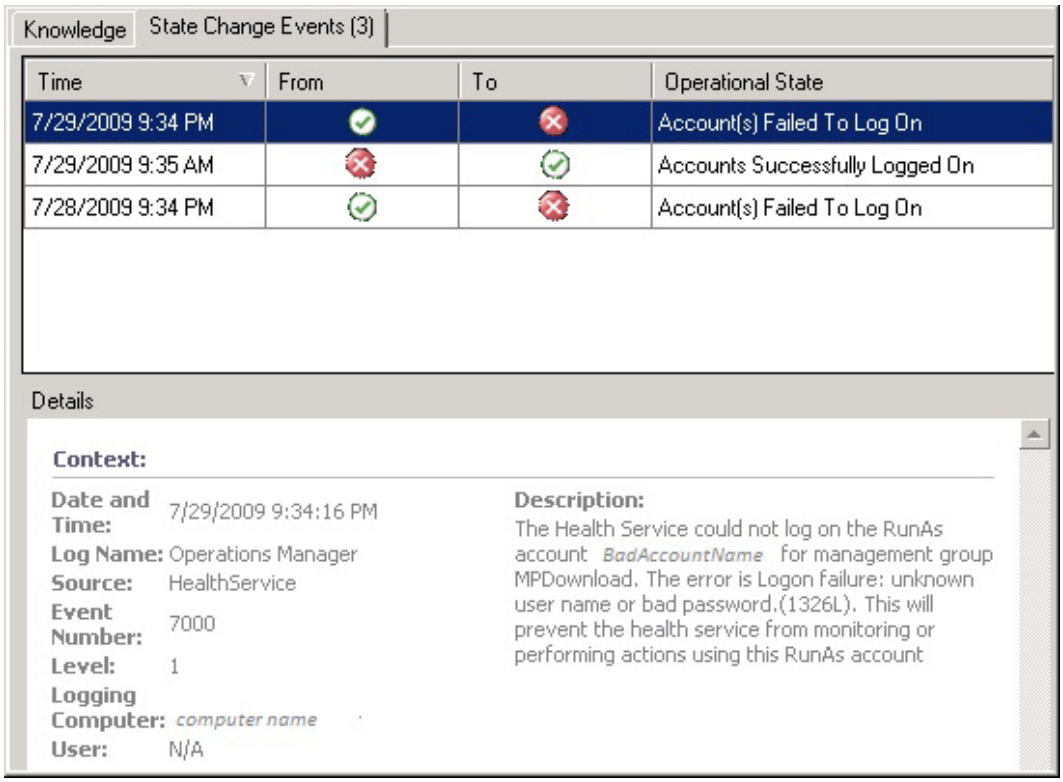
The following illustration shows monitors in a healthy state:



The following illustration shows some monitors in a critical state:



Click a monitor to view more information about the monitor in the **Details** pane. The **State Change Events** tab in the **Details** pane shows you when the state for the monitor changed, and the details give you information for the context of the state change:



See Also

[How Heartbeats Work in Operations Manager]

[Resolving Heartbeat Alerts]

[Viewing Active Alerts]

[Viewing Alert Details]

[Examining Properties of Alerts, Rules, and Monitors]

[Impact of Closing an Alert]

[How to Close an Alert Generated by a Monitor]

[How to Reset Health]

[Identifying the Computer Experiencing a Problem]

[How an Alert is Produced]

[Using Event View to Investigate Problems]

[Investigating Alert Storms]

[How to View All Rules and Monitors Running on an Agent-Managed Computer]

[How to Set Alert Resolution States]

[How to Configure Automatic Alert Resolution]

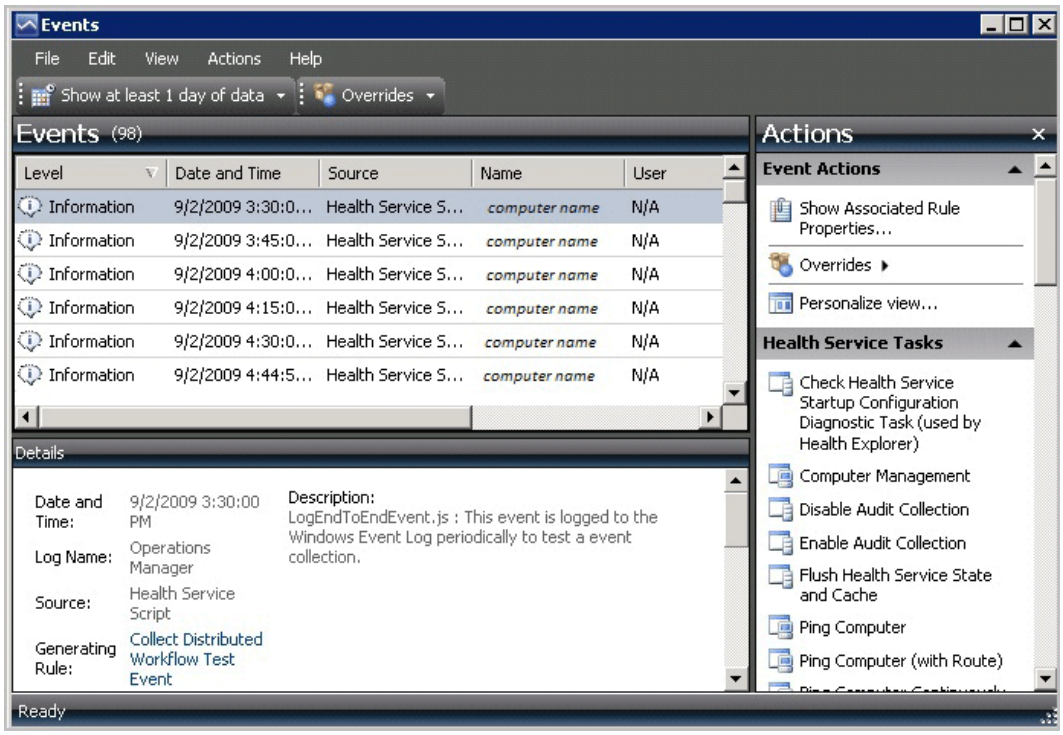
[Diagnostic and Recovery Tasks]

[Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)]
[Using Health Explorer in Operations Manager]

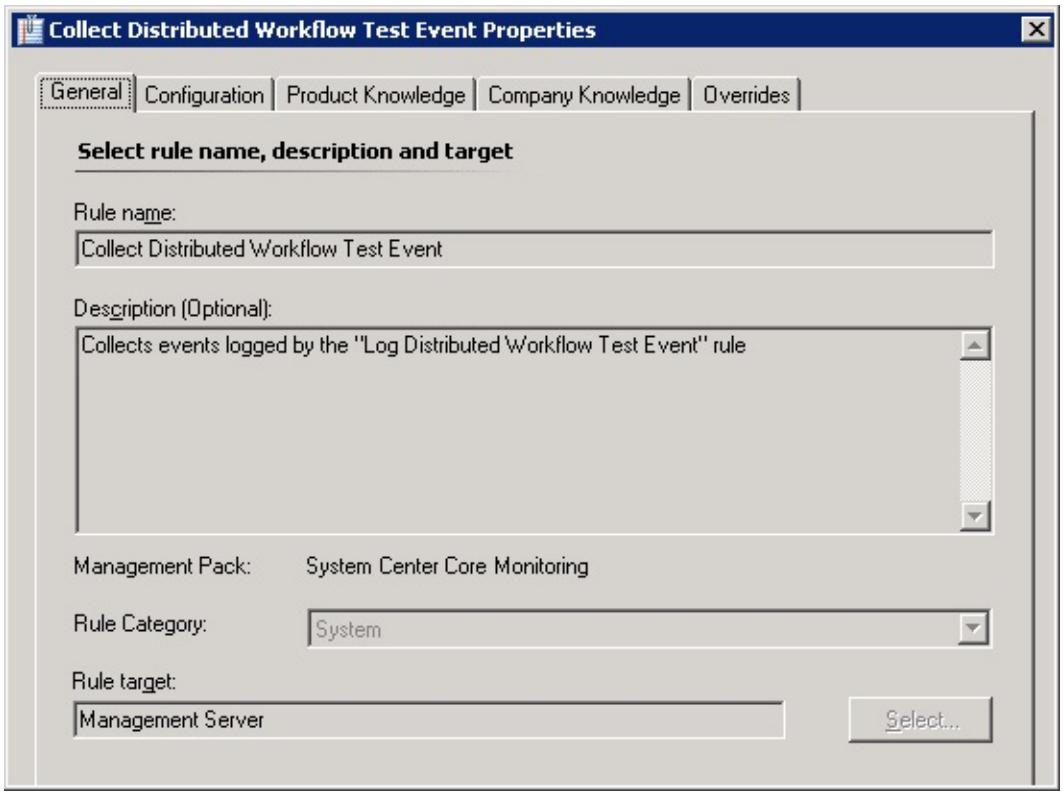
Using Event View to Investigate Problems

In System Center 2012 – Operations Manager, you can use an event view for an alert to help you investigate the problem that caused the alert.

Right-click an alert, point to **Open**, and click **Event View**. In the **Event View** window, you see information about the events associated with the alert.



In the **Details** pane, click **Generating Rule** to view information about the rule that generated the alert. The **General** tab shows you the name, description, and the source management pack of the rule.



See Also

[How Heartbeats Work in Operations Manager]

[Resolving Heartbeat Alerts]

[Viewing Active Alerts]

[Viewing Alert Details]

[Examining Properties of Alerts, Rules, and Monitors]

[Impact of Closing an Alert]

[How to Close an Alert Generated by a Monitor]

[How to Reset Health]

[Identifying the Computer Experiencing a Problem]

[Using Health Explorer to Investigate Problems]

[How an Alert is Produced]

[Investigating Alert Storms]

[How to View All Rules and Monitors Running on an Agent-Managed Computer]

[How to Set Alert Resolution States]

[How to Configure Automatic Alert Resolution]

Diagnostic and Recovery Tasks

Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

Investigating Alert Storms

A large and sudden increase in the number of alerts is called an alert storm. An alert storm can be a symptom of massive changes of some kind within your management group, such as the catastrophic failure of networks. An alert storm can also be a symptom of configuration issues within System Center 2012 – Operations Manager.

Installing new or updated management packs can give rise to an alert storm. Monitors in a management pack begin working as soon as the management pack has been imported. Use best practices in importing management packs to minimize alert storms.

Finding Alert Storms

For general, real-time monitoring of alerts, use the **Active Alerts** view. Make sure **Scope** is not active and hiding alerts. For more information, see How to Change Scope.

Check for large numbers of alerts when your network undergoes changes. Monitor closely when you install a new management pack.

Operations Manager offers reports that can be useful in identifying alert storms. From an Operations console with access to a reporting server, look at the **Microsoft Generic Report Library**. The reports **Most Common Alerts** and **Most Common Events** help identify high-volume alerts.

Modifying Monitors and Rules

If you are getting a large number of alerts that do not point to issues in your managed systems, you need to modify the monitors or rules that create those alerts.

View active alert details in the **Monitoring** workspace. **Alert Details** specifies the monitor or rule for an alert.

Modify the monitor using overrides. The procedure for overriding rules is the same as for monitors. See how your overrides affect the amount of alerts and continue to fine-tune the monitors as necessary. For more information, see Tuning Monitoring by Using Targeting and Overrides.

About Suppressed Alerts

Rules offer the option of suppressing duplicate alerts. A suppressed alert is not displayed in the Operations console. Each suppressed alert increments the repeat count for the alert that is displayed. You can examine the repeat count in the properties for an alert.

Operations Manager suppresses only duplicate alerts as defined by the alert suppression criteria. Fields stated in the suppression criteria must be identical for the alert to be considered a duplicate and suppressed. An alert must be created by the same rule and be unresolved to be considered a duplicate.

See Also

How Heartbeats Work in Operations Manager

Resolving Heartbeat Alerts

Viewing Active Alerts

Viewing Alert Details

Examining Properties of Alerts, Rules, and Monitors

Impact of Closing an Alert

How to Close an Alert Generated by a Monitor

How to Reset Health

Identifying the Computer Experiencing a Problem

Using Health Explorer to Investigate Problems

Using Event View to Investigate Problems

How an Alert is Produced

How to View All Rules and Monitors Running on an Agent-Managed Computer

How to Set Alert Resolution States

How to Configure Automatic Alert Resolution

Diagnostic and Recovery Tasks

Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

How to Set Alert Resolution States

In System Center 2012 – Operations Manager, there are two default resolution states for alerts: **New** and **Closed**.

When an alert is generated, its resolution state is **New**. Operators can change the resolution state for a new alert to Closed or to a custom resolution state that an administrator has created for the management group.

Custom alert resolution states can used any descriptor you want, such as “Assigned to support” or “Requires investigation”. The default resolution states cannot be changed or deleted.

Each resolution state is assigned an ID, a number which uniquely identifies that resolution state. The ID for **New** is 0 and the ID for **Closed** is 255. You can assign custom resolution states any value between 1 and 254.

To set the resolution state for an alert

1. In the Operations console, click **Monitoring**.
2. Click any view that displays alerts, such as **Active Alerts**.
3. Right-click an alert, point to **Set Resolution State**, and then click the desired resolution state.

To create an alert resolution state

1. In the Operations console, click **Administration**.
2. Click **Settings**.
3. Double-click **Alerts**.
4. On the **Alert Resolution States** tab, click **New**.
5. In **Add Alert Resolution State**, type a name for the resolution state and select a value in the **Unique ID** box, and then click **OK**.
6. In **Global Management Group Settings – Alerts**, click **OK**.

See Also

How Heartbeats Work in Operations Manager

Resolving Heartbeat Alerts

Viewing Active Alerts

Viewing Alert Details

Examining Properties of Alerts, Rules, and Monitors

Impact of Closing an Alert

How to Close an Alert Generated by a Monitor

How to Reset Health

Identifying the Computer Experiencing a Problem

Using Health Explorer to Investigate Problems

Using Event View to Investigate Problems

Investigating Alert Storms

How to View All Rules and Monitors Running on an Agent-Managed Computer

How an Alert is Produced

How to Configure Automatic Alert Resolution

Diagnostic and Recovery Tasks

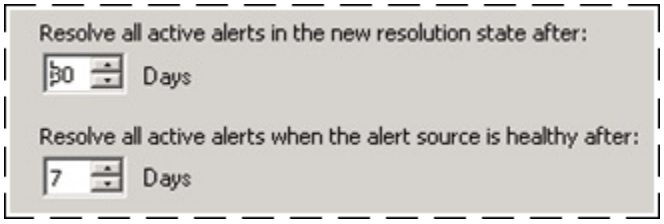
Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

How to Configure Automatic Alert Resolution

In System Center 2012 – Operations Manager, alerts are resolved automatically after a specific number of days. You can change the automatic alert resolution settings globally for the management group. Using automatic alert resolution, you can configure all active alerts with a resolution state of **New** to be changed to **Closed** after a specific number of days. You can also configure all active alerts with a resolution state of **New** to be changed to **Closed** after a specific number of days when the alert source is healthy.

To change the global settings for automatic alert resolution

1. In the Operations console, click **Administration**.
2. Click **Settings**.
3. Double-click **Alerts**.
4. Click the **Automatic Alert Resolution** tab.
5. Change the days for either or both of the following settings:



6. Click **OK**.

See Also

How Heartbeats Work in Operations Manager

Resolving Heartbeat Alerts

Viewing Active Alerts

Viewing Alert Details

Examining Properties of Alerts, Rules, and Monitors

Impact of Closing an Alert

How to Close an Alert Generated by a Monitor

How to Reset Health

Identifying the Computer Experiencing a Problem

Using Health Explorer to Investigate Problems

Using Event View to Investigate Problems

Investigating Alert Storms

How to View All Rules and Monitors Running on an Agent-Managed Computer

How to Set Alert Resolution States
How an Alert is Produced
Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)
Running Tasks in Operations Manager
Diagnostic and Recovery Tasks

Diagnostic and Recovery Tasks

Monitors in System Center 2012 – Operations Manager can do more than notify you of problems by sending an alert. Some monitors also provide diagnostic and recovery tasks to help investigate and resolve those problems.

A task is a script or other executable code that runs either on the computer running the Operations console or on the server, client, or device that is being managed. Tasks can potentially perform any kind of activity, including restarting a failed application and deleting files.

Monitors can have two kinds of tasks associated with them: diagnostic tasks that try to discover the cause of a problem or provide you with additional information to assist with that diagnosis, and recovery tasks that try to fix the problem.

Diagnostic and recovery tasks can run a script or command line executable. These tasks can be run automatically when the monitor enters an error state, providing an automated way to solve problems.

Diagnostic and recovery tasks can only be created for a specific monitor. A diagnostic or recovery task that you create for one monitor cannot be shared with or associated with a different monitor; you must recreate the task for each monitor. In addition, tasks that you create in the **Authoring** workspace using the **Create Task Wizard** cannot be used as a diagnostic or recovery for a monitor.

For example, the **Health Service Heartbeat Failure** monitor has several diagnostic and recovery tasks associated with it. The following list provides a sample of the tasks associated with the monitor.

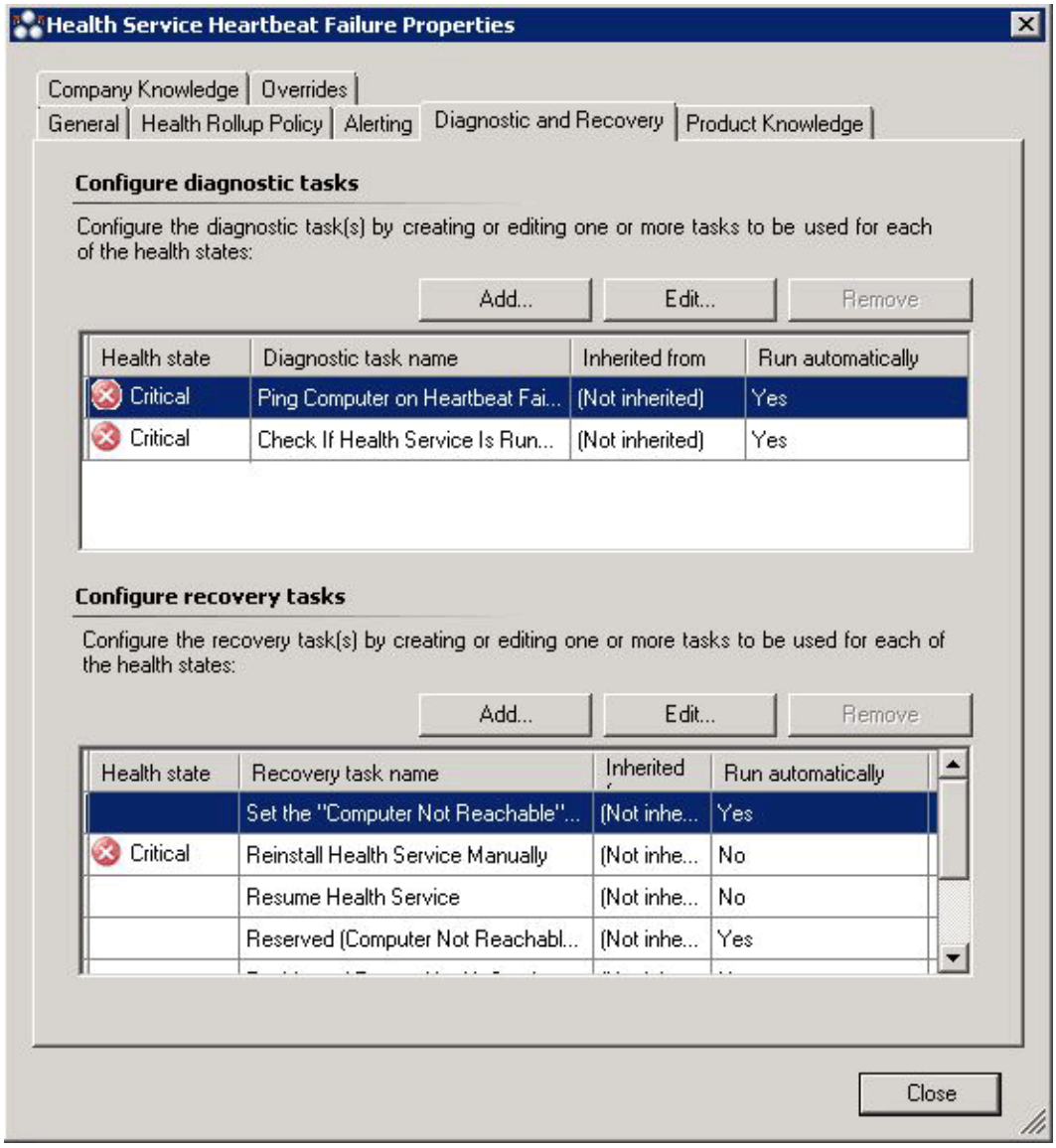
- **Ping Computer on Heartbeat Failure** and **Check If Health Service Is Running**

  These are diagnostic tasks that run automatically when the state for this monitor changes to critical (red).
- **Set the "Computer Not Reachable" monitor to success because the "Ping Computer on Heartbeat Failure" diagnostic succeeded**

  This is a recovery task that runs automatically when the **Ping Computer on Heartbeat Failure** task succeeds.
- **Restart Health Service**

  This is a recovery task that you can run manually or you can enable it to run automatically by using an override.

You can see the tasks available for a monitor on the **Diagnostic and Recovery** tab in the properties of the monitor, as shown in the following illustration.



On this tab, you can also add tasks or edit tasks that you have added previously. For more information on how to add diagnostic and recovery tasks, see Diagnostics and Recoveries in the Author's Guide. Tasks that are configured by a sealed management pack can only be modified by using overrides. For more information, see How to Enable Recovery and Diagnostic Tasks.

See Also

How Heartbeats Work in Operations Manager

Resolving Heartbeat Alerts

Viewing Active Alerts

Viewing Alert Details

Examining Properties of Alerts, Rules, and Monitors

Impact of Closing an Alert

How to Close an Alert Generated by a Monitor

How to Reset Health

Identifying the Computer Experiencing a Problem

Using Health Explorer to Investigate Problems

Using Event View to Investigate Problems

Investigating Alert Storms

How to View All Rules and Monitors Running on an Agent-Managed Computer

How to Set Alert Resolution States

How to Configure Automatic Alert Resolution

How an Alert is Produced

Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

Running Tasks in Operations Manager

How to Suspend Monitoring Temporarily by Using Maintenance Mode

Maintenance mode, available from the **Monitoring** workspace of the Operations console in Operations Manager, enables you to avoid any alerts or errors that might occur when a monitored object, such as a computer or distributed application, is taken offline for maintenance. Maintenance mode suspends the following features:

- Rules and monitors
- Notifications
- Automatic responses
- State changes
- New alerts

Use the following procedure to place one or more monitored objects into maintenance mode.

To put a monitored object into maintenance mode

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Monitoring**.
3. In the **Monitoring** workspace, expand **Monitoring**, and then click **Windows Computers**.

4. In the **Windows Computers** pane, right-click the computer that you want to place into maintenance mode, click **Maintenance Mode**, and then click **Start Maintenance Mode**. You can use ctrl+click or shift+click to select multiple computers to place into maintenance mode.
5. In the **Maintenance Mode Settings** dialog box, under **Apply to**, click **Selected objects only** if only the computer is to be placed into maintenance mode; otherwise, click **Selected objects and all their contained objects**.
6. Select **Planned** if this is a planned event; otherwise, leave it cleared.
7. In the **Category** list, click the appropriate maintenance category.
8. Under **Duration**, select and enter the **Number of minutes** or select and enter the **Specific end time**, and then click **OK**. A maintenance mode icon appears in the **Computers** pane, in the **Maintenance Mode** column for the computer you selected.

   Note
   The minimum value for **Number of minutes** is 5. The maximum value is 1,051,200 (2 years).

To edit maintenance mode settings for a monitored object

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Monitoring**.
3. In the **Monitoring** workspace, expand **Monitoring**, and then click **Windows Computers**.
4. Right-click the computer in the **Windows Computers** pane whose settings you want to edit, click **Maintenance Mode**, and then click **Edit Maintenance Mode settings**.
5. In the **Maintenance Mode Settings** dialog box, edit the settings you want to change, and then click **OK**.

To stop maintenance mode on a monitored object

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Monitoring**.
3. In the **Monitoring** workspace, expand **Monitoring**, and then click **Windows Computers**.
4. In the **Windows Computers** pane, right-click the computer that you want to take out of maintenance mode, click **Maintenance Mode**, and then click **Stop Maintenance Mode**.
5. In the **Maintenance Mode** dialog box, do the following:
   - If you selected **Selected objects and all their contained objects** when you placed the computer into maintenance mode, select **Remove contained objects** and then click **Yes**.
   - If you selected **Selected objects only**, clear **Remove contained objects** and then click **Yes**.
6. In the **Windows Computers** pane, the maintenance mode icon disappears from the **Maintenance Mode** column for the computer you selected.

Note
Because Operations Manager polls maintenance mode settings only once every 5 minutes, there can be a delay in an object's scheduled removal from maintenance mode.

See Also

General Tasks in Operations Manager

Managing Alerts

Connecting Management Groups in Operations Manager

Creating and Managing Groups

Running Tasks in Operations Manager

How to Create a Resource Pool

Managing Resource Pools for UNIX and Linux Computers

Using Operations Manager Shell

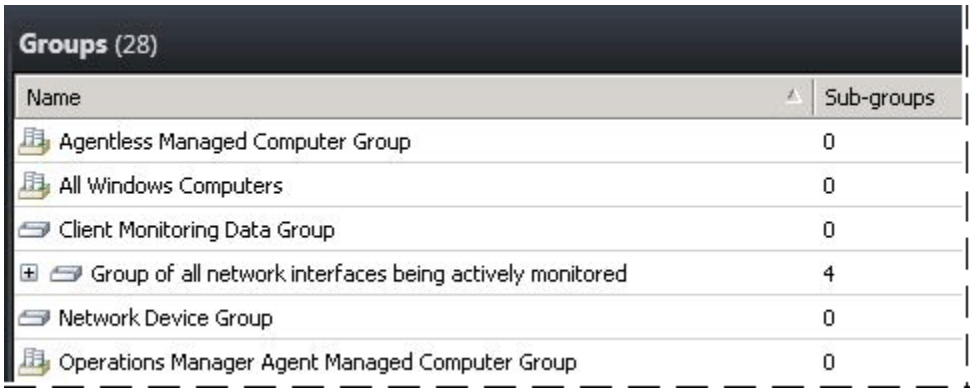
Creating and Managing Groups

In System Center 2012 – Operations Manager, groups are logical collections of objects, such as Windows-based computers, hard disks, or instances of Microsoft SQL Server. You create a group by using the Create Group Wizard. You can explicitly assign membership to a group or you can create rules that will generate a dynamic group membership.

Some of the purposes for using groups are:

- To scope overrides to a specific subset of computers. For more information, see Using Classes and Groups for Overrides in Operations Manager.
- To scope alert notifications or product connector subscriptions for a specific set of computers. How to Create Subscriptions Using Classes and Groups
- To scope user consoles, so the user role only sees the servers they are responsible for.
- To scope a set of computers that need to go into a scheduled maintenance mode.
- To scope application views only to computers that host a given application. For more information, see Guidance for Scoping and Targeting Views.
- To create a rollup health state view of an otherwise unrelated set of computers. For more information, see Guidance for Scoping and Targeting Views.
- To create a set of computers for a report.

You create and manage groups in the **Authoring** workspace of the Operations console. A number of groups are created when you install Operations Manager, and other groups may be added when you import management packs. The following image shows the display of groups in the Operations console.



The icons differentiate between computer groups and instance groups, as shown in the following image.

Computer groups only contain computers. Instance groups can contain all object types, such as an instance of a health service or an instance of a SQL database. Both computer groups and instance groups can contain other computer and instance groups. Another way to view the difference between the group types is:

- An instance group is populated with objects that match your criteria.
- A computer group is populated by computers that host objects that match your criteria.

Using the Operations console, you can only create instance groups. To create a computer group, you must use the Authoring console or work directly in the XML of a management pack.

Creating and Managing Groups topics

- **How to Create Groups in Operations Manager**
- **How to View Group Members, State, and Diagram**

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- General Tasks in Operations Manager
- How to Suspend Monitoring Temporarily by Using Maintenance Mode
- Managing Alerts
- Running Tasks in Operations Manager

- How to Create a Resource Pool
- Connecting Management Groups in Operations Manager
- Operations Manager Report Authoring Guide

See Also

General Tasks in Operations Manager

Managing Alerts

How to Suspend Monitoring Temporarily by Using Maintenance Mode

Using Operations Manager Shell

Running Tasks in Operations Manager

How to Create a Resource Pool

Managing Resource Pools for UNIX and Linux Computers

Connecting Management Groups in Operations Manager

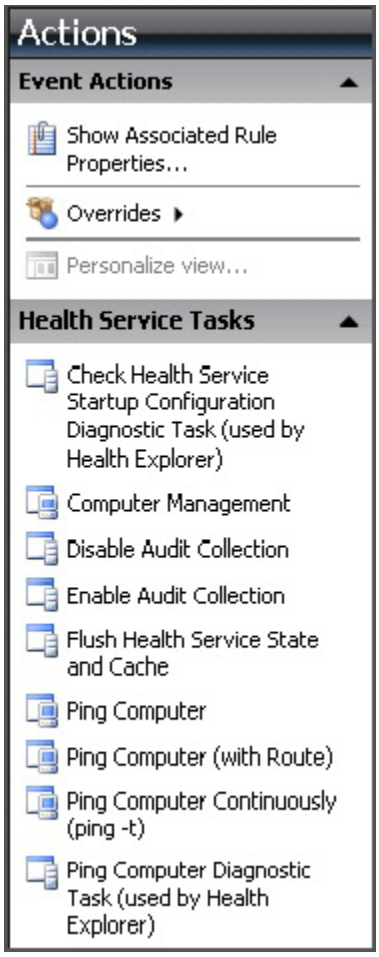
Running Tasks in Operations Manager

In the System Center 2012 – Operations Manager Operations console, the **Tasks** pane provides links to tasks. A task is a user-initiated action from the Operations console that is run on an Operations Manager agent. The tasks that are available depend on the management packs that are installed. For example, Operations Manager comes with a core set of functionality that provides the ping task. When you install the SQL Server management pack, it adds SQL-specific tasks, such as a task to start or stop the SQL Server agent.

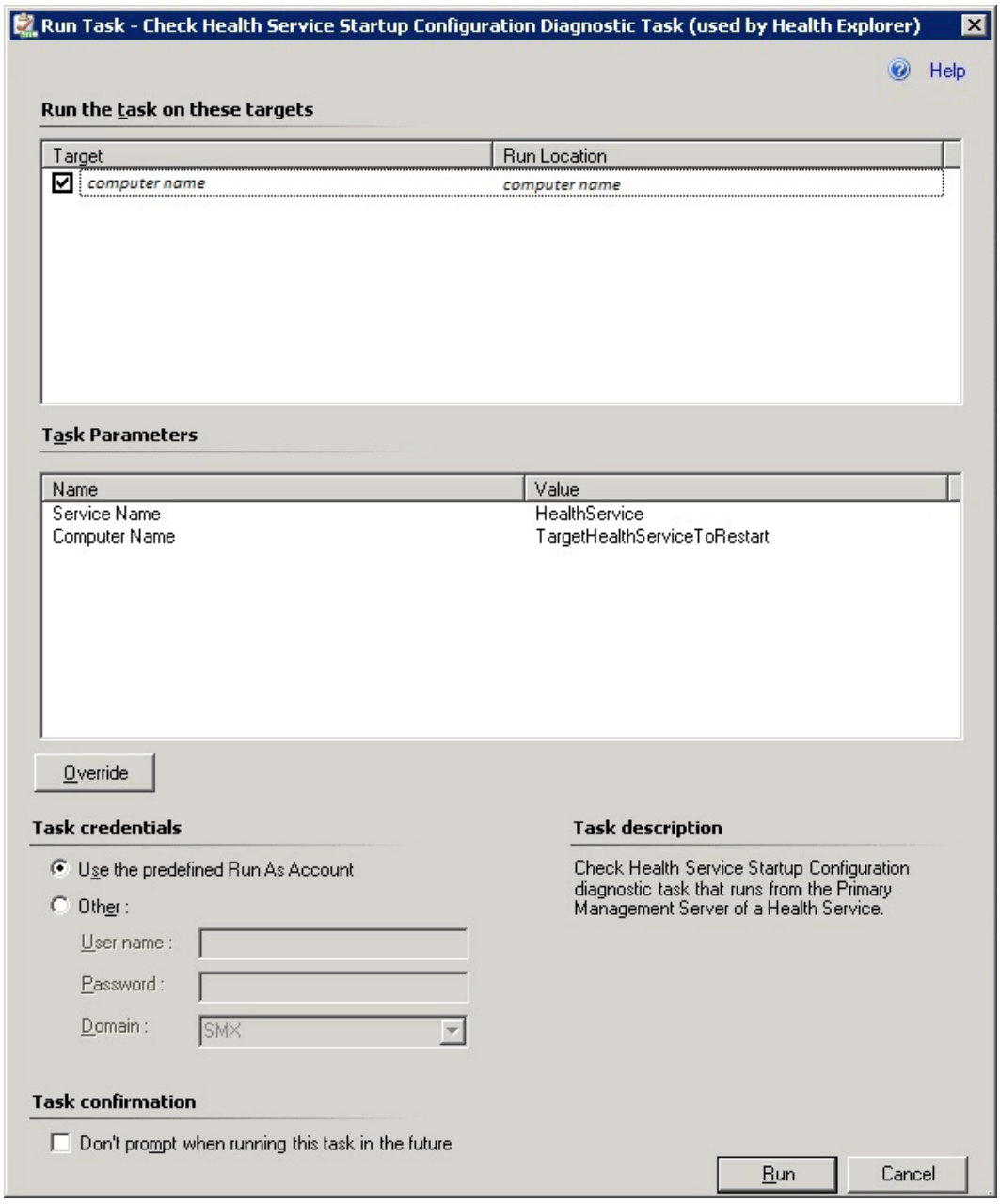
Note

If the **Tasks** pane is not displayed, click **Tasks** on the toolbar to display it.

Click an alert or object to see tasks for that alert or object. Click a task to run the task.

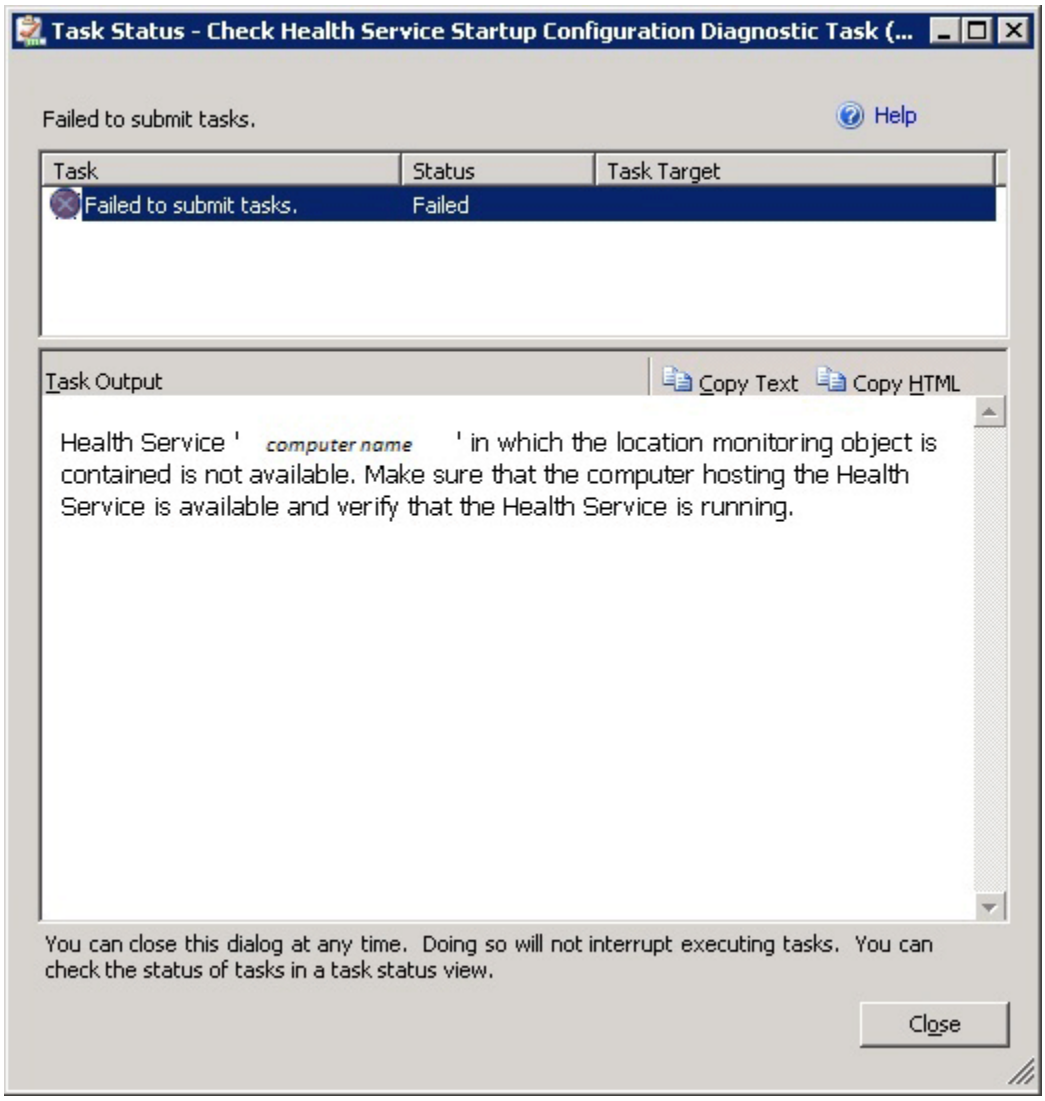


In the example above, if you click the first task (**Check Health Service Startup Configuration Diagnostic Task**), you see a **Run Task** dialog box:



Tasks use the default action account, unless you specify other credentials in this dialog box. Tasks can also be configured by a management pack author to use a specific Run As profile.

Generally, you should accept the defaults and click **Run**. You will then see a **Task Status** window:



In this instance, the task could not be completed successfully. **Task Output** provides you with instructions on troubleshooting the issue.

See Also

General Tasks in Operations Manager

Managing Alerts

How to Suspend Monitoring Temporarily by Using Maintenance Mode

Creating and Managing Groups

Connecting Management Groups in Operations Manager

How to Create a Resource Pool

Managing Resource Pools for UNIX and Linux Computers

How to Create a Resource Pool

A new feature in System Center 2012 – Operations Manager is the *resource pool*. A resource pool is a collection of management servers used to distribute work amongst themselves and take over work from a failed member.

You can use resource pools for:

- Monitoring network devices.
- Monitoring UNIX and Linux computers.

Resource pools ensure the continuity of monitoring by providing multiple management servers that can take on monitoring workflows if one of the management servers becomes unavailable. You can create resource pools for specific purposes. For example, you might create a resource pool of management servers that are located in the same geographic area to provide network device monitoring.

When Operations Manager is installed, three resource pools are created: All Management Servers Resource Pool, Notifications Resource Pool, and AD Assignment Resource Pool. All management servers are automatically members of these resource pools. For information about removing a management server from the Notifications Resource Pool and AD Assignment Resource Pool, see Modifying Resource Pool Membership.

Note
The membership of the All Management Servers Resource Pool is read-only.

For information about configuring resource pools with managed UNIX and Linux computers and for configuring certificates, see Managing Resource Pools for UNIX and Linux Computers.

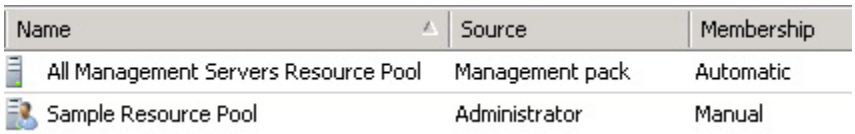
To create a resource pool

1. Log on to the Operations console with an account that is a member of the Operations Manager Administrators role.
2. Click **Administration**.
3. In the navigation pane, click **Resource Pools**.
4. In the **Tasks** pane, click **Create Resource Pool**.
5. In the **Create Resource Pool** wizard, on the **General Properties** page, enter a name and, optionally, a description for the resource pool, and then click **Next**.
6. On the **Pool Membership** page, click **Add**.
7. In the **Member Selection** window, enter text to filter the search results if desired, and then click **Search**. If you click **Search** without entering anything in the filter field, all available management servers will be displayed.
8. In **Available items**, select the servers that you want in the resource pool, click **Add**, and then click **OK**.

9. Click **Next**.
10. On the **Summary** page, review the settings and then click **Create**.
11. When the wizard completes, click **Close**.

Modifying Resource Pool Membership

When you view the resource pools in the **Administration** workspace, you will see that resource pools that you create have a manual membership type and resource pools created when Operations Manager was installed have an automatic membership type, as shown in the following image.



Name	Source	Membership
All Management Servers Resource Pool	Management pack	Automatic
Sample Resource Pool	Administrator	Manual

By default, all management servers are members of the resource pools created when Operations Manager is installed, and any management servers added to the management group are automatically added to the resource pools that have an automatic membership type. You can remove individual management servers from those resource pools, however that will change the membership type to manual. If you add a management server to a management group after the membership type of the resource pools created when Operations Manager was installed is changed to manual, you must add the management server to the resource pool manually.

To remove a member from an automatic resource pool

1. Log on to the Operations console with an account that is a member of the Operations Manager Administrators role.
2. Click **Administration**.
3. In the navigation pane, click **Resource Pools**.
4. In the results pane, click the resource pool that you want to modify.
5. In the **Tasks** pane, click **Manual Membership**, and then click **Yes** in the **Manual Membership** message.

   Important
   When you click **Yes**, the membership type of the selected resource pool changes to manual. Even if you make no changes to the resource pool membership and cancel the properties dialog box, the membership type will remain manual after this step.
6. On the **General Properties** page for the resource pool, click **Next**.
7. On the **Pool Membership** page, click the management servers that you want to remove from the resource pool, click **Remove**, and then click **Next**.
8. On the **Summary** page, click **Save**.

See Also

General Tasks in Operations Manager

Managing Alerts

How to Suspend Monitoring Temporarily by Using Maintenance Mode

Creating and Managing Groups

Running Tasks in Operations Manager

Connecting Management Groups in Operations Manager

Managing Resource Pools for UNIX and Linux Computers

Using Operations Manager Shell

Managing Resource Pools for UNIX and Linux Computers

You can specify the resource pool that manages a particular UNIX or Linux computer. This capability allows you to create a resource pool dedicated to managing only UNIX and Linux computers.

The following procedures show how to change a resource pool for a managed UNIX or Linux computer, and how to configure certificates for a resource pool. Configuring certificates is required to maintain high availability in resource pools and must be performed whenever a resource pool is created and when a management server is added to a resource pool.

Changing Resource Pools

Changing a resource pool for a UNIX or Linux computer is different than modifying the set of management servers that are members of resource pool, as described in How to Create a Resource Pool. The following procedure does not modify the members of a resource pool, only what the resource pool manages.

To change resource pools

1. Click **Administration**.
2. In the navigation pane, click **Resource Pools**.
3. In the **Tasks** pane, click **Change Resource Pool**.
4. In the upper list, select the computers that you want to change to be managed by a different resource pool.
5. In the lower list, select the resource pool to manage computers selected in the upper list.
6. Click **Change**.

Configure Certificates for Resource Pools

An additional task must be performed in order to configure UNIX and Linux computers for resource pools. Operations Manager uses certificates to authenticate access to the computers it is managing. When the Discovery Wizard deploys an agent, it retrieves the certificate from the agent, signs the certificate, deploys the certificate back to the agent, and then restarts the agent.

To configure high availability, each management server in the resource pool must have all the root certificates that are used to sign the certificates that are deployed to the agents on the UNIX and Linux computers. Otherwise, if a management server becomes unavailable, the other management servers would not be able to trust the certificates that were signed by the server that failed. The process for this task is as follows:

1. Export the root certificates from each management server in the resource pool to a file.
2. Import all the exported certificate files into each management server (except for the file that was exported by that same server).

To configure certificates for high availability

1. Log on to a management server to start the process of exporting certificates.
2. At the command prompt, change the directory to %ProgramFiles%\System Center Operations Manager 2012\Server.
3. Run the following command, specifying a file name of your choosing such as **Server3.cert**:

   ```
   scxcertconfig.exe – export <filename>
   ```

4. Copy the exported file to a shared directory that is accessible by all the management servers in the resource pool.
5. Repeat the previous four steps until the shared directory contains all the exported certificate files from each management server in the resource pool.
6. Log on to a management server to start the process of importing certificates.
7. At the command prompt, change the directory to %ProgramFiles%\System Center Operations Manager 2012\Server.
8. Run the following command for each exported certificate file (except for the file that was exported by the current management server):

   ```
   scxcertconfig.exe –import <filename>
   ```

   Note

   If you attempt to import the certificate file that was exported by that same management server, the process will fail with an error message that the object or property already exists.
9. Repeat the previous three steps until all the certificate files have been imported to the applicable management servers in the resource pool.
10. Delete the certificate files from the shared directory. Although the file contains only the public key of the certificate, you should still treat it as a security-sensitive file.

Perform this procedure whenever you add a new management server to the resource pool so that high availability is maintained.

See Also

General Tasks in Operations Manager

Managing Alerts

How to Suspend Monitoring Temporarily by Using Maintenance Mode

Creating and Managing Groups

Running Tasks in Operations Manager

How to Create a Resource Pool

Using Operations Manager Shell

Connecting Management Groups in Operations Manager

Connecting management groups in System Center 2012 – Operations Manager enables the ability to view and interact with data from multiple management groups in a single Operations console. The management group in which the consolidated view is available is called the local management group, and those that contribute their data to the consolidated view are called the connected management groups. They relate to each other in a hierarchical fashion, with connected groups in the bottom tier and the local group in the top tier. The connected groups are in a peer-to-peer relationship with each other. Each connected group has no visibility or interaction with the other connected groups; the visibility is strictly from the local group into the connected group.

Note
Operations Manager does not support communication of data between peer management groups. Only the local to connected hierarchy configuration is supported. Multiple tiers, where a management group would be both a local group and a connected group, are not supported.

When you connect management groups, you are not deploying any new servers; rather, you are allowing the local management group to have access to the alerts and discovery information that is in a connected management group. In this way, you can view and interact with all the alerts and other monitoring data from multiple management groups in a single Operations console. In addition, you can run tasks on the monitored computers of the connected management groups.

Connecting management groups offers these additional services:

- Consolidated monitoring and alerting for greater than 6,000 agents
- Consolidated monitoring across trust boundaries

Important

Both management groups must be running the same build of Operations Manager. For example, both management groups must be running System Center 2012 – Operations Manager.

In addition to all of the communications channels used in the multiple server, single management group configuration, connected management groups require communication between the management servers of the local group and the management servers of the connected group over TCP 5723 and 5724. For a complete list of ports used by Operations Manager, see Operations Manager Supported Configurations.

Connected management groups support all Operations Manager user roles and makes use of the Operations Manager Connector Framework to enable bidirectional communication between the connected groups and local groups.

In this procedure, you create a connection between two management groups. These management groups can be in the same domain, or they can be in trusted domains. You can connect to management groups that are in domains that are not trusted, but you cannot view data from those domains until you add an account from the domain of the local management groups to an Operations Manager role for the connected management group. To do this, a trust must be established between the domains.

Before you start

1. To connect management groups, you must provide the fully qualified domain name (FQDN) of the root management server (RMS) of the connected management group. The management server of the local management group must be able to resolve this FQDN. If the two management groups do not use the same Domain Name System (DNS) service, you must create a secondary DNS zone in the DNS service that the local management group uses. This secondary DNS zone transfers the DNS information from the primary DNS zone of the connected management group. The transferred information is essentially a copy of the DNS information that is available to the management server of the local management group.
2. Add the System Center Data Access service and System Center Management Configuration service account of the connected management groups to the Operations Manager Administrator role for the connected management group, or add it to the domain-based Operations Manager Administrator security group in the connected management group's domain, which has already been added to the Operations Manager Administrator role.
3. Collect the System Center Data Access service and System Center Management Configuration service account credentials from the connected management groups. These credentials are needed when you add the connected management group in the local management group.
4. Identify users in the domain of the local management group that will need access to data from the connected management groups. They must be added to the appropriate Operations Manager roles in the connected management group.

To connect management groups

1. Log on to the computer with an account that is a member of the Operations Manager Administrators user role.
2. In the Operations console that is connected to the destination management group, click **Administration**.
3. In the **Administration** workspace, right-click **Connected Management Groups**, and then click **Add Management Group**.
4. In the **Add Management Group** dialog box, do the following:
   a. Type the **Management Group name** of the management group to be connected.
   b. Type the fully qualified domain name (FQDN) of a **Management Server** in the desired management group to be connected.
   c. Specify the account that will be used for the initial connection to the connected management group, either by leaving **Use SDK service account** selected or selecting **Other user account** and typing in the **User name**, **Password**, and **Domain**. The account must be a member of the Operations Manager Administrators role for the connected management group.
5. Click **Add**.

To grant access to Connected Management Groups

1. Identify users in the local management group that need access to the connected management groups.
2. Add those users as members to the appropriate user role in the connected management groups.

   Note
   If local and connected management groups are not in the same domain and there is no trust relationship between the two domains, you will have to create accounts in the connected management group domain for the users in the local management group domain to use.
3. In the Operations console for the local management group, in the **Administration** view, expand **Security**, and then click **User Roles**.
4. In the right pane, right-click the user role to which you want to grant connected management group access, and then click **Properties**.
5. On the **Group Scope** tab, select the connected management groups to which you want to grant access to this user role, and then click **OK**. A user with both permission and access to at least one connected management group will see the **Show Connected Alerts** button in the toolbar of any **Alert** view in the **Monitoring** space.
6. A **Log On** dialog box appears and prompts the user for credentials (to log on to the connected management groups). Enter the credentials, and then click **OK**. Alerts appear from all connected management groups for which you have access and permission. You can run tasks in the managed computers of connected management groups.

See Also

General Tasks in Operations Manager

Managing Alerts

How to Suspend Monitoring Temporarily by Using Maintenance Mode

Creating and Managing Groups

Running Tasks in Operations Manager

How to Create a Resource Pool

Managing Resource Pools for UNIX and Linux Computers

Using Operations Manager Shell

Using Operations Manager Shell

In System Center 2012 – Operations Manager, the Operations Manager Shell is installed with the Operations Manager console; it provides a command-line environment and task-based scripting technology that you can use to automate many Operations Manager administrative tasks.

The Operations Manager Shell is built on Windows PowerShell. The Operations Manager Shell extends Windows PowerShell with an additional set of *cmdlets*, which can either be run directly from the command shell prompt or called from within a script. Cmdlets can be used individually to perform a specific task, or they can be combined with other cmdlets to perform complex administrative tasks. Unlike traditional command-line environments that work by returning text results to the end user or routing ("piping") text to different command-line utilities, Windows PowerShell manipulates Microsoft .NET Framework objects directly. This provides a more robust and efficient mechanism for interacting with the system.

To open the Operations Manager Shell, click **Start**, click **All Programs**, click **Microsoft System Center 2012**, click **Operations Manager**, and then click **Operations Manager Shell**. You can also import the Operations Manager module into an existing Windows PowerShell session by typing the following at the command prompt:

```
Import-Module –Name OperationsManager
```

You can access cmdlet help in the Operations Manager Shell by typing Get-Help *cmdlet name* or view the help online at Cmdlets in System Center 2012 – Operations Manager.

To learn more about Windows PowerShell, see Windows PowerShell Getting Started Guide.

See Also

General Tasks in Operations Manager

Managing Alerts

How to Suspend Monitoring Temporarily by Using Maintenance Mode

Creating and Managing Groups

Running Tasks in Operations Manager

How to Create a Resource Pool

Managing Resource Pools for UNIX and Linux Computers

Connecting Management Groups in Operations Manager

Maintenance of Operations Manager

Maintenance of Operations Manager topics

- **Monitoring the Health of the Management Group**
- **Inventory of Operations Manager Infrastructure**
- **Scheduling Maintenance in Operations Manager**
- **How and When to Clear the Cache**
- **How to Restart a Management Server**
- **How to Configure Grooming Settings for the Operations Manager Database**
- **How to Configure Grooming Settings for the Reporting Data Warehouse Database**
- **Recommendations for Daily, Weekly, and Monthly Operations Manager Tasks**

Other resources for this component

- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Initial Monitoring After Operations Manager Is Installed
- Managing Access in Operations Manager
- Operations Manager Monitoring Scenarios
- General Tasks in Operations Manager
- Getting Information from Operations Manager
- Operations Manager Report Authoring Guide

Integrating Operations Manager with Development Processes

Streamlining the communications between development and information technology (IT) operations teams (often called DevOps) can help you decrease the time it takes for application maintenance and delivery into production, where your application delivers value to customers. To speed interactions between these teams, it is essential to quickly detect and fix problems that might need assistance from the engineering team.

These topics can help you integrate your version of System Center 2012 with development tools, such as Team Foundation Server (TFS) and Visual Studio. This integration enables deep troubleshooting and provides greater efficiency between development and IT operations teams.

Integrating Operations Manager with Development Processes (DevOps) Topics

- Integrating Operations Manager with Development Processes in System Center 2012 R2
- Integrating Operations Manager with Development Processes in System Center 2012 SP1
- Monitoring with Microsoft Monitoring Agent

Integrating Operations Manager with Development Processes in System Center 2012 R2

Streamlining the communications between development and information technology (IT) operations teams (often called DevOps) can help you decrease the time it takes for application maintenance and delivery into production, where your application delivers value to customers. To speed interactions between these teams, it is essential to quickly detect and fix problems that might need assistance from the engineering team.

The topics in this section can help you integrate System Center 2012 R2 Operations Manager with development tools, such as Team Foundation Server (TFS) and Visual Studio. This integration enables deep troubleshooting and provides greater efficiency between development and IT operations teams.

Integrating Operations Manager with Development Processes (DevOps) Topics

- How to Configure Integration with TFS in System Center 2012 R2

  You can synchronize System Center 2012 R2 Operations Manager alerts and TFS work items. When synchronization is enabled, IT operations can assign alerts to the engineering team.
- How to Configure File Attachments for Operations Manager Alerts in System Center 2012 R2

  You will need to configure file attachments for Operations Manager alerts. Proper configuration enables integration with TFS, IntelliTrace Historical Profiling, sharing Application Performance Monitoring events with developers, Global Service Monitor web tests, and any other scenarios that require files to be associated with Operations Manager alerts.
- How to Synchronize Alerts with TFS in System Center 2012 R2

TFS lets you configure engineering process templates. Operations Manager integration with TFS introduces a new "Operational Issue" work item type definition that can be embedded into any of your organization's engineering processes.

- How to Configure Integration with IntelliTrace Historical Profiling in System Center 2012 R2

  You can help developers to debug applications by collecting IntelliTrace snapshots directly from Operations Manager. When TFS and Operations Manager are integrated, these snapshots can be automatically attached to TFS work items.

- How to Collect IntelliTrace Historical Profiling Traces from System Center 2012 R2

  After configuring integration with IntelliTrace, you can collect and share IntelliTrace snapshots with developers.

- Monitoring Integration between Operations Manager and TFS in System Center 2012 R2

  Depending on your environment, you can import TFS monitoring and management packs that give you real-time visibility into the health of the TFS developer environment.

How to Configure Integration with TFS in System Center 2012 R2

In System Center 2012 R2 Operations Manager, you can synchronize Operations Manager alerts and TFS work items. After enabling synchronization, information technology (IT) operations can assign alerts to the engineering team. When you first assign an alert to engineering, TFS creates a new work item. The workflow then tracks and synchronizes changes that are made to TFS work items and changes that are made to associated Operations Manager alerts. You can synchronize alerts with team projects in TFS 2012, TFS 2010, or both.

Important

If your environment was upgraded from System Center 2012 Service Pack 1 (SP1) to Operations Manager and used the versions of the management packs that shipped with System Center 2012 SP1, you can continue to use them, but you will be limited to the scenarios that System Center 2012 SP1 supported. If you want to simultaneously synchronize Operations Manager alerts with Team Foundation Server (TFS) and Service Manager, you need to use the management packs shipped with System Center 2012 R2 Operations Manager.

Important

Before you enable configuration, you must have TFS administrator credentials to be able to import the Operational Issue Work Item Type Definition that is used by integration with TFS. Additionally, you must have a configured domain account with TFS contributor rights in the team projects that you want to synchronize Operations Manager alerts with.

To prepare your environment for synchronization with TFS

1. Import and configure the Alert Attachment Management Pack. For more information, see How to Configure File Attachments for Operations Manager Alerts in System Center 2012 R2.
2. Decide which management servers you want to use to synchronize Operations Manager alerts and TFS work items. Each management server that is used for synchronization must have TFS Object Model installed. You can install the TFS Object Model for TFS 2010 from the MSDN Download Center (Team Foundation Server 2010 SP1 Object Model Installer) or by installing the TFS Object Model for TFS 2012 from the MSDN Download Center (Team Foundation Server 2012 Update 1 Object Model Installer). You can also install the TFS Object Model for TFS 2012 when you install Visual Studio 2012. Installing TFS on a server also installs the TFS Object Model on that server.

   Note
   Either version of the TFS Object Model can be used for synchronization with either version of TFS. However, in order to synchronize with TFS 2012 using TFS Object Model 2010, you must manually import the Operational Issue work item type definition (WITD) into each team project that will be used for synchronization. Do this by using the **witadmin** command-line tool. For more information about manually importing the Operational Issue WITD, see How to Manually Import an Operational Issue WITD to TFS in System Center 2012 R2.

   Tip
   Installing synchronization on all management servers in the management group will help to simplify maintenance and bring redundancy into the integration between Operations Manager and TFS.
3. Create a domain account that will be used for TFS synchronization.
4. Give this domain account TFS contributor permissions for each project that you plan to use for TFS synchronization. For more information, see Add Users to Team Projects.
5. If you intend to synchronize alert file attachments with TFS work items, give this account read/write access to the Alert Attachment file share. This is the file share that was established when you configured the Alert Attachment Management Pack.

To configure synchronization for the TFS Work Item Synchronization Management Pack

1. Import the TFS Work Item Synchronization Management Pack from the Operations Manager installation media. In the Operations Manager console, click **Administration**, click **Management Packs**, and then, in the **Tasks** pane, click **Import Management Packs**. In the Import Management Packs Wizard, click **Add**, and then click **Add from disk**. Import the TFS Work Item Synchronization Management Pack (Microsoft.SystemCenter.TFSWISynchronization.mpb) from the ManagementPacks folder on the Operations Manager installation media. Click **Install**, and then click **Close**.
2. To begin configuring the TFS Work Item Synchronization Management Pack, in the Operations Manager console, in the navigation pane, click **Authoring**, click **Management Pack Templates**, and then, in the **Tasks** pane, click **Add Monitoring Wizard**.

Important

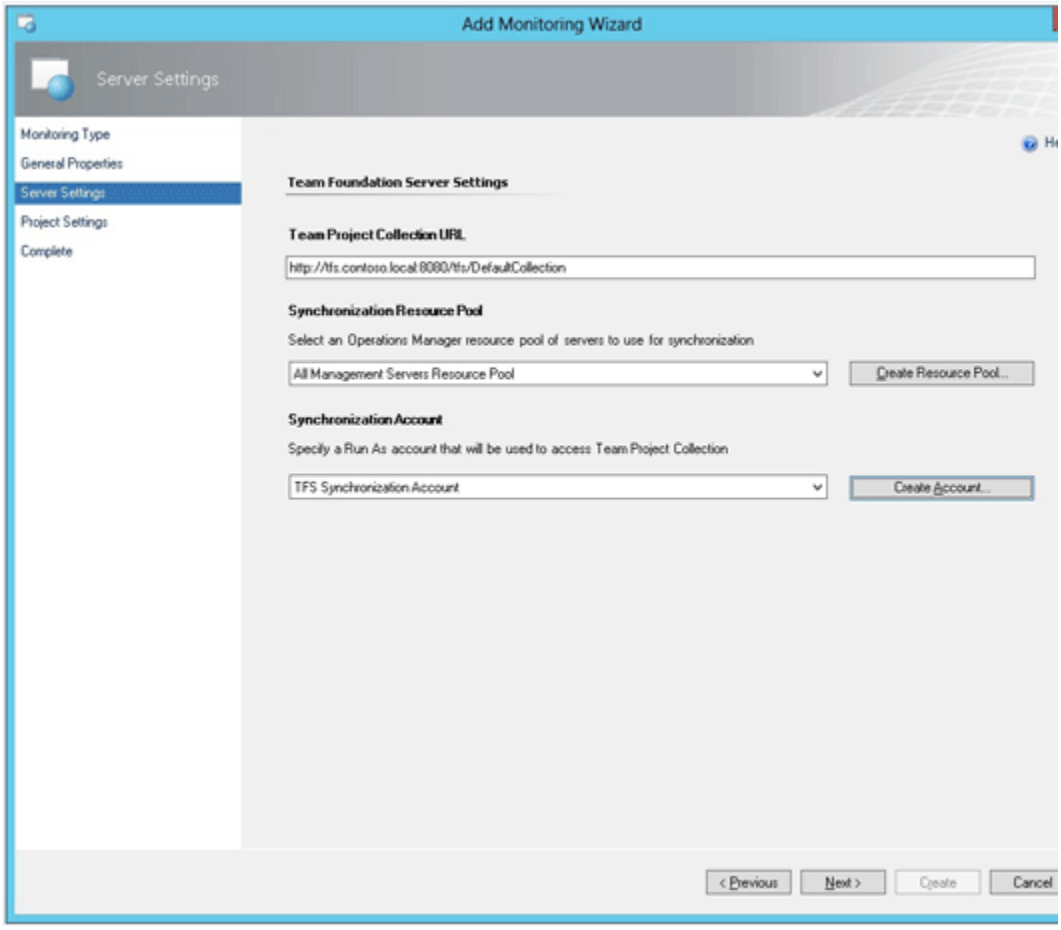
You must run the Add Monitoring Wizard for each team project collection that you want to synchronize alerts with.

3. To open the TFS Work Item Synchronization template, in the Add Monitoring Wizard, on the **Monitoring Type** page, select **TFS Work Item Synchronization**.
4. On the **General Properties** page, type a display name for this team project collection and a description, and then select a target management pack to store your configuration settings.
5. On the **Server Settings** page, enter the **Team Project Collection URL** (for example: http://tfs.contoso.local:8080/tfs/DefaultCollection/), and then select the **Synchronization Resource Pool** of the management servers that are used for load-balancing synchronization. Each server in this resource pool must already have the TFS Object Model installed. Then, create or select a Run As account that will be used for synchronization. This Run As account must have contributor permissions in each TFS team project. If you want to synchronize alert file attachments, the Run As account must have read/write access to the Alert Attachment file share. Make sure that these credentials are distributed to all management servers that are used for synchronization. For more information about using Run As profiles, see Managing Run As Accounts and Profiles.

   Note

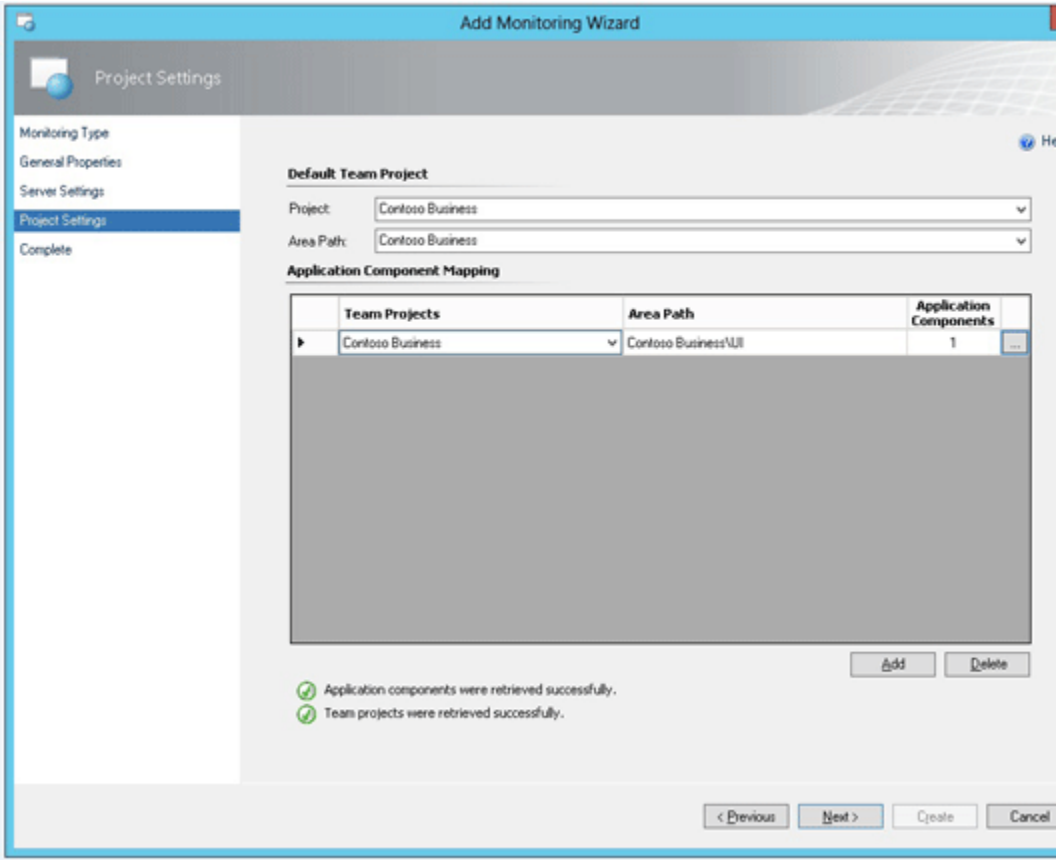
   You can get the TFS Team Project Collections URL from the Team Foundation Server Administration Console. If the TFS Team Project Collection that you choose is offline or otherwise unavailable, the wizard will warn you, but it will still let you finish the configuration. Additionally, when TFS is not available, there is no validation for your input in the wizard. The team project and area path will not be prepopulated with existing values.

   Server Settings page



6. On the **Project Settings** page, specify the **Project** and **Area Path** that will be used to synchronize all alerts. You can customize these settings for each .NET application component that was previously configured for monitoring with .NET Application Performance Monitoring (APM). To customize the team project and TFS area path for an APM component, click **Add**, which will add a new row. Choose a target **Team Project** and **Area Path** combination, and then click the (**…**) button to select which configured application components will synchronize with this team project and area path. The application components must already be configured for monitoring with the .NET Application Performance Monitoring template. For more information, see .NET Application Performance Monitoring Template.

   Project Settings page



Note

You can configure synchronization with multiple Team Foundation Servers or multiple Team Project Collections by running the configuration wizard multiple times. However, only one configuration can have the **Default Team Project** and **Default Area Path** specified.

7. When you finish the wizard, you will be asked for TFS administrator credentials so that the wizard can automatically import the Operational Issue WITD to each team project that is used in the configured synchronization. You can skip this step if you want to manually import the Operational Issue WITD. You must manually import the WITD when you are synchronizing with Team Foundation Server 2012 using TFS Object Model 2010. For more information, see [How to Manually Import an Operational Issue WITD to TFS in System Center 2012 R2].

Note

After you configure synchronization, the TFS Work Item Synchronization management pack will monitor the synchronization infrastructure, and it will generate alerts if synchronization fails. However, to monitor the complete TFS infrastructure, you need additional monitoring packs that can alert you about a wide range of potential problems with TFS components. When you import the

TFS Work Item Synchronization management pack, you should also import and configure these monitoring packs. Together, they help you make sure that you are monitoring the complete health of the developer TFS environment. For more information, see Monitoring Integration between Operations Manager and TFS in System Center 2012 R2.

Changing Synchronization Settings

You can view or change synchronization settings for the TFS Work Item Synchronization Management Pack. You will need to change these settings to modify a destination team project and area path or to customize synchronization rules for a monitored .NET application component.

To prevent inconsistent synchronization while new settings are being applied, turn off synchronization before you change the configuration. For information about stopping and resuming synchronization, see How to Stop and Resume Synchronization with TFS in System Center 2012 R2. The process of replicating configuration changes to all management servers in the synchronization pool might take an hour or more, depending on the system performance of your management group. After the replication is complete, you can turn synchronization on again. If the configuration was changed while synchronization was running, you might have to force a reset of the configuration by restarting the System Center Management Service on all management servers in the synchronization pool.

If you change a destination team project for synchronization, the rules in the following table apply.

Changes in TFS team project location	How synchronization is affected
An application is mapped to a new TFS project within the same TFS project collection.	New alerts go to the new project and old alerts keep synchronizing with the old project. If you delete old ticket IDs and reassign the related alerts to engineering, new work items are created in the new project. These new work items are not linked to any of the pre-existing work items.
An application is mapped to a new TFS project within the same TFS server, but in a different TFS project collection.	New alerts go to the new TFS project. The old alerts stop synchronizing completely. If you delete old ticket IDs and reassign the related alerts to engineering, new work items are created. These new work items are not linked to any of the pre-existing work items.
An application is mapped to a project on a different server.	New work items are created for alerts that are newly assigned to engineering. Synchronization of any previously synchronized alerts stops.

To change synchronization settings

1. To change synchronization settings, in the Operations Manager console, in the navigation pane, click **Authoring**, expand **Management Pack Templates**, and then click **TFS Work Item Synchronization**.
2. Locate a previously configured team project collection, and in the **Tasks** pane, click **Properties**.

   Note
   If you recently changed configuration and the change has not been replicated to the management servers, you must wait for the changes to be replicated before you can view and work with the new configuration. The replication of configuration changes to all management servers in the synchronization pool might take an hour or more, depending on the system performance of your management group.
3. On the **Server Settings** tab, you can change the **Synchronization Resource Pool** of the management servers that are used for load-balancing synchronization. Each server in this resource pool must already have the TFS Object Model installed. Also, you can change the Run As account that will be used for synchronization. This account must have contributor permissions in each TFS team project, and, if you want to synchronize alert file attachments, the account must have read/write access to the Alert Attachment file share. Make sure that these credentials are distributed to all management servers that are used for synchronization. For more information about using Run As profiles, see Managing Run As Accounts and Profiles.

   Note
   If you need to change the Team Project Collection URL, you must delete the configuration and run the wizard again.
4. On the **Project Settings** tab, specify the **Default Team Project** and **Default Area Path** that will be used to synchronize all alerts. You can customize these settings for each .NET application component that was previously configured for monitoring with .NET Application Performance Monitoring (APM). To customize the team project and TFS area path for an APM component, click **Add** to add a new row. Choose a target **Team Project** and **Area Path** combination, and then click the (**…**) button to select which configured application components will synchronize with this team project and area path. The application components must already be configured for monitoring with the .NET Application Performance Monitoring template. For more information, see .NET Application Performance Monitoring Template.

   Note
   To configure synchronization with multiple Team Foundation Servers or multiple Team Project Collections, you can run the configuration wizard multiple times. However, only one configuration can have the **Default Team Project** and **Default Area Path** specified.
5. Click **OK**.

6. If you added a new team project to synchronize with, you will be asked for TFS administrator credentials so that the wizard can automatically import the Operational Issue WITD to the new team project that is used in the configured synchronization. You can skip this step if you want to manually import the Operational Issue WITD. You must manually import the WITD when you are synchronizing with TFS 2012 using TFS Object Model 2010. For more information, see How to Manually Import an Operational Issue WITD to TFS in System Center 2012 R2.

Procedures Related to Configuring Integration with TFS

For additional information, see the following procedures related to configuring integration with TFS in System Center 2012 R2:

- How to Change the Frequency of Synchronization for Integration with TFS in System Center 2012 R2
- How to Manually Import an Operational Issue WITD to TFS in System Center 2012 R2
- How to Configure Whether Files Are Attached or Linked in Synchronization with TFS in System Center 2012 R2
- How to Configure Notifications when Developers Reassign Work Items to IT Operations in System Center 2012 R2
- How to Automatically Assign New Alerts to Engineering in System Center 2012 R2
- How to Automatically Close Alerts When Work Items Are Resolved in TFS in System Center 2012 R2
- How to Stop and Resume Synchronization with TFS in System Center 2012 R2

How to Change the Frequency of Synchronization for Integration with TFS in System Center 2012 R2

In System Center 2012 R2 Operations Manager, synchronizing Operations Manager alerts and work items is key to working effectively and efficiently with your development team. When you assign an alert to engineering, the matching work item in Team Foundation Server (TFS) will not be created immediately. The synchronization frequency is controlled by overrides in the Operations Manager TFS Work Item Synchronization management pack (Microsoft.SystemCenter.TFSWISynchronization.mpb). To change the synchronization frequency, you can change the overrides listed in the following table.

Override description	Target object	Rule	Parameter	Default Value
How often new TFS work items are created from alerts	TFS Connector	TFS Work Items Creation Rule	Interval Seconds	300 seconds

Override description	Target object	Rule	Parameter	Default Value
assigned to Engineering				
How often alerts assigned to Engineering and their associated TFS work items are synchronized	TFS Collection	TFS Work Items Synchronization Rule	Interval Seconds	900 seconds
How often alert attachments are added from the network file share to TFS work items	TFS Collection	Attachments Synchronization Rule	Interval in Seconds	900 seconds
The time range of the TFS work item history that will be synchronized with the alerts. You might want to temporarily change this value to allow synchronization of previous changes to catch up if synchronization was turned off for more than 24 hours. The default value of 24 means that changes that are made to a TFS work item only during the past 24 hours will be synchronized.	TFS Collection	TFS Work Items Synchronization Rule	Delta in Hours	24 hours
How often the APM alerts will receive converted IntelliTrace logs. The value is defined	IntelliTrace attachments for APM alerts singleton object	Add IntelliTrace as an APM attachment rule	IntelliTrace conversion data source polling interval	15 minutes

Override description	Target object	Rule	Parameter	Default Value
in minutes.				

Caution
Setting the override frequencies too low might add substantial load to your management servers and TFS.

To change the frequency of synchronization

1. Using the table above, find the override parameter that you want to change.
2. In the Operations Manager console, click **Authoring**, expand **Management Pack Objects**, and then click **Rules**. To set the scope of displayed rules, click **Scope**, and then select **View all targets**. Locate and select **TFS Collection** and **TFS Connector**. Click **OK**.

   Important
   If you are using IntelliTrace, you must also select **IntelliTrace attachments for APM alerts singleton object**.
3. In the list of scoped rules, right-click the rule with the parameter that you want to override. Click **Overrides**, click **Override the Rule**, and then click **For all objects of class**.
4. Override the parameter to a new value, and save the settings to a management pack.

See Also

How to Override a Rule or Monitor

How to Manually Import an Operational Issue WITD to TFS in System Center 2012 R2

System Center 2012 R2 Operations Manager integration with Team Foundation Server (TFS) uses the work item type *Operational Issue*, which must be present in each team project that synchronization uses. Generally, the TFS Work Item Synchronization Configuration Wizard can import this work item type definition (WITD). In some cases, however, you must manually import the WITD directly to TFS. You must manually import the Operational Issue WITD in the following cases:

- A separate TFS administrator controls the development process model in TFS.
- You are running the TFS 2010 Object Model to integrate with TFS 2012 or TFS 2013.
- You are running the TFS 2012 Object Model to integrate with TFS 2010 or TFS 2013.
- An external procedure has removed the Operational Issue WITD from the team projects in TFS, and you still want to synchronize with this team project.

Caution

The Operational Issue work item type should not be renamed. Renaming this work item type breaks synchronization. Any modifications to this work item type will be overridden when you change configuration settings. This might cause problems with synchronization.

To manually import the Operational Issue WITD file

1. Locate the correct Operational Issue WITD for your version of TFS on the installation media for Operations Manager in System Center 2012 SP1 in the **SupportTools** folder. For TFS 2010, the file name is OperationalIssue.xml. For TFS 2012, the file name is OperationalIssue_11.xml. For TFS 2013, the file name is OperationalIssue_11.xml.
2. Use TFS administrator credentials to run the **witadmin** command-line tool in TFS and import the Operational Issue WITD to each TFS project you plan to use with synchronization.

   Example for TFS 2010: `witadmin importwitd /collection:http://tfs.contoso.com:8080/tfs /p:ProjectName /f:OperationalIssue.xml`

   Example for TFS 2012: `witadmin importwitd /collection:http://tfs.contoso.com:8080/tfs /p:ProjectName /f:OperationalIssue_11.xml`

   Example for TFS 2013: `witadmin importwitd /collection:http://tfs.contoso.com:8080/tfs /p:ProjectName /f:OperationalIssue_11.xml`
3. Repeat the previous step for each team project that will be used in synchronization.

See Also

witAdmin: Administering Objects for Tracking Work Items

How to Configure Whether Files Are Attached or Linked in Synchronization with TFS in System Center 2012 R2

Creating work items in Team Foundation Server (TFS) with large attachments can take a lot of database space. This is why you might want to save the attachments on a network file share and link to these files from the TFS work items rather than physically attaching them to the work items. By default files are saved as links rather than attachments, however, this creates additional requirements for maintaining the files and controlling permissions. If you want to keep attachments in the database, you can override this default and configure TFS integration to

physically attach files and remove them from the network file share. You can also choose to attach the files and keep the files on the network share.

To configure alert attachments to be saved as files that are physically attached to work items in the TFS database

1. In TFS, configure the maximum attachment size for work items to accommodate your business needs. For more information, see How to: Set the Maximum Attachment Size for Work Items.
2. In the Operations Manager console, click **Authoring**, expand **Management Pack Objects**, and then click **Rules**.
3. To set the scope of displayed rules, click **Scope**, and then click **View all targets**. Locate and select **TFS Collection**. Click **OK**.
4. In the list of scoped rules, right-click **Attachments Synchronization Rule**, click **Overrides**, click **Override the Rule**, and then click **For all objects of class: TFS Collection**.
5. Add an override for the parameter **Link as attachments**, and set its value to **True**.

   Important
   Some alert attachments can be very large. For example, a typical production IntelliTrace Historical Profiling snapshot might be several hundred megabytes (MB). When this override is configured, the attachments are stored permanently in the TFS team project database. Make sure you allocate enough storage space for attachments in your database.
6. Save the settings to a management pack.

To configure alert attachments to be saved on the network file share and linked to TFS work items

1. Share access to the alert attachment network file share with developers who need to open these attachments.

   Note
   By default, alert attachments that are synchronized with TFS work items are added as links that point to the alert attachment network file share.
2. In the Operations Manager console, click **Authoring**, expand **Management Pack Objects**, and then click **Rules**.
3. To set the scope of displayed rules, click **Scope**, and then click **View all targets**. Locate and select **TFS Collection**. Click **OK**.
4. In the list of scoped rules, right-click **Attachments Synchronization Rule**, click **Overrides**, click **Override the Rule**, and then click **For all objects of class: TFS Collection**.
5. Add an override for parameter **Link as URL**, and set its value to **True**.

   Important

Some alert attachments can be very large. For example, a typical production IntelliTrace Historical Profiling snapshot might be several hundred megabytes. Make sure you allocate enough storage space on the network file share to meet your business needs.

6. Save the settings to a management pack.

See Also

How to Configure File Attachments for Operations Manager Alerts in System Center 2012 R2

How to Configure Notifications when Developers Reassign Work Items to IT Operations in System Center 2012 R2

As an Information Technology (IT) operator, you need to know when developers request additional information or assign work items back to IT. Receiving notifications when developers make requests helps you respond faster. You can subscribe to get notifications when alerts are set to specific states. For example, you might want to receive notifications when work items are resolved or closed or when an alert is set to Resolved and ready for IT operations. You can configure instant messaging, text messages, email, or custom notifications. For more information about using notifications, see Subscribing to Alert Notifications.

Use the following procedure to configure notifications when developers assign work items to IT operations.

To configure notifications when developers assign work items to IT operations

1. In the Operations Manager console, click **Administration**, expand **Notifications**, and then click **Subscriptions**.
2. In the **Tasks** pane, click **New**.
3. In the Notification Subscription Wizard, enter a new subscription name, and then click **Next**.
4. On the **Criteria** page, in the **Conditions** section, select **with specific resolution state**. In the **Criteria description** section, click the **specific** link. For more information, see How to Specify Which Alerts Generate Notifications (Conditions).
5. In the **Resolution State**, select the resolution state for which you want to receive notifications. For example, if you want to receive notifications when developers request additional information from IT operations, select **Awaiting evidence**. Click **OK**, and then click **Next**.
6. On the **Subscribers** page, to specify recipients of new notifications, click **New**. For details about using the Notification Subscriber Wizard, see How to Create Notification

Subscribers.

7. On the **Channels** page, to configure a new notification channel, such as email, instant message (IM), or text message, click **New**. Or, to search for a previously configured subscription channel, click **Add**. For details about using the Notification Channel Configuration Wizard, see How to Create Notification Subscriptions.
8. Click **Next**, and then click **Finish**.

How to Automatically Assign New Alerts to Engineering in System Center 2012 R2

Through Team Foundation Server (TFS) synchronization, you can establish automatic work item routing for alerts that are raised in System Center 2012 R2 Operations Manager. This can be helpful if your information technology (IT) department uses TFS or if your process model requires that all application alerts must be tracked in TFS. Additionally, you can specify which alert resolution states that are defined in Operations Manager will automatically create work items in TFS.

To route alerts to TFS automatically

1. In the Operations Manager console, click **Authoring**, expand **Management Pack Objects**, and then click **Rules**.
2. To set the scope of displayed rules, click **Scope**, click **View all targets**, locate and select **TFS Connector**, and then click **OK**.
3. In the list of scoped rules, right-click **TFS Work Items Creation Rule**, click **Overrides**, click **Override the Rule**, and then click **For all objects of class: TFS Connector**.
4. Add an override for the parameter **Assign To Engineering State Codes** and set its value to a semicolon-separated list of alert resolution states that route to TFS automatically. For example, to automatically create TFS work items for all new alerts (state 0) and alerts Assigned to Engineering (state 248), in the override value, enter **0;248**.

   Note
   Even though each alert is created as new, you must still list other resolution states that need to route to TFS. This is necessary because an alert can be assigned to engineering in the Operations Manager console before the synchronization workflow has created the work item in TFS.

   In System Center 2012 R2 Operations Manager has the predefined alert resolution states that are described in the following table.

Alert resolution state	Resolution state ID	Description

New	0	New alert
Awaiting Evidence	247	A developer requested additional information from IT operations. With TFS synchronization turned on, this resolution state indicates that the developer has put the Operational Issue work item on hold while waiting for more information. Check the alert history for a Resolution Note from the developer.
Assigned to Engineering	248	The alert is being reviewed by developers. With TFS synchronization turned on, this resolution state initiates the creation of a new Operational Issue work item in TFS.
Acknowledged	249	A developer has received and accepted the Operational Issue work item for this alert. With TFS synchronization turned on, the Alert Owner field shows the current developer to whom the work item is assigned.
Scheduled	250	A fix is scheduled for the problem.
Resolved	254	A problem is resolved from a development perspective. With TFS synchronization turned on, this resolution state indicates that the associated Operational Issue work item is either resolved or closed. The alert might still be generated until

		the updated code is deployed to the operational environment.
Closed	255	The alert is closed.

Note
You can define your own alert resolution states in the Operations Manager console Administration pane.

5. Save the settings to a management pack.

How to Automatically Close Alerts When Work Items Are Resolved in TFS in System Center 2012 R2

Typically, when developers implement and verify a solution for a problem, they resolve and close the related work items in Team Foundation Server (TFS). However, the problem is not fully resolved on the servers until the build containing the solution is actually deployed. Information technology (IT) operators can close the alert in System Center 2012 R2 Operations Manager only when the solution is deployed on the server and the system no longer generates the same type of alert. Because of this, when a work item is closed by a developer, TFS synchronization automatically marks alerts as resolved, not closed. However, you can override the default and have TFS synchronization automatically close alerts when the associated TFS work items are closed.

To automatically close alerts when associated work items are closed

1. In the Operations Manager console, click **Authoring**, expand **Management Pack Objects**, and then click **Rules**.
2. To set the scope of displayed rules, click **Scope** select **View all targets**, locate and select **TFS Collection**, and then click **OK**.
3. In the list of scoped rules, right-click **TFS Work Items Synchronization Rule**, click **Overrides**, click **Override the Rule**, and then click **For all objects of class: TFS Collection**.
4. Add an override for parameter **Auto Close Alerts**, and set its value to **True**.

Note
You can override this rule on a team project collection basis. To do so, when you click **Override the Rule**, override **For a specific object of class: TFS Collection**, and then select the configured TFS collections for which the

associated alerts should be closed. For more information, see How to Override a Rule or Monitor.

5. Save the settings to a management pack.

See Also

How to Configure Integration with TFS in System Center 2012 R2

How to Stop and Resume Synchronization with TFS in System Center 2012 R2

Sometimes you might need to temporarily stop synchronization in System Center 2012 R2 Operations Manager with Team Foundation Server (TFS). For example, this may be necessary when a team project collection is unavailable because of maintenance, during maintenance of management servers in the synchronization management pool, or when you are changing synchronization settings to prevent inconsistent synchronization while new settings are applied. When you know synchronization is not working, turning off synchronization keeps unnecessary alerts about synchronization not working from being generated.

If you need to stop synchronization permanently, you can delete the TFS Work Item Synchronization template for the team project collection that you no longer want to use.

Use the following procedure to temporarily stop synchronization without deleting configuration settings. Use the next procedure to resume synchronization.

Tip
To restart synchronization, you can restart System Center Management service on all management servers in the synchronization pool.

To temporarily stop synchronization without deleting configuration settings

1. To control synchronization, the system uses three independent rules:
   - The TFS Work Items Synchronization Rule
   - The Attachments Synchronization Rule
   - The TFS Work Items Creation Rule

   To temporarily stop synchronization, you must disable all three of these rules. For more information, see How to Override a Rule or Monitor.

   In the Operations Manager console, click **Authoring**, expand **Management Pack Objects**, and then click **Rules**. To scope the displayed rules, click **Scope**, and then click **View all targets**. Look for and then select the **TFS Collection** and **TFS Connector** targets. Click **OK**.
2. To disable the TFS Work Items Synchronization Rule:

a. In the list of scoped rules, expand **TFS Collection**, right-click **TFS Work Items Synchronization Rule**, click **Overrides**, click **Disable the Rule**, and then click **For all objects of class: TFS Collection**.

b. On the **Override Properties** page, override the **Enabled** parameter to **False**, and then save your settings to a management pack.

3. To disable the Attachment Synchronization Rule:

   a. In the list of scoped rules, expand **TFS Collection**, right-click **Attachments Synchronization Rule**, click **Overrides**, click **Disable the Rule**, and then click **For all objects of class: TFS Collection**.

   b. On the **Override Properties** page, override the **Enabled** parameter to **False**, and then save your settings to a management pack.

4. To disable the TFS Work Items Creation Rule:

   a. In the list of scoped rules, expand **TFS Connector**, right-click **TFS Work Items Creation Rule**, click **Overrides**, click **Disable the Rule**, and then click **For all objects of class: TFS Connector**.

   b. On the **Overrides Properties** page, override the **Enabled** parameter to **False**, and then save your settings to a management pack.

To resume synchronization

1. To control synchronization, the system uses three independent rules:
   - The TFS Work Items Synchronization Rule
   - The Attachments Synchronization Rule
   - The TFS Work Items Creation Rule

   To resume synchronization, you must re-enable all three of these rules. For more information about override settings, see How to Override a Rule or Monitor.

2. In the Operations Manager console, click **Authoring**, expand **Management Pack Objects**, and then click **Rules**. To scope the displayed rules, click **Scope**, and then select **View all targets**. Look for and then select the **TFS Collection** and **TFS Connector** targets. Click **OK**.

3. To enable the TFS Work Items Synchronization Rule:

   In the list of scoped rules, expand **TFS Collection**, right-click **TFS Work Items Synchronization Rule**, click **Override Summary**, click the **Enabled** parameter for class TFS Collection, and then click **Delete**. Click **Close**.

4. To enable the Attachments Synchronization Rule:

   In the list of scoped rules, expand **TFS Collection**, right-click **Attachments Synchronization Rule**, click **Override Summary**, click the **Enabled** parameter for class TFS Collection, and then click **Delete**. Click **Close**.

5. To enable the TFS Work Items Creation Rule:

   In the list of scoped rules, expand **TFS Connector**, right-click **TFS Work Items Creation Rule**, click **Override Summary**, click the **Enabled** parameter for class TFS Connector, and then click **Delete**. Click **Close**.

See Also

Applying Overrides to Object Discoveries

How to Change the Frequency of Synchronization for Integration with TFS in System Center 2012 R2

How to Configure File Attachments for Operations Manager Alerts in System Center 2012 R2

Some management packs for Operations Manager attach additional information to alerts. This information is stored as files on the network share, and it is updated by workflows that run on the management servers. Only management servers write to this network share. Other computers in the management group can add attachments to alerts. They do so by uploading files to the management server first. Therefore, these other computers do not need direct access to the file share. Files are uploaded to the management server using the same secure Operations Manager channel that agents use to communicate with the management servers. A separate Run As profile controls the credentials that the management servers use to access the network file share.

Security

As a preliminary action, you must configure file attachments for Operations Manager alerts in System Center 2012 R2. This will enable integration with Team Foundation Server (TFS), IntelliTrace Historical Profiling, sharing Application Performance Monitoring events with developers, Global Service Monitor web tests, and any other scenarios that require files to be associated with Operations Manager alerts.

To configure file attachments for Operations Manager alerts

1. Create an Alert Attachment network file share with enough space to accommodate your anticipated storage needs.

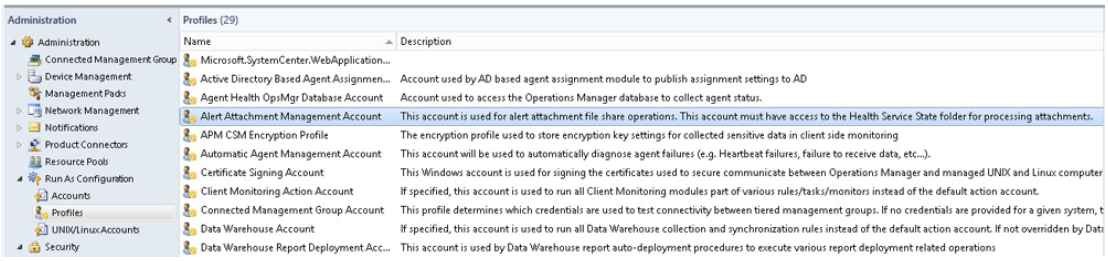
   Important
   Some alert attachments can be very large. For example, a typical production IntelliTrace Historical Profiling snapshot might be several hundred megabytes (MB). Make sure you allocate enough storage space to meet your business needs.

2. Create an active directory account that has read/write permission to the Alert Attachment network file share. Make this account a local administrator on each management server that you plan to use for synchronizing with Team Foundation Server. Make sure that the disk space quota on the network file share does not restrict this account from writing a large amount of information. This account will be used to retrieve the files that are uploaded to the management server and will place those files on the Alert Attachment

network file share.

3. In the Operations Manager console, click the **Administration** button, click **Management Packs**, and then in the **Tasks** pane, click **Import Management Packs**. In the Import Management Packs Wizard, click **Add**, and then click **Add from disk**. Import the Alert Attachment Management Pack (Microsoft.SystemCenter.AlertAttachment.mpb) from the ManagementPacks folder on the System Center 2012 R2 Operations Manager installation media. Click **Install**, and then click **Close**.
4. Configure the Run As profile to use the account that you created for file attachments. In the Operations Manager console, click **Administration**, expand **Run As Configuration**, and then click **Profiles**. Double-click **Alert Attachment Management Account**. Locate and configure the Alert Attachment Management Account for all targeted objects. For more information about using Run As profiles, see Managing Run As Accounts and Profiles.

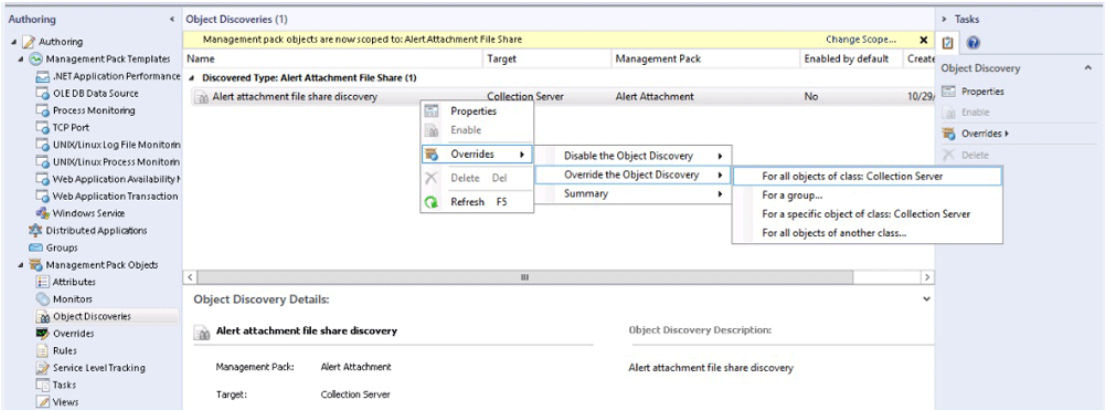
   The location of the Alert Attachment Management Account to be configured



5. Enable the Alert Attachment discovery rule, and configure the override to point to the Alert Attachment file share location. In the Operations Manager console, click **Authoring**, expand **Management Pack Objects**, and then click **Object Discoveries**. To set the object discovery scope, click **Scope**, and then click **View all targets**. Locate and select **Alert Attachment File Share**. Click **OK**.

   In the list of scoped objects, expand **Discovered Type: Alert Attachment File Share**, right-click **Alert attachment file share discovery**, click **Overrides**, click **Override the Object Discovery**, and then click **For all objects of class: Collection Server**.

   Override menus



On the **Override Properties** page, set **Enabled** to **True**, and then set **Path to the alert**

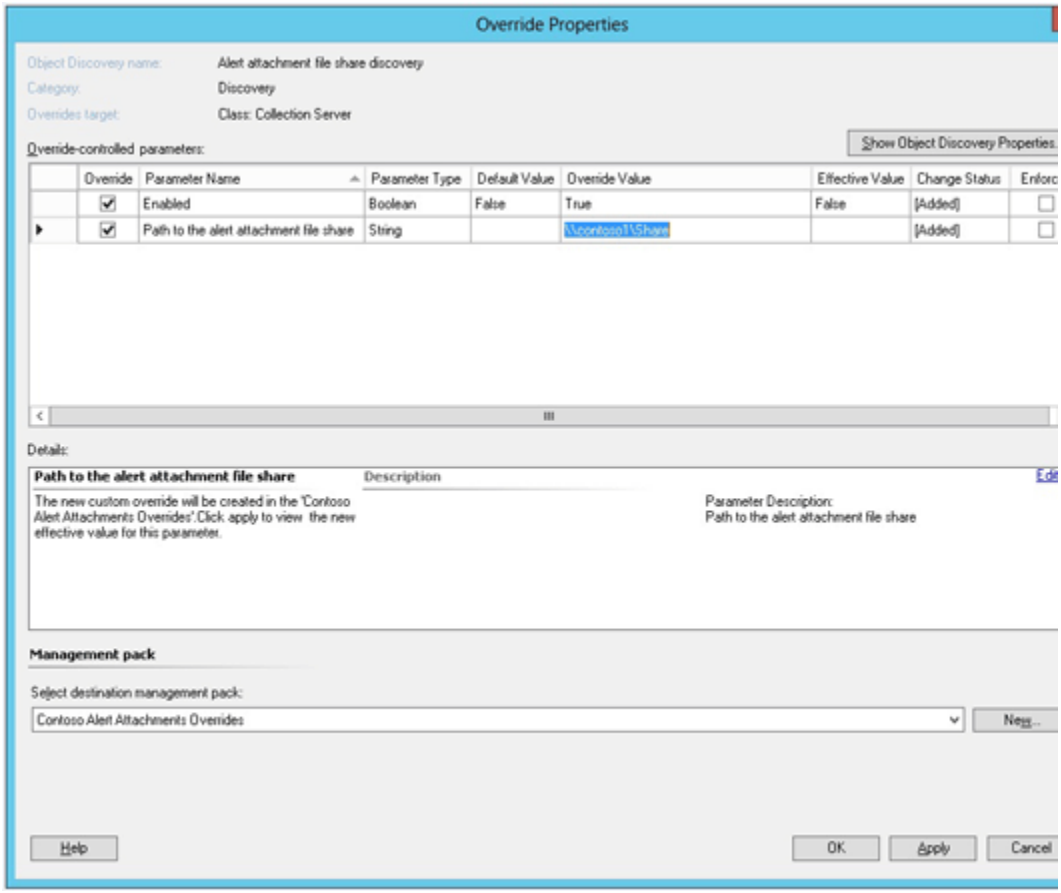
attachment file share to the location of the network file share you created.

Important

You must specify the **Path to the alert attachment file share** in Uniform Naming Convention (UNC) format. For example, this is a valid format: \\contoso1\share. You cannot use a path to a hard drive, such as C:\AttachmentFiles.

In the **Management pack** section, select a target management pack or create a new management pack to save the override values. For more information, see Applying Overrides to Object Discoveries.

Override Properties page



How to Collect IntelliTrace Historical Profiling Traces from System Center 2012 R2

In System Center 2012 R2 Operations Manager, you can use Operations Manager to capture historical snapshots (traces) directly from the Operations Manager console and to receive IntelliTrace snapshots from .NET Application Performance Monitoring (APM) events. These snapshots can help developers investigate problems. They provide visibility to application execution history without needing to access the servers where the problems occurred. Developers can use Microsoft Visual Studio 2012 Ultimate or Microsoft Visual Studio 2013 Preview to open collected snapshots. For information about IntelliTrace for developers, see Debug Your App by Recording Code Execution with IntelliTrace

Snapshots can be accessed from a network file share or from Team Foundation Server (TFS) work item attachments if TFS synchronization is enabled. For more information, see How to Configure Integration with IntelliTrace Historical Profiling in System Center 2012 R2.

Important
After you import and configure the IntelliTrace Profiling management pack, the IntelliTrace tasks are not available until you restart the Operations Manager console.

Collecting IntelliTrace Historical Profiling Snapshots

To collect IntelliTrace snapshots for an existing APM alert

1. You can perform this procedure when you want to keep collected snapshots and attach an IntelliTrace snapshot to an alert. When TFS synchronization is enabled, the collected snapshots are attached or linked to associated work items in TFS.
2. In the Operations Manager console, click **Monitoring**, open an alert view, and then click the alert that you want to investigate.
3. In the **Tasks** pane, expand **IntelliTrace Tasks**, and then click **Start IntelliTrace Collection**.
4. On the **Run Task – Start IntelliTrace** page, in the **Run the task on these targets** section, select the servers from which you want to collect snapshots. The list shows all servers on which the application is configured for monitoring by the APM template in the environment where the alert occurred.
5. In the **Task credentials section**, select **Use the predefined Run As Account** if the Default Action Account has administrative privileges on the application Internet Information Services (IIS) pool. Otherwise, select **Other** to specify credentials that have administrative privileges for this IIS pool.
6. If you want to customize collection parameters, click **Override**.
7. Click **Run**, wait for the task to be completed successfully, and then click **Close**.

Important

When you click **Run**, the application IIS pool automatically recycles on all of the servers that you selected in the **Run the task on these targets** section. APM turns off for all applications that are running in the same application pool.

8. Reproduce the application problem that resulted in the APM exception alert.
9. Select the same alert on which you started IntelliTrace. In the **Tasks** pane, click **Collect IntelliTrace Snapshot**.
10. On the **Run Task – Collect IntelliTrace Snapshot** page, select the same servers and same **Task credentials** that you previously selected when you started IntelliTrace collection.
11. Click **Run**, wait for the task to be completed successfully, and then click **Close**. The task output indicates whether any problems occurred while running the IntelliTrace collector tasks.
12. To collect multiple snapshots, repeat the previous four steps. All snapshots that you collect are attached to the same APM alert.
13. To stop IntelliTrace collection, select the same alert on which you started IntelliTrace. In the **Tasks** pane, click **Stop IntelliTrace Collection**.

    Important

    Be sure to stop IntelliTrace collection. If you do not stop IntelliTrace collection, IntelliTrace will continue to run. This will impact application performance, and APM will remain off so that you will not receive new alerts from this application. To stop IntelliTrace when the alert is already closed and no longer shows in the Operations Manager console, complete the step from the subsequent procedure that stops IntelliTrace: To collect IntelliTrace snapshots when there are no APM exception alerts
14. To see the IntelliTrace snapshots that are attached to an alert, select the alert. In the **Tasks** pane, click **Open Snapshot Location**.
15. If TFS synchronization is turned on, you can assign an alert to engineering. To do so, set the alert resolution state to **Assigned to Engineering**. This creates a new work item in TFS, with the snapshot attached or linked. For more information, see How to Configure Integration with TFS in System Center 2012 R2.

To collect IntelliTrace snapshots when there are no APM alerts

1. You can perform this procedure when you are investigating problems with application logic, poor performance (when performance alerting on particular SLA violations is not turned on), or when APM is not enabled for an application. The subject application in this procedure must be discovered by the IIS management packs.
2. In the Operations Manager console, click **Monitoring**, expand **Application Monitoring**, and then expand **.NET Monitoring**.
3. If your application is running on Windows Server 2008 R2, click **IIS 7.0 ASP .NET Web Application Inventory**. If your application is running on Windows Server 2012, click **IIS**

8.0 ASP .NET Web Application Inventory.

4. Select the application pool on which you want to run IntelliTrace profiling.
5. In the **Tasks** pane, expand **IntelliTrace Tasks**, and then click **Start IntelliTrace Collection**.
6. On the **Run Task – Start IntelliTrace** page, in the **Run the task on these targets** section, select the application pool in which you want to collect snapshots.
7. In the **Task credentials section**, select **Use the predefined Run As Account** if the Default Action Account has administrative privileges on the application IIS pool. Otherwise, select **Other** to specify alternative credentials that have administrative privileges for this IIS pool.
8. If you want to customize collection parameters, click **Override**.
9. Click **Run**, wait for the task to be completed successfully, and then click **Close**.

   Important
   When you click **Run**, the application IIS pool automatically recycles on all of the servers that you selected in the **Run the task on these targets** section. APM turns off for all applications that are running in the same application pool.
10. Run your application and reproduce the behavior that you want to investigate.
11. Select the same application pool on which you started IntelliTrace. In the **Tasks** pane, click **Collect IntelliTrace Snapshot**.
12. On the **Run Task – Collect IntelliTrace Snapshot** page, select the same target and same **Task credentials** that you previously selected when you started IntelliTrace collection.
13. Click **Run**, wait for the task to be completed successfully, and then click **Close**. The task output indicates whether any problems occurred while running the IntelliTrace collector tasks.
14. To collect multiple snapshots, repeat the previous four steps. For each snapshot that you collected, you will receive a new informational alert when the snapshot is uploaded to the network file share.
15. To stop IntelliTrace collection, select the same application pool on which you started IntelliTrace. In the **Tasks** pane, click **Stop IntelliTrace Collection**.

    Important
    Be sure to stop IntelliTrace collection. If you do not stop IntelliTrace collection, IntelliTrace will continue to run. This will impact application performance and APM will remain off so that you will not receive new alerts from this application.
16. To see the IntelliTrace snapshots, in the Operations Manager console, click **Monitoring**, expand **IntelliTrace Profiling**, and then click **New Alerts**. The **New Traces** pane shows an alert for each snapshot that you have collected.
17. In the **Tasks** pane, expand **Alert Attachment Tasks**, and then click **Open Attachment Location**.
18. If TFS synchronization is turned on, you can assign an alert to engineering. To do so, set the alert resolution state to **Assigned to Engineering**. This creates a new work item in

TFS with the snapshot attached or linked. For more information, see How to Configure Integration with TFS in System Center 2012 R2.

To access IntelliTrace snapshots that are generated from APM data

1. You can perform this procedure when you want to investigate an existing APM performance or exception alert that is based solely on historical data without having to run IntelliTrace Profiling on your application.
2. In the Operations Manager console, click **Monitoring**, open an alert view, and then click the alert that you want to investigate.
3. In the **Tasks** pane, expand **Alert Attachment Tasks**, and then click **Open Attachment Location**. Windows Explorer opens the location of the files that are attached to the alert you have selected.
4. To see the IntelliTrace snapshot for this alert, in Windows Explorer, open the **APMException** folder.
5. If TFS synchronization is turned on, you can assign this alert to engineering. To do so, set the alert resolution state to **Assigned to Engineering**. This creates a new work item in TFS, with the snapshot attached or linked. For more information, see How to Configure Integration with TFS in System Center 2012 R2.

How to Configure Integration with IntelliTrace Historical Profiling in System Center 2012 R2

System Center 2012 R2 Operations Manager includes the IntelliTrace Profiling Management Pack. This management pack lets you capture historical snapshots (traces) directly from the Operations Manager console, and to automatically generate IntelliTrace snapshots from .NET Application Performance Monitoring (APM) events. These snapshots can help developers investigate problems by giving them visibility to application execution history without the developers needing access to the servers where the applications ran. Developers can use Microsoft Visual Studio 2012 Ultimate or Microsoft Visual Studio 2013 Preview to open the collected snapshots. For information about IntelliTrace for developers, see Debug Your App by Recording Code Execution with IntelliTrace

IntelliTrace Profiling Management Pack in System Center 2012 R2 Operations Manager uses a built-in feature of Microsoft Monitoring Agent (MMA) for collecting application historical snapshots (traces). The collected snapshots are uploaded to a network file share and attached to Operations Manager alerts. Snapshots are uploaded to the management server using the same secure Operations Manager channel that agents use to communicate with the management servers. You can configure Team Foundation Server (TFS) synchronization so that the IntelliTrace snapshots will be automatically added or linked to TFS work items. For more information, see How to Configure Integration with TFS in System Center 2012 R2.

Important

In System Center 2012 SP1 Operations Manager IntelliTrace Collector was deployed to the monitored servers as a separate package by the IntelliTrace Collector Management Pack. If your Operations Manager environment was upgraded from System Center 2012 SP1 to Operations Manager and you imported System Center 2012 SP1 versions of the IntelliTrace management packs, to continue to collect IntelliTrace information, you must remove the IntelliTrace Collector Deployment Management Pack and update Alert Attachment Management Pack and IntelliTrace Profiling Management Pack with the versions included in System Center 2012 R2 Operations Manager. Additionally, you must upgrade the Operations Manager agent to Microsoft Monitoring Agent on each monitored server where you want to collect historical snapshots or automatically generate IntelliTrace snapshots from APM events.

Caution

IntelliTrace snapshots contain application runtime data that might include personal and sensitive information. Review your company's privacy policies before you enable this feature.

To configure integration with IntelliTrace Historical Profiling

1. Import and configure the Alert Attachment Management Pack. This management pack links the collected IntelliTrace snapshots to Operations Manager alerts. For more information, see How to Configure File Attachments for Operations Manager Alerts in System Center 2012 R2.
2. If you want to synchronize IntelliTrace snapshots with TFS work items, import and configure the TFS Work Item Synchronization Management Pack. When snapshots are synchronized with work items, developers can receive IntelliTrace snapshots with TFS work items in Visual Studio. Additionally, developers can set work item state to **Awaiting Evidence** and use TFS to submit requests to capture IntelliTrace snapshots. For more information, see How to Configure Integration with TFS in System Center 2012 R2.

   Note

   You can use IntelliTrace snapshots without TFS integration. If you do so, the IntelliTrace snapshots are not attached to work items, but they are uploaded to the Alert Attachment network file share instead.
3. In the Operations Manager console, click the **Administration** button, click **Management Packs**, and then, in the **Tasks** pane, click **Import Management Packs**. In the Import Management Packs Wizard, click **Add**, and then click **Add from disk**. Import IntelliTrace Profiling (Microsoft.SystemCenter.IntelliTraceProfiling.mpb) from the ManagementPacks folder on the System Center 2012 R2 Operations Manager installation media.

   Click **Install**, and then click **Close**.

   Important

   The IntelliTrace tasks are not available until you restart the Operations Manager

console.

How to Synchronize Alerts with TFS in System Center 2012 R2

In System Center 2012 R2 Operations Manager, you can synchronize Operations Manager alerts and Team Foundation Server (TFS) work items. When synchronization is enabled, IT operations can then assign alerts to the engineering team. Assigning an alert to engineering creates a new work item in TFS. The workflow will track and synchronize any changes that are made to TFS work items and any associated Operations Manager alerts. In order to synchronize alerts with TFS, you must first configure alert synchronization. For more information, see How to Configure Integration with TFS in System Center 2012 R2.

Note

Integration between System Center 2012 SP1 and TFS used the Ticket ID and Owner fields of the Operations Manager alert to store and display which work item is associated with an alert and who it is assigned to. Beginning in System Center 2012 R2 Operations Manager, two new alert fields, TFS Work Item ID and TFS Work Item Owner, hold these values. These fields are read-only in the Operations Manager console to prevent accidental changes of the values that are controlled in TFS.

If you previously personalized any standard alert views or created your own alert views in System Center 2012 SP1 using Ticket ID and Owner fields to display TFS information, you must replace those fields with the TFS Work Item ID and TFS Work Item Owner fields to continue displaying the same information. The previous Ticket ID and Owner fields are still used for synchronization of alerts with incidents in Service Manager Alert Connector.

To assign alerts to engineering

1. In the Operations Manager console, you can view all application problems that have been collected. To view alerts in Operations Manager, in the navigation pane, click **Monitoring**, and then click **Active Alerts**.
2. To assign an alert to engineering, right-click the alert, select **Set Resolution State**, and select **Assigned to Engineering**. This action creates a TFS work item and adds the TFS work item ID to the alert.
3. The system synchronizes all changes to the alert inside Operations Manager and all changes to the work item in TFS.

   Tip

   Any comments that you add to an Operations Manager alert on the alert **History** tab are automatically added to the corresponding TFS work items. You can use

this function to provide additional information to engineering.

To review alerts that are awaiting evidence from engineering

1. In the Operations Manager console, you can view all application problems that have been collected. To view alerts in Operations Manager, in the navigation pane, click **Monitoring**, expand **Team Foundation Server Synchronization**, expand **Alerts**, and then click **Awaiting Evidence**.

To review and close alerts that have been resolved by engineering

1. In the Operations Manager console, you can view all application problems that have been collected. To view alerts in Operations Manager, in the navigation pane, click **Monitoring**, expand **Team Foundation Server Synchronization**, expand **Alerts**, and then click **Resolved**.
2. When you want to close the resolved alerts, you can right-click an alert, select **Set Resolution State**, and then set the resolution state to **Closed**.

Monitoring Integration between Operations Manager and TFS in System Center 2012 R2

Synchronization between Operations Manager and Team Foundation Server (TFS) makes efficient communication possible between information technology (IT) operations and developers. A healthy TFS environment is essential for all development processes. Depending on your environment, you can import TFS monitoring and management packs that give you real-time visibility into the health of the TFS developer environment.

The TFS Work Item Synchronization management pack synchronizes Operations Manager alerts and TFS work items. Additionally, it monitors the synchronization infrastructure, and it generates alerts when synchronization fails. However, to monitor the complete TFS infrastructure, you need additional monitoring packs that alert you about a wide range of problems with TFS components. When you import the TFS Work Item Synchronization management pack, it is a best practice to also import and configure these monitoring packs. Together, they help you make sure that you are monitoring the complete health of the developer TFS environment.

Management and Monitoring Packs to Use with TFS Integration

Use the management packs and monitoring packs in the following table for TFS integration.

Management Pack	Description	Use with …	Where to get it
Microsoft Visual Studio 2010 Team Foundation Server Monitoring Management Pack for Microsoft System Center	Monitors TFS infrastructure. Provides both proactive and reactive monitoring of Microsoft Team Foundation Server 2010. Monitors TFS components, such as application tier server instances, team project collections, build servers, and proxy servers.	• Microsoft Team Foundation Server 2010 • Operations Manager 2007 R2 • System Center 2012 – Operations Manager • Operations Manager in System Center 2012 Service Pack 1 (SP1)	Microsoft Download Center
Microsoft Visual Studio 2012 Team Foundation Server Monitoring Management Pack for Microsoft System Center	Monitors TFS infrastructure. Provides both proactive and reactive monitoring of Microsoft Team Foundation Server 2012. Monitors TFS components, such as application tier server instances, team project collections, build servers, and proxy servers.	• Microsoft Team Foundation Server 2012 • Operations Manager 2007 R2 • System Center 2012 – Operations Manager • Operations Manager in System Center 2012 SP1 • System Center 2012 R2 Operations Manager	Microsoft Download Center
System Center Management Pack for Microsoft Visual Studio Team Foundation Server 2010 Work Item Synchronization	Provides synchronization with Microsoft Team Foundation Server 2010. Monitors its own synchronization infrastructure only. Use this if you are running System Center 2012 – Operations Manager	• Microsoft Team Foundation Server 2010 • System Center 2012 – Operations Manager • Operations Manager in System Center	Microsoft Download Center

Management Pack	Description	Use with …	Where to get it
	without SP1.	2012 SP1 • System Center 2012 R2 Operations Manager	
Team Foundation Server Work Item Synchronization Management Pack	Provides synchronization with Microsoft Team Foundation Server 2010 and Microsoft Team Foundation Server 2012. Monitors its own synchronization infrastructure only.	• Microsoft Team Foundation Server 2010 • Microsoft Team Foundation Server 2012 • Operations Manager in System Center 2012 SP1 • System Center 2012 R2 Operations Manager	• Operations Manager in System Center 2012 SP1 media • System Center 2012 R2 Operations Manager media

Note

If your environment contains TFS 2010 and TFS 2012, you can use both monitoring packs together (Microsoft Visual Studio 2010 Team Foundation Server Monitoring Management Pack for Microsoft System Center and Microsoft Visual Studio 2012 Team Foundation Server Monitoring Management Pack for Microsoft System Center). Also, you can use these management packs without enabling synchronization between Operations Manager alerts and TFS work items to get visibility into the health of the TFS environment.

See Also

How to Configure Integration with TFS in System Center 2012 R2

Integrating Operations Manager with Development Processes in System Center 2012 SP1

Streamlining the communications between development and information technology (IT) operations teams (often called DevOps) can help you decrease the time it takes for application maintenance and delivery into production, where your application delivers value to customers. To speed interactions between these teams, it is essential to quickly detect and fix problems that might need assistance from the engineering team.

The topics in this section can help you integrate System Center 2012 – Operations Manager with development tools, such as Team Foundation Server (TFS) and Visual Studio. This integration enables deep troubleshooting and provides greater efficiency between development and IT operations teams.

Integrating Operations Manager with Development Processes (DevOps) Topics

- How to Configure Integration with TFS in System Center 2012 SP1

  You can synchronize System Center 2012 – Operations Manager alerts and TFS work items. When synchronization is enabled, IT operations can assign alerts to the engineering team.
- How to Configure File Attachments for Operations Manager Alerts in System Center 2012 SP1

  You will need to configure file attachments for Operations Manager alerts. Proper configuration enables integration with TFS, IntelliTrace Historical Profiling, sharing Application Performance Monitoring events with developers, Global Service Monitor web tests, and any other scenarios that require files to be associated with Operations Manager alerts.
- How to Synchronize Alerts with TFS in System Center 2012 SP1

  TFS lets you configure engineering process templates. Operations Manager integration with TFS introduces a new "Operational Issue" work item type definition that can be embedded into any of your organization’s engineering processes.
- How to Configure Integration with IntelliTrace Historical Profiling in System Center 2012 SP1

  You can help developers to debug applications by collecting IntelliTrace snapshots directly from Operations Manager. When TFS and Operations Manager are integrated, these snapshots can be automatically attached to TFS work items.
- How to Collect IntelliTrace Historical Profiling Traces from System Center 2012 SP1

  After configuring integration with IntelliTrace, you can collect and share IntelliTrace snapshots with developers.
- Monitoring Integration between Operations Manager and TFS in System Center 2012 SP1

Depending on your environment, you can import TFS monitoring and management packs that give you real-time visibility into the health of the TFS developer environment.

How to Configure Integration with TFS in System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

If you need to synchronize with System Center 2012 without Service Pack 1 (SP1), you can use TFS Work Item Synchronization Management Pack for Team Foundation Server (TFS) 2010. To download the management pack and the guide, see System Center Management Pack for Microsoft Visual Studio Team Foundation Server 2010 Work Item Synchronization.

In System Center 2012 SP1, you can synchronize Operations Manager alerts and TFS work items. After enabling synchronization, information technology (IT) operations can assign alerts to the engineering team. When you first assign an alert to engineering, TFS creates a new work item. The workflow then tracks and synchronizes changes that are made to TFS work items and changes that are made to associated Operations Manager alerts. You can synchronize alerts with team projects in TFS 2012, TFS 2010, or both.

Important

Before you enable configuration, you must have TFS administrator credentials to be able to import the Operational Issue Work Item Type Definition that is used by integration with TFS. Additionally, you must have a configured domain account with TFS contributor rights in the team projects that you want to synchronize Operations Manager alerts with.

To prepare your environment for synchronization with TFS

1. Import and configure the Alert Attachment Management Pack. For more information, see How to Configure File Attachments for Operations Manager Alerts in System Center 2012 SP1.
2. Decide which management servers you want to use to synchronize Operations Manager alerts and TFS work items. Each management server that is used for synchronization must have TFS Object Model installed. You can install the TFS Object Model for TFS 2010 from the MSDN Download Center (Team Foundation Server 2010 SP1 Object Model Installer) or by installing the TFS Object Model for TFS 2012 from the MSDN Download Center (Team Foundation Server 2012 Update 1 Object Model Installer). You can also install the TFS Object Model for TFS 2012 when you install Visual Studio 2012. Installing TFS on a server also installs the TFS Object Model on that server.

   Note

   Either version of the TFS Object Model can be used for synchronization with either version of TFS. However, in order to synchronize with TFS 2012 using TFS Object Model 2010, you must manually import the Operational Issue work item type definition (WITD) into each team project that will be used for

synchronization. Do this by using the **witadmin** command-line tool. For more information about manually importing the Operational Issue WITD, see How to Manually Import an Operational Issue WITD to TFS in System Center 2012 SP1.

Tip
Installing synchronization on all management servers in the management group will help to simplify maintenance and bring redundancy into the integration between Operations Manager and TFS.

3. Create a domain account that will be used for TFS synchronization.
4. Give this domain account TFS contributor permissions for each project that you plan to use for TFS synchronization. For more information, see Add Users to Team Projects.
5. If you intend to synchronize alert file attachments with TFS work items, give this account read/write access to the Alert Attachment file share. This is the file share that was established when you configured the Alert Attachment Management Pack.

To configure synchronization for the TFS Work Item Synchronization Management Pack

1. Import the TFS Work Item Synchronization Management Pack from the Operations Manager installation media. In the Operations Manager console, click **Administration**, click **Management Packs**, and then, in the **Tasks** pane, click **Import Management Packs**. In the Import Management Packs Wizard, click **Add**, and then click **Add from disk**. Import the TFS Work Item Synchronization Management Pack (Microsoft.SystemCenter.TFSWISynchronization.mpb) from the ManagementPacks folder on the Operations Manager installation media. Click **Install**, and then click **Close**.
2. To begin configuring the TFS Work Item Synchronization Management Pack, in the Operations Manager console, in the navigation pane, click **Authoring**, click **Management Pack Templates**, and then, in the **Tasks** pane, click **Add Monitoring Wizard**.

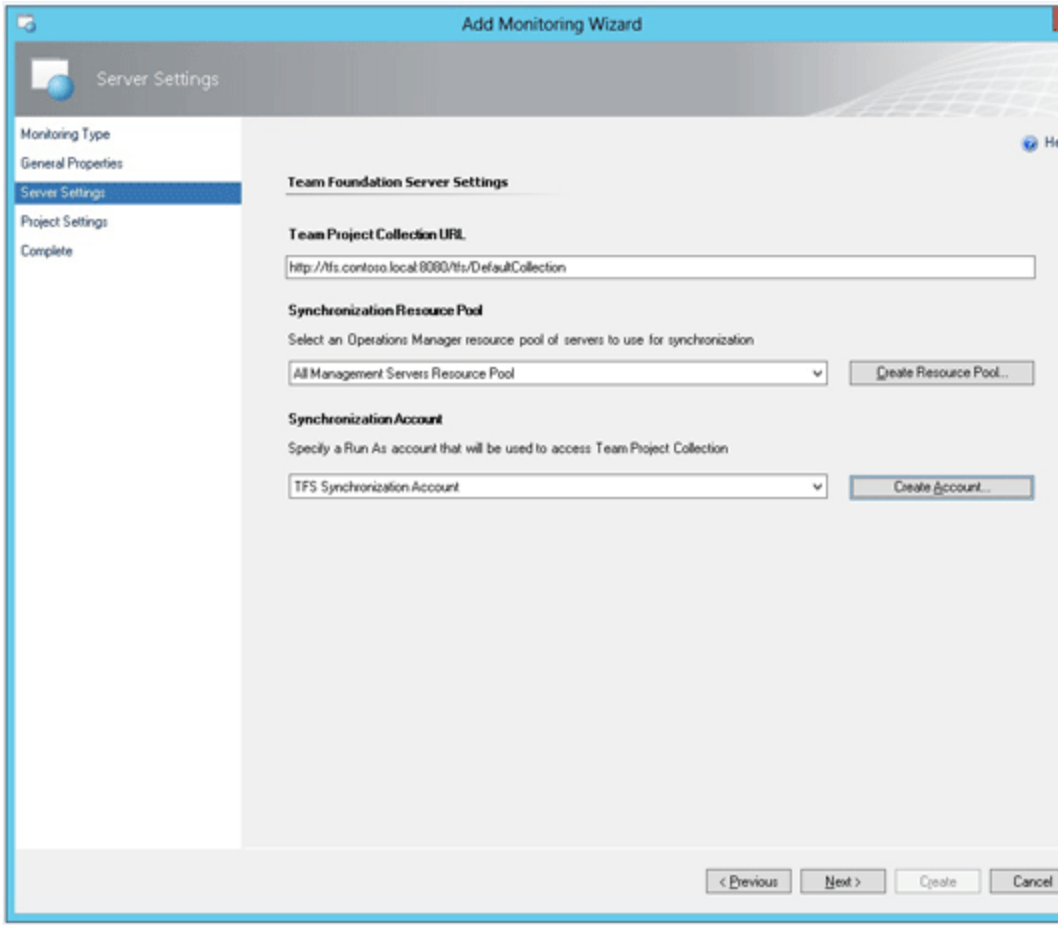
   Important
   You must run the Add Monitoring Wizard for each team project collection that you want to synchronize alerts with.
3. To open the TFS Work Item Synchronization template, in the Add Monitoring Wizard, on the **Monitoring Type** page, select **TFS Work Item Synchronization**.
4. On the **General Properties** page, type a display name for this team project collection and a description, and then select a target management pack to store your configuration settings.
5. On the **Server Settings** page, enter the **Team Project Collection URL** (for example: http://tfs.contoso.local:8080/tfs/DefaultCollection/), and then select the **Synchronization Resource Pool** of the management servers that are used for load-balancing synchronization. Each server in this resource pool must already have the TFS Object Model installed. Then, create or select a Run As account that will be used for synchronization. This Run As account must have contributor permissions in each TFS team project. If you want to synchronize alert file attachments, the Run As account must have read/write access to the Alert Attachment file share. Make sure that these

credentials are distributed to all management servers that are used for synchronization. For more information about using Run As profiles, see Managing Run As Accounts and Profiles.

Note

You can get the TFS Team Project Collections URL from the Team Foundation Server Administration Console. If the TFS Team Project Collection that you choose is offline or otherwise unavailable, the wizard will warn you, but it will still let you finish the configuration. Additionally, when TFS is not available, there is no validation for your input in the wizard. The team project and area path will not be prepopulated with existing values.

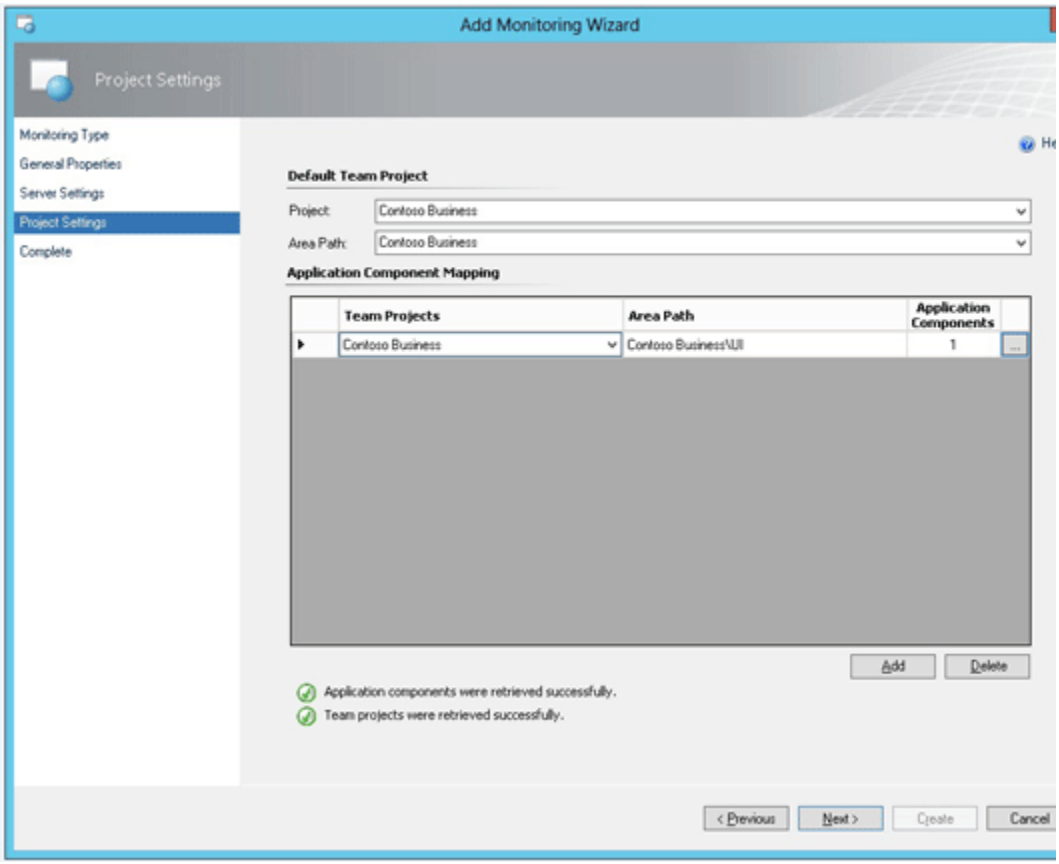
Server Settings page



6. On the **Project Settings** page, specify the **Project** and **Area Path** that will be used to synchronize all alerts. You can customize these settings for each .NET application component that was previously configured for monitoring with .NET Application Performance Monitoring (APM). To customize the team project and TFS area path for an APM component, click **Add**, which will add a new row. Choose a target **Team Project** and **Area Path** combination, and then click the (**…**) button to select which configured

application components will synchronize with this team project and area path. The application components must already be configured for monitoring with the .NET Application Performance Monitoring template. For more information, see .NET Application Performance Monitoring Template.

Project Settings page



Note

You can configure synchronization with multiple Team Foundation Servers or multiple Team Project Collections by running the configuration wizard multiple times. However, only one configuration can have the **Default Team Project** and **Default Area Path** specified.

7. When you finish the wizard, you will be asked for TFS administrator credentials so that the wizard can automatically import the Operational Issue WITD to each team project that is used in the configured synchronization. You can skip this step if you want to manually import the Operational Issue WITD. You must manually import the WITD when you are synchronizing with Team Foundation Server 2012 using TFS Object Model 2010. For more information, see How to Manually Import an Operational Issue WITD to TFS in System Center 2012 SP1.

Note

After you configure synchronization, the TFS Work Item Synchronization management pack will monitor the synchronization infrastructure, and it will generate alerts if synchronization fails. However, to monitor the complete TFS infrastructure, you need additional monitoring packs that can alert you about a wide range of potential problems with TFS components. When you import the TFS Work Item Synchronization management pack, you should also import and configure these monitoring packs. Together, they help you make sure that you are monitoring the complete health of the developer TFS environment. For more information, see Monitoring Integration between Operations Manager and TFS in System Center 2012 SP1.

Changing Synchronization Settings

You can view or change synchronization settings for the TFS Work Item Synchronization Management Pack. You will need to change these settings to modify a destination team project and area path or to customize synchronization rules for a monitored .NET application component.

To prevent inconsistent synchronization while new settings are being applied, turn off synchronization before you change the configuration. For information about stopping and resuming synchronization, see How to Stop and Resume Synchronization with TFS in System Center 2012 SP1. The process of replicating configuration changes to all management servers in the synchronization pool might take an hour or more, depending on the system performance of your management group. After the replication is complete, you can turn synchronization on again. If the configuration was changed while synchronization was running, you might have to force a reset of the configuration by restarting the System Center Management Service on all management servers in the synchronization pool.

If you change a destination team project for synchronization, the rules in the following table apply.

Changes in TFS team project location	How synchronization is affected
An application is mapped to a new TFS project within the same TFS project collection.	New alerts go to the new project and old alerts keep synchronizing with the old project. If you delete old ticket IDs and reassign the related alerts to engineering, new work items are created in the new project. These new work items are not linked to any of the pre-existing work items.
An application is mapped to a new TFS project within the same TFS server, but in a different TFS project collection.	New alerts go to the new TFS project. The old alerts stop synchronizing completely. If you delete old ticket IDs and reassign the related alerts to engineering, new work items are created. These new work items are not linked to any of the pre-existing work items.

Changes in TFS team project location	How synchronization is affected
An application is mapped to a project on a different server.	New work items are created for alerts that are newly assigned to engineering. Synchronization of any previously synchronized alerts stops.

To change synchronization settings

1. To change synchronization settings, in the Operations Manager console, in the navigation pane, click **Authoring**, expand **Management Pack Templates**, and then click **TFS Work Item Synchronization**.
2. Locate a previously configured team project collection, and in the **Tasks** pane, click **Properties**.

   Note
   If you recently changed configuration and the change has not been replicated to the management servers, you must wait for the changes to be replicated before you can view and work with the new configuration. The replication of configuration changes to all management servers in the synchronization pool might take an hour or more, depending on the system performance of your management group.
3. On the **Server Settings** tab, you can change the **Synchronization Resource Pool** of the management servers that are used for load-balancing synchronization. Each server in this resource pool must already have the TFS Object Model installed. Also, you can change the Run As account that will be used for synchronization. This account must have contributor permissions in each TFS team project, and, if you want to synchronize alert file attachments, the account must have read/write access to the Alert Attachment file share. Make sure that these credentials are distributed to all management servers that are used for synchronization. For more information about using Run As profiles, see Managing Run As Accounts and Profiles.

   Note
   If you need to change the Team Project Collection URL, you must delete the configuration and run the wizard again.
4. On the **Project Settings** tab, specify the **Default Team Project** and **Default Area Path** that will be used to synchronize all alerts. You can customize these settings for each .NET application component that was previously configured for monitoring with .NET Application Performance Monitoring (APM). To customize the team project and TFS area path for an APM component, click **Add** to add a new row. Choose a target **Team Project** and **Area Path** combination, and then click the (**…**) button to select which configured application components will synchronize with this team project and area path. The application components must already be configured for monitoring with the .NET Application Performance Monitoring template. For more information, see .NET Application Performance Monitoring Template.

Note
To configure synchronization with multiple Team Foundation Servers or multiple Team Project Collections, you can run the configuration wizard multiple times. However, only one configuration can have the **Default Team Project** and **Default Area Path** specified.

5. Click **OK**.
6. If you added a new team project to synchronize with, you will be asked for TFS administrator credentials so that the wizard can automatically import the Operational Issue WITD to the new team project that is used in the configured synchronization. You can skip this step if you want to manually import the Operational Issue WITD. You must manually import the WITD when you are synchronizing with TFS 2012 using TFS Object Model 2010. For more information, see How to Manually Import an Operational Issue WITD to TFS in System Center 2012 SP1.

Procedures Related to Configuring Integration with TFS

For additional information, see the following procedures related to configuring integration with TFS in System Center 2012 Service Pack 1 (SP1):

- How to Change the Frequency of Synchronization for Integration with TFS in System Center 2012 SP1
- How to Manually Import an Operational Issue WITD to TFS in System Center 2012 SP1
- How to Configure Whether Files Are Attached or Linked in Synchronization with TFS in System Center 2012 SP1
- How to Configure Notifications when Developers Reassign Work Items to IT Operations in System Center 2012 SP1
- How to Automatically Assign New Alerts to Engineering in System Center 2012 SP1
- How to Automatically Close Alerts When Work Items Are Resolved in TFS in System Center 2012 SP1
- How to Stop and Resume Synchronization with TFS in System Center 2012 SP1

How to Change the Frequency of Synchronization for Integration with TFS in System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

In System Center 2012 SP1, synchronizing Operations Manager alerts and work items is key to working effectively and efficiently with your development team. When you assign an alert to engineering, the matching work item in Team Foundation Server (TFS) will not be created immediately. The synchronization frequency is controlled by overrides in the Operations Manager TFS Work Item Synchronization management pack

(Microsoft.SystemCenter.TFSWISynchronization.mpb). To change the synchronization frequency, you can change the overrides listed in the following table.

Override description	Target object	Rule	Parameter	Default Value
How often new TFS work items are created from alerts assigned to Engineering	TFS Connector	TFS Work Items Creation Rule	Interval Seconds	300 seconds
How often alerts assigned to Engineering and their associated TFS work items are synchronized	TFS Collection	TFS Work Items Synchronization Rule	Interval Seconds	900 seconds
How often alert attachments are added from the network file share to TFS work items	TFS Collection	Attachments Synchronization Rule	Interval in Seconds	900 seconds
The time range of the TFS work item history that will be synchronized with the alerts. For example, the default value of 24 means that changes that are made to a TFS work item only during the past 24 hours will be synchronized. With that setting, this parameter is important if synchronization is turned off for more than 24 hours, which might create a gap in the alert	TFS Collection	TFS Work Items Synchronization Rule	Delta in Hours	24 hours

Override description	Target object	Rule	Parameter	Default Value
history that reflects the associated TFS work item history after synchronization is turned back on. The synchronization cycle is always shorter than Delta in hours when synchronization constantly stays on. This guarantees that complete work item history is synchronized if at least one synchronization cycle has occurred during the past 24 hours.				
How often the APM alerts will receive converted IntelliTrace logs. The value is defined in minutes.	IntelliTrace attachments for APM alerts singleton object	Add IntelliTrace as an APM attachment rule	IntelliTrace conversion data source polling interval	15 minutes

Caution
Setting the override frequencies too low might add substantial load to your management servers and TFS.

To change the frequency of synchronization

1. Using the table above, find the override parameter that you want to change.
2. In the Operations Manager console, click **Authoring**, expand **Management Pack Objects**, and then click **Rules**. To set the scope of displayed rules, click **Scope**, and then select **View all targets**. Locate and select **TFS Collection** and **TFS Connector**. Click **OK**.

   Important

If you are using IntelliTrace, you must also select **IntelliTrace attachments for APM alerts singleton object**.

3. In the list of scoped rules, right-click the rule with the parameter that you want to override. Click **Overrides**, click **Override the Rule**, and then click **For all objects of class**.
4. Override the parameter to a new value, and save the settings to a management pack.

See Also

How to Override a Rule or Monitor

How to Manually Import an Operational Issue WITD to TFS in System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

In System Center 2012 Service Pack 1 (SP1), Operations Manager integration with Team Foundation Server (TFS) introduces a new work item type, *Operational Issue*, which must be present in each team project that synchronization uses. Generally, the TFS Work Item Synchronization Configuration Wizard can import this work item type definition (WITD). In some cases, however, you must manually import the WITD directly to TFS. You must manually import the Operational Issue WITD in the following cases:

- A separate TFS administrator controls the development process model in TFS.
- You are running the TFS 2010 Object Model to integrate with TFS 2012.
- An external procedure has removed the Operational Issue WITD from the team projects in TFS, and you still want to synchronize with this team project.

Caution

The Operational Issue work item type should not be renamed. Renaming this work item type breaks synchronization. Any modifications to this work item type will be overridden when you change configuration settings. This might cause problems with synchronization.

To manually import the Operational Issue WITD file

1. Locate the correct Operational Issue WITD for your version of TFS on the installation media for Operations Manager in System Center 2012 SP1 in the **SupportTools** folder. For TFS 2010, the file name is OperationalIssue.xml. For TFS 2012, the file name is OperationalIssue_11.xml.
2. Use TFS administrator credentials to run the **witadmin** command-line tool in TFS and import the Operational Issue WITD to each TFS project you plan to use with synchronization.

   Example for TFS 2010: `witadmin importwitd`

```
/collection:http://tfs.contoso.com:8080/tfs /p:ProjectName /f:OperationalIssue.xml
```

Example for TFS 2012: `witadmin importwitd /collection:http://tfs.contoso.com:8080/tfs /p:ProjectName /f:OperationalIssue_11.xml`

3. Repeat the previous step for each team project that will be used in synchronization.

See Also

witAdmin: Administering Objects for Tracking Work Items

How to Configure Whether Files Are Attached or Linked in Synchronization with TFS in System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

Creating work items in Team Foundation Server (TFS) with large attachments can take a lot of database space. This is why you might want to save the attachments on a network file share and link to these files from the TFS work items rather than physically attaching them to the work items. By default files are saved as links rather than attachments, however, this creates additional requirements for maintaining the files and controlling permissions. If you want to keep attachments in the database, you can override this default and configure TFS integration to physically attach files and remove them from the network file share. You can also choose to attach the files and keep the files on the network share.

To configure alert attachments to be saved as files that are physically attached to work items in the TFS database

1. In TFS, configure the maximum attachment size for work items to accommodate your business needs. For more information, see How to: Set the Maximum Attachment Size for Work Items.
2. In the Operations Manager console, click **Authoring**, expand **Management Pack Objects**, and then click **Rules**.
3. To set the scope of displayed rules, click **Scope**, and then click **View all targets**. Locate and select **TFS Collection**. Click **OK**.
4. In the list of scoped rules, right-click **Attachments Synchronization Rule**, click **Overrides**, click **Override the Rule**, and then click **For all objects of class: TFS Collection**.
5. Add an override for the parameter **Link as attachments**, and set its value to **True**.

   Important
   Some alert attachments can be very large. For example, a typical production

IntelliTrace Historical Profiling snapshot might be several hundred megabytes (MB). When this override is configured, the attachments are stored permanently in the TFS team project database. Make sure you allocate enough storage space for attachments in your database.

6. Save the settings to a management pack.

To configure alert attachments to be saved on the network file share and linked to TFS work items

1. Share access to the alert attachment network file share with developers who need to open these attachments.

   Note
   By default, alert attachments that are synchronized with TFS work items are added as links that point to the alert attachment network file share.

2. In the Operations Manager console, click **Authoring**, expand **Management Pack Objects**, and then click **Rules**.
3. To set the scope of displayed rules, click **Scope**, and then click **View all targets**. Locate and select **TFS Collection**. Click **OK**.
4. In the list of scoped rules, right-click **Attachments Synchronization Rule**, click **Overrides**, click **Override the Rule**, and then click **For all objects of class: TFS Collection**.
5. Add an override for parameter **Link as URL**, and set its value to **True**.

   Important
   Some alert attachments can be very large. For example, a typical production IntelliTrace Historical Profiling snapshot might be several hundred megabytes. Make sure you allocate enough storage space on the network file share to meet your business needs.

6. Save the settings to a management pack.

See Also

How to Configure File Attachments for Operations Manager Alerts in System Center 2012 SP1

How to Configure Notifications when Developers Reassign Work Items to IT Operations in System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

As an Information Technology (IT) operator, you need to know when developers request additional information or assign work items back to IT. Receiving notifications when developers make requests helps you respond faster. You can subscribe to get notifications when alerts are set to specific states. For example, you might want to receive notifications when work items are resolved or closed or when an alert is set to Resolved and ready for IT operations. You can configure instant messaging, text messages, email, or custom notifications. For more information about using notifications, see Subscribing to Alert Notifications.

Use the following procedure to configure notifications when developers assign work items to IT operations.

To configure notifications when developers assign work items to IT operations

1. In the Operations Manager console, click **Administration**, expand **Notifications**, and then click **Subscriptions**.
2. In the **Tasks** pane, click **New**.
3. In the Notification Subscription Wizard, enter a new subscription name, and then click **Next**.
4. On the **Criteria** page, in the **Conditions** section, select **with specific resolution state**. In the **Criteria description** section, click the **specific** link. For more information, see How to Specify Which Alerts Generate Notifications (Conditions).
5. In the **Resolution State**, select the resolution state for which you want to receive notifications. For example, if you want to receive notifications when developers request additional information from IT operations, select **Awaiting evidence**. Click **OK**, and then click **Next**.
6. On the **Subscribers** page, to specify recipients of new notifications, click **New**. For details about using the Notification Subscriber Wizard, see How to Create Notification Subscribers.
7. On the **Channels** page, to configure a new notification channel, such as email, instant message (IM), or text message, click **New**. Or, to search for a previously configured subscription channel, click **Add**. For details about using the Notification Channel Configuration Wizard, see How to Create Notification Subscriptions.
8. Click **Next**, and then click **Finish**.

How to Automatically Assign New Alerts to Engineering in System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

Through Team Foundation Server (TFS) synchronization, you can establish automatic work item routing for alerts that are raised in Operations Manager in System Center 2012 Service Pack 1 (SP1). This can be helpful if your information technology (IT) department uses TFS or if your

process model requires that all application alerts must be tracked in TFS. Additionally, you can specify which alert resolution states that are defined in Operations Manager will automatically create work items in TFS.

To route alerts to TFS automatically

1. In the Operations Manager console, click **Authoring**, expand **Management Pack Objects**, and then click **Rules**.
2. To set the scope of displayed rules, click **Scope**, click **View all targets**, locate and select **TFS Connector**, and then click **OK**.
3. In the list of scoped rules, right-click **TFS Work Items Creation Rule**, click **Overrides**, click **Override the Rule**, and then click **For all objects of class: TFS Connector**.
4. Add an override for the parameter **Assign To Engineering State Codes** and set its value to a semicolon-separated list of alert resolution states that route to TFS automatically. For example, to automatically create TFS work items for all new alerts (state 0) and alerts Assigned to Engineering (state 248), in the override value, enter **0;248**.

   Note
   Even though each alert is created as new, you must still list other resolution states that need to route to TFS. This is necessary because an alert can be assigned to engineering in the Operations Manager console before the synchronization workflow has created the work item in TFS.

   In System Center 2012 SP1, Operations Manager has the predefined alert resolution states that are described in the following table.

Alert resolution state	Resolution state ID	Description
New	0	New alert
Awaiting Evidence	247	A developer requested additional information from IT operations. With TFS synchronization turned on, this resolution state indicates that the developer has put the Operational Issue work item on hold while waiting for more information. Check the alert history for a Resolution Note from the developer.
Assigned to Engineering	248	The alert is being reviewed by developers. With TFS

		synchronization turned on, this resolution state initiates the creation of a new Operational Issue work item in TFS.
Acknowledged	249	A developer has received and accepted the Operational Issue work item for this alert. With TFS synchronization turned on, the Alert Owner field shows the current developer to whom the work item is assigned.
Scheduled	250	A fix is scheduled for the problem.
Resolved	254	A problem is resolved from a development perspective. With TFS synchronization turned on, this resolution state indicates that the associated Operational Issue work item is either resolved or closed. The alert might still be generated until the updated code is deployed to the operational environment.
Closed	255	The alert is closed.

Note

You can define your own alert resolution states in the Operations Manager console Administration pane.

5. Save the settings to a management pack.

How to Automatically Close Alerts When Work Items Are Resolved in TFS in System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

Typically, when developers implement and verify a solution for a problem, they resolve and close the related work items in Team Foundation Server (TFS). However, the problem is not fully resolved on the servers until the build containing the solution is actually deployed. Information technology (IT) operators can close the alert in Operations Manager in System Center 2012 Service Pack 1 (SP1) only when the solution is deployed on the server and the system no longer generates the same type of alert. Because of this, when a work item is closed by a developer, TFS synchronization automatically marks alerts as resolved, not closed. However, you can override the default and have TFS synchronization automatically close alerts when the associated TFS work items are closed.

To automatically close alerts when associated work items are closed

1. In the Operations Manager console, click **Authoring**, expand **Management Pack Objects**, and then click **Rules**.
2. To set the scope of displayed rules, click **Scope** select **View all targets**, locate and select **TFS Collection**, and then click **OK**.
3. In the list of scoped rules, right-click **TFS Work Items Synchronization Rule**, click **Overrides**, click **Override the Rule**, and then click **For all objects of class: TFS Collection**.
4. Add an override for parameter **Auto Close Alerts**, and set its value to **True**.

   Note
   You can override this rule on a team project collection basis. To do so, when you click **Override the Rule**, override **For a specific object of class: TFS Collection**, and then select the configured TFS collections for which the associated alerts should be closed. For more information, see How to Override a Rule or Monitor.
5. Save the settings to a management pack.

See Also

How to Configure Integration with TFS in System Center 2012 SP1

How to Stop and Resume Synchronization with TFS in System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

Sometimes you might need to temporarily stop synchronization in Operations Manager in System Center 2012 Service Pack 1 (SP1) with Team Foundation Server (TFS). For example, this may be necessary when a team project collection is unavailable because of maintenance, during maintenance of management servers in the synchronization management pool, or when you are changing synchronization settings to prevent inconsistent synchronization while new settings are applied. When you know synchronization is not working, turning off synchronization keeps unnecessary alerts about synchronization not working from being generated.

If you need to stop synchronization permanently, you can delete the TFS Work Item Synchronization template for the team project collection that you no longer want to use.

Use the following procedure to temporarily stop synchronization without deleting configuration settings. Use the next procedure to resume synchronization.

Tip

To restart synchronization, you can restart System Center Management service on all management servers in the synchronization pool.

To temporarily stop synchronization without deleting configuration settings

1. To control synchronization, the system uses three independent rules:
   - The TFS Work Items Synchronization Rule
   - The Attachments Synchronization Rule
   - The TFS Work Items Creation Rule

   To temporarily stop synchronization, you must disable all three of these rules. For more information, see How to Override a Rule or Monitor.

   In the Operations Manager console, click **Authoring**, expand **Management Pack Objects**, and then click **Rules**. To scope the displayed rules, click **Scope**, and then click **View all targets**. Look for and then select the **TFS Collection** and **TFS Connector** targets. Click **OK**.
2. To disable the TFS Work Items Synchronization Rule:
   a. In the list of scoped rules, expand **TFS Collection**, right-click **TFS Work Items Synchronization Rule**, click **Overrides**, click **Disable the Rule**, and then click **For all objects of class: TFS Collection**.
   b. On the **Override Properties** page, override the **Enabled** parameter to **False**, and then save your settings to a management pack.
3. To disable the Attachment Synchronization Rule:
   a. In the list of scoped rules, expand **TFS Collection**, right-click **Attachments Synchronization Rule**, click **Overrides**, click **Disable the Rule**, and then click **For**

all objects of class: TFS Collection.

b. On the **Override Properties** page, override the **Enabled** parameter to **False**, and then save your settings to a management pack.

4. To disable the TFS Work Items Creation Rule:

a. In the list of scoped rules, expand **TFS Connector**, right-click **TFS Work Items Creation Rule**, click **Overrides**, click **Disable the Rule**, and then click **For all objects of class: TFS Connector**.

b. On the **Overrides Properties** page, override the **Enabled** parameter to **False**, and then save your settings to a management pack.

To resume synchronization

1. To control synchronization, the system uses three independent rules:
   - The TFS Work Items Synchronization Rule
   - The Attachments Synchronization Rule
   - The TFS Work Items Creation Rule

   To resume synchronization, you must re-enable all three of these rules. For more information about override settings, see How to Override a Rule or Monitor.
2. In the Operations Manager console, click **Authoring**, expand **Management Pack Objects**, and then click **Rules**. To scope the displayed rules, click **Scope**, and then select **View all targets**. Look for and then select the **TFS Collection** and **TFS Connector** targets. Click **OK**.
3. To enable the TFS Work Items Synchronization Rule:

   In the list of scoped rules, expand **TFS Collection**, right-click **TFS Work Items Synchronization Rule**, click **Override Summary**, click the **Enabled** parameter for class TFS Collection, and then click **Delete**. Click **Close**.
4. To enable the Attachments Synchronization Rule:

   In the list of scoped rules, expand **TFS Collection**, right-click **Attachments Synchronization Rule**, click **Override Summary**, click the **Enabled** parameter for class TFS Collection, and then click **Delete**. Click **Close**.
5. To enable the TFS Work Items Creation Rule:

   In the list of scoped rules, expand **TFS Connector**, right-click **TFS Work Items Creation Rule**, click **Override Summary**, click the **Enabled** parameter for class TFS Connector, and then click **Delete**. Click **Close**.

See Also

Applying Overrides to Object Discoveries

How to Change the Frequency of Synchronization for Integration with TFS in System Center 2012 SP1

How to Configure File Attachments for Operations Manager Alerts in System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

Some management packs for Operations Manager attach additional information to alerts. This information is stored as files on the network share, and it is updated by workflows that run on the management servers. Only management servers write to this network share. Other computers in the management group can add attachments to alerts. They do so by uploading files to the management server first. Therefore, these other computers do not need direct access to the file share. Files are uploaded to the management server using the same secure Operations Manager channel that agents use to communicate with the management servers. A separate Run As profile controls the credentials that the management servers use to access the network file share.

Security

As a preliminary action, you must configure file attachments for Operations Manager alerts in System Center 2012 Service Pack 1 (SP1). This will enable integration with Team Foundation Server (TFS), IntelliTrace Historical Profiling, sharing Application Performance Monitoring events with developers, Global Service Monitor web tests, and any other scenarios that require files to be associated with Operations Manager alerts.

To configure file attachments for Operations Manager alerts

1. Create an Alert Attachment network file share with enough space to accommodate your anticipated storage needs.

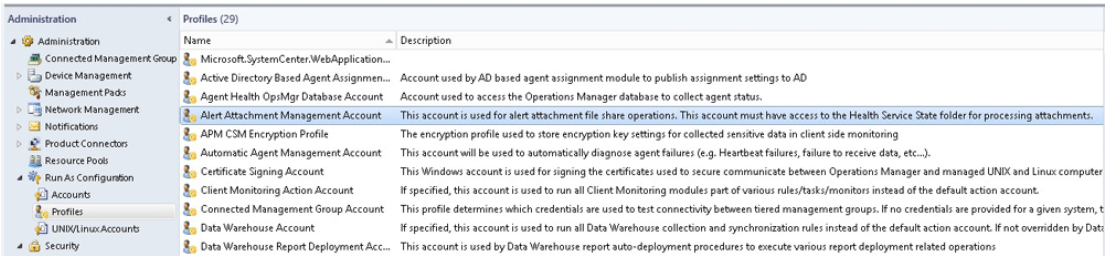
   Important
   Some alert attachments can be very large. For example, a typical production IntelliTrace Historical Profiling snapshot might be several hundred megabytes (MB). Make sure you allocate enough storage space to meet your business needs.

2. Create an active directory account that has read/write permission to the Alert Attachment network file share. Make this account a local administrator on each management server that you plan to use for synchronizing with Team Foundation Server. Make sure that the disk space quota on the network file share does not restrict this account from writing a large amount of information. This account will be used to retrieve the files that are uploaded to the management server and will place those files on the Alert Attachment network file share.
3. In the Operations Manager console, click the **Administration** button, click **Management Packs**, and then in the **Tasks** pane, click **Import Management Packs**. In the Import Management Packs Wizard, click **Add**, and then click **Add from disk**. Import the Alert Attachment Management Pack (Microsoft.SystemCenter.AlertAttachment.mpb) from the ManagementPacks folder on the System Center 2012 SP1 Operations Manager

installation media. Click **Install**, and then click **Close**.

4. Configure the Run As profile to use the account that you created for file attachments. In the Operations Manager console, click **Administration**, expand **Run As Configuration**, and then click **Profiles**. Double-click **Alert Attachment Management Account**. Locate and configure the Alert Attachment Management Account for all targeted objects. For more information about using Run As profiles, see [Managing Run As Accounts and Profiles].

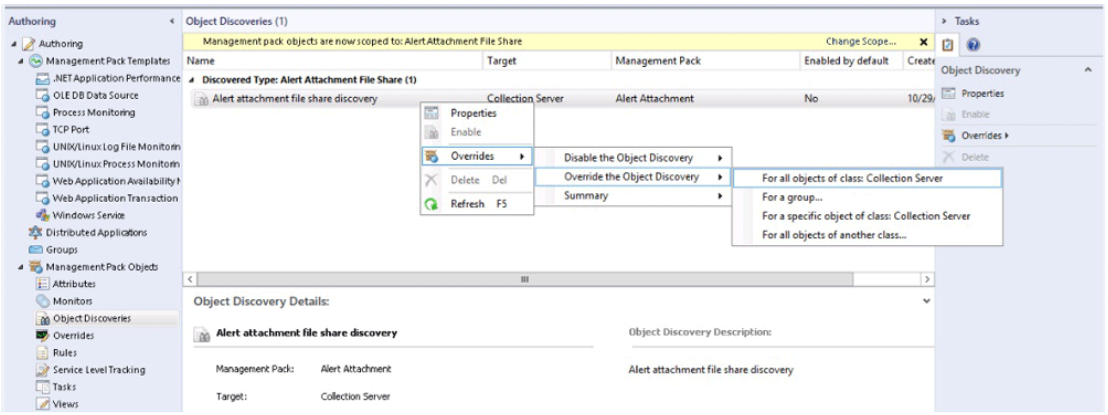
   The location of the Alert Attachment Management Account to be configured



5. Enable the Alert Attachment discovery rule, and configure the override to point to the Alert Attachment file share location. In the Operations Manager console, click **Authoring**, expand **Management Pack Objects**, and then click **Object Discoveries**. To set the object discovery scope, click **Scope**, and then click **View all targets**. Locate and select **Alert Attachment File Share**. Click **OK**.

   In the list of scoped objects, expand **Discovered Type: Alert Attachment File Share**, right-click **Alert attachment file share discovery**, click **Overrides**, click **Override the Object Discovery**, and then click **For all objects of class: Collection Server**.

   Override menus



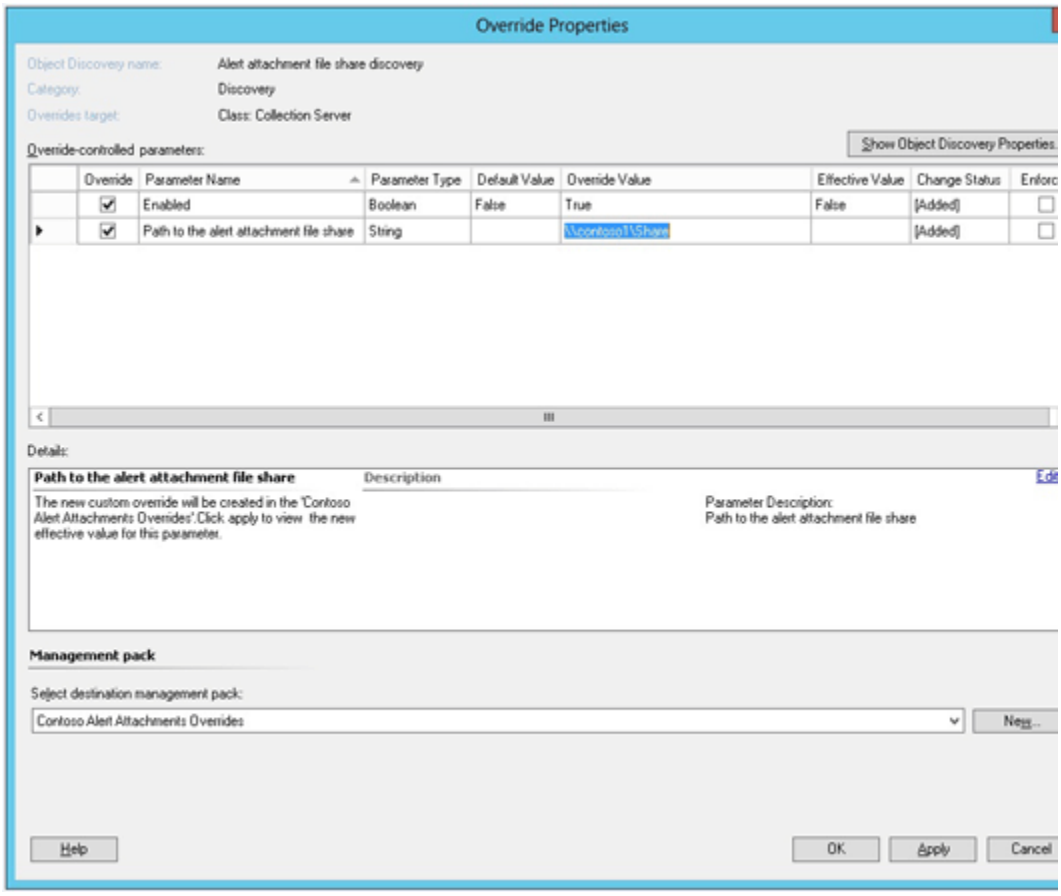
   On the **Override Properties** page, set **Enabled** to **True**, and then set **Path to the alert attachment file share** to the location of the network file share you created.

> **Important**
> You must specify the **Path to the alert attachment file share** in Uniform Naming Convention (UNC) format. For example, this is a valid format: \\contoso1\share.

You cannot use a path to a hard drive, such as C:\AttachmentFiles.

In the **Management pack** section, select a target management pack or create a new management pack to save the override values. For more information, see Applying Overrides to Object Discoveries.

Override Properties page



How to Collect IntelliTrace Historical Profiling Traces from System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

In System Center 2012 Service Pack 1 (SP1), you can use Operations Manager to capture historical snapshots (traces) directly from the Operations Manager console and to receive IntelliTrace snapshots from .NET Application Performance Monitoring (APM) exception events.

These snapshots can help developers investigate problems. They provide visibility to application execution history without needing to access the servers where the problems occurred. Developers can use Microsoft Visual Studio 2012 Ultimate to open collected snapshots. For information about IntelliTrace for developers, see Debug Your App by Recording Code Execution with IntelliTrace

Snapshots can be accessed from a network file share or from Team Foundation Server (TFS) work item attachments if TFS synchronization is enabled. For more information, see How to Configure Integration with IntelliTrace Historical Profiling in System Center 2012 SP1.

Important
After you import and configure the IntelliTrace Profiling management pack, the IntelliTrace tasks are not available until you restart the Operations Manager console.

Collecting IntelliTrace Historical Profiling Snapshots

To collect IntelliTrace snapshots for an existing APM exception alert

1. You can perform this procedure when you want to keep collected snapshots and attach an IntelliTrace snapshot to an exception alert. When TFS synchronization is enabled, the collected snapshots are attached or linked to associated work items in TFS.
2. In the Operations Manager console, click **Monitoring**, open an alert view, and then click the alert that you want to investigate.
3. In the **Tasks** pane, expand **IntelliTrace Tasks**, and then click **Start IntelliTrace Collection**.
4. On the **Run Task – Start IntelliTrace** page, in the **Run the task on these targets** section, select the servers from which you want to collect snapshots. The list shows all servers on which the application is configured for monitoring by the APM template in the environment where the alert occurred.
5. In the **Task credentials section**, select **Use the predefined Run As Account** if the Default Action Account has administrative privileges on the application Internet Information Services (IIS) pool. Otherwise, select **Other** to specify credentials that have administrative privileges for this IIS pool.
6. If you want to customize collection parameters, click **Override**.
7. Click **Run**, wait for the task to be completed successfully, and then click **Close**.

   Important
   When you click **Run**, the application IIS pool automatically recycles on all of the servers that you selected in the **Run the task on these targets** section. APM turns off for all applications that are running in the same application pool.
8. Reproduce the application problem that resulted in the APM exception alert.
9. Select the same alert on which you started IntelliTrace. In the **Tasks** pane, click **Collect**

IntelliTrace Snapshot.

10. On the **Run Task – Collect IntelliTrace Snapshot** page, select the same servers and same **Task credentials** that you previously selected when you started IntelliTrace collection.
11. Click **Run**, wait for the task to be completed successfully, and then click **Close**. The task output indicates whether any problems occurred while running the IntelliTrace collector tasks.
12. To collect multiple snapshots, repeat the previous four steps. All snapshots that you collect are attached to the same APM exception alert.
13. To stop IntelliTrace collection, select the same alert on which you started IntelliTrace. In the **Tasks** pane, click **Stop IntelliTrace Collection**.

    Important
    Be sure to stop IntelliTrace collection. If you do not stop IntelliTrace collection, IntelliTrace will continue to run. This will impact application performance, and APM will remain off so that you will not receive new alerts from this application. To stop IntelliTrace when the alert is already closed and no longer shows in the Operations Manager console, complete the step from the subsequent procedure that stops IntelliTrace: To collect IntelliTrace snapshots when there are no APM exception alerts
14. To see the IntelliTrace snapshots that are attached to an alert, select the alert. In the **Tasks** pane, click **Open Snapshot Location**.
15. If TFS synchronization is turned on, you can assign an alert to engineering. To do so, set the alert resolution state to **Assigned to Engineering**. This creates a new work item in TFS, with the snapshot attached or linked. For more information, see How to Configure Integration with TFS in System Center 2012 SP1.

To collect IntelliTrace snapshots when there are no APM exception alerts

1. You can perform this procedure when you are investigating problems with application logic or when APM is not enabled for an application. The subject application in this procedure must be discovered by the IIS management packs.
2. In the Operations Manager console, click **Monitoring**, expand **Application Monitoring**, and then expand **.NET Monitoring**.
3. If your application is running on Windows Server 2008 R2, click **IIS 7.0 ASP .NET Web Application Inventory**. If your application is running on Windows Server 2012, click **IIS 8.0 ASP .NET Web Application Inventory**.
4. Select the application pool on which you want to run IntelliTrace profiling.
5. In the **Tasks** pane, expand **IntelliTrace Tasks**, and then click **Start IntelliTrace Collection**.
6. On the **Run Task – Start IntelliTrace** page, in the **Run the task on these targets** section, select the application pool in which you want to collect snapshots.
7. In the **Task credentials section**, select **Use the predefined Run As Account** if the Default Action Account has administrative privileges on the application IIS pool.

Otherwise, select **Other** to specify alternative credentials that have administrative privileges for this IIS pool.

8. If you want to customize collection parameters, click **Override**.
9. Click **Run**, wait for the task to be completed successfully, and then click **Close**.

   Important
   When you click **Run**, the application IIS pool automatically recycles on all of the servers that you selected in the **Run the task on these targets** section. APM turns off for all applications that are running in the same application pool.
10. Run your application and reproduce the behavior that you want to investigate.
11. Select the same application pool on which you started IntelliTrace. In the **Tasks** pane, click **Collect IntelliTrace Snapshot**.
12. On the **Run Task – Collect IntelliTrace Snapshot** page, select the same target and same **Task credentials** that you previously selected when you started IntelliTrace collection.
13. Click **Run**, wait for the task to be completed successfully, and then click **Close**. The task output indicates whether any problems occurred while running the IntelliTrace collector tasks.
14. To collect multiple snapshots, repeat the previous four steps. For each snapshot that you collected, you will receive a new informational alert when the snapshot is uploaded to the network file share.
15. To stop IntelliTrace collection, select the same application pool on which you started IntelliTrace. In the **Tasks** pane, click **Stop IntelliTrace Collection**.

    Important
    Be sure to stop IntelliTrace collection. If you do not stop IntelliTrace collection, IntelliTrace will continue to run. This will impact application performance and APM will remain off so that you will not receive new alerts from this application.
16. To see the IntelliTrace snapshots, in the Operations Manager console, click **Monitoring**, expand **IntelliTrace Profiling**, and then click **New Alerts**. The **New Traces** pane shows an alert for each snapshot that you have collected.
17. In the **Tasks** pane, expand **Alert Attachment Tasks**, and then click **Open Attachment Location**.
18. If TFS synchronization is turned on, you can assign an alert to engineering. To do so, set the alert resolution state to **Assigned to Engineering**. This creates a new work item in TFS with the snapshot attached or linked. For more information, see How to Configure Integration with TFS in System Center 2012 SP1.

To access IntelliTrace snapshots that are generated from APM exception data

1. You can perform this procedure when you want to investigate an existing APM exception event that is based solely on historical data without having to run IntelliTrace Profiling on your application. Only .NET exception events generate IntelliTrace snapshots.
2. In the Operations Manager console, click **Monitoring**, open an alert view, and then click

the alert that you want to investigate.

3. In the **Tasks** pane, expand **Alert Attachment Tasks**, and then click **Open Attachment Location**. Windows Explorer opens the location of the files that are attached to the alert you have selected.
4. To see the IntelliTrace snapshot for this alert, in Windows Explorer, open the **APMException** folder.
5. If TFS synchronization is turned on, you can assign this alert to engineering. To do so, set the alert resolution state to **Assigned to Engineering**. This creates a new work item in TFS, with the snapshot attached or linked. For more information, see How to Configure Integration with TFS in System Center 2012 SP1.

How to Configure Integration with IntelliTrace Historical Profiling in System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

In System Center 2012 SP1, Operations Manager includes the IntelliTrace Profiling Management Pack. This management pack lets you capture historical snapshots (traces) directly from the Operations Manager console, and to automatically generate IntelliTrace snapshots from .NET Application Performance Monitoring (APM) exception events. These snapshots can help developers investigate problems by giving them visibility to application execution history without the developers needing access to the servers where the applications ran. Developers can use Microsoft Visual Studio 2012 Ultimate to open the collected snapshots. For information about IntelliTrace for developers, see Debug Your App by Recording Code Execution with IntelliTrace

IntelliTrace Profiling Management Pack automatically deploys the necessary infrastructure, which is called the IntelliTrace Collector, to the designated servers. The collected snapshots are uploaded to a network file share and attached to Operations Manager alerts. Snapshots are uploaded to the management server using the same secure Operations Manager channel that agents use to communicate with the management servers. You can configure Team Foundation Server (TFS) synchronization so that the IntelliTrace snapshots will be automatically added or linked to TFS work items. For more information, see How to Configure Integration with TFS in System Center 2012 SP1.

Caution

IntelliTrace snapshots contain application runtime data that might include personal and sensitive information. Review your company's privacy policies before you enable this feature.

To configure integration with IntelliTrace Historical Profiling

1. Import and configure the Alert Attachment Management Pack. This management pack links the collected IntelliTrace snapshots to Operations Manager alerts. For more information, see How to Configure File Attachments for Operations Manager Alerts in System Center 2012 SP1.
2. If you want to synchronize IntelliTrace snapshots with TFS work items, import and configure the TFS Work Item Synchronization Management Pack. When snapshots are synchronized with work items, developers can receive IntelliTrace snapshots with TFS work items in Visual Studio. Additionally, developers can set work item state to **Awaiting Evidence** and use TFS to submit requests to capture IntelliTrace snapshots. For more information, see How to Configure Integration with TFS in System Center 2012 SP1.

   Note
   You can use IntelliTrace snapshots without TFS integration. If you do so, the IntelliTrace snapshots are not attached to work items, but they are uploaded to the Alert Attachment network file share instead.
3. In the Operations Manager console, click the **Administration** button, click **Management Packs**, and then, in the **Tasks** pane, click **Import Management Packs**. In the Import Management Packs Wizard, click **Add**, and then click **Add from disk**. Import the following management packs from the ManagementPacks folder on the System Center 2012 SP1 Operations Manager installation media:
   - IntelliTrace Collector Deployment (Microsoft.SystemCenter.IntelliTraceCollectorInstallation.mpb)
   - IntelliTrace Profiling (Microsoft.SystemCenter.IntelliTraceProfiling.mpb)

   Click **Install**, and then click **Close**.

   Important
   The IntelliTrace tasks are not available until you restart the Operations Manager console.

How to Synchronize Alerts with TFS in System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

In System Center 2012 SP1, you can synchronize Operations Manager alerts and Team Foundation Server (TFS) work items. When synchronization is enabled, IT operations can then assign alerts to the engineering team. Assigning an alert to engineering creates a new work item in TFS. The workflow will track and synchronize any changes that are made to TFS work items and any associated Operations Manager alerts. In order to synchronize alerts with TFS, you must first configure alert synchronization. For more information, see How to Configure Integration with TFS in System Center 2012 SP1.

To assign alerts to engineering

1. In the Operations Manager console, you can view all application problems that have been collected. To view alerts in Operations Manager, in the navigation pane, click **Monitoring**, and then click **Active Alerts**.
2. To assign an alert to engineering, right-click the alert, select **Set Resolution State**, and select **Assigned to Engineering**. This action creates a TFS work item and adds the TFS work item ID to the alert.
3. The system synchronizes all changes to the alert inside Operations Manager and all changes to the work item in TFS.

   Tip
   Any comments that you add to an Operations Manager alert on the alert **History** tab are automatically added to the corresponding TFS work items. You can use this function to provide additional information to engineering.

To review alerts that are awaiting evidence from engineering

1. In the Operations Manager console, you can view all application problems that have been collected. To view alerts in Operations Manager, in the navigation pane, click **Monitoring**, expand **Team Foundation Server Synchronization**, expand **Alerts**, and then click **Awaiting Evidence**.

To review and close alerts that have been resolved by engineering

1. In the Operations Manager console, you can view all application problems that have been collected. To view alerts in Operations Manager, in the navigation pane, click **Monitoring**, expand **Team Foundation Server Synchronization**, expand **Alerts**, and then click **Resolved**.
2. When you want to close the resolved alerts, you can right-click an alert, select **Set Resolution State**, and then set the resolution state to **Closed**.

Monitoring Integration between Operations Manager and TFS in System Center 2012 SP1

Synchronization between Operations Manager and Team Foundation Server (TFS) makes efficient communication possible between information technology (IT) operations and developers. A healthy TFS environment is essential for all development processes. Depending on your environment, you can import TFS monitoring and management packs that give you real-time visibility into the health of the TFS developer environment.

The TFS Work Item Synchronization management pack synchronizes Operations Manager alerts and TFS work items. Additionally, it monitors the synchronization infrastructure, and it generates alerts when synchronization fails. However, to monitor the complete TFS infrastructure, you need additional monitoring packs that alert you about a wide range of problems with TFS components. When you import the TFS Work Item Synchronization management pack, it is a best practice to also import and configure these monitoring packs. Together, they help you make sure that you are monitoring the complete health of the developer TFS environment.

Management and Monitoring Packs to Use with TFS Integration

Use the management packs and monitoring packs in the following table for TFS integration.

Management Pack	Description	Use with …	Where to get it
Microsoft Visual Studio 2010 Team Foundation Server Monitoring Management Pack for Microsoft System Center	Monitors TFS infrastructure. Provides both proactive and reactive monitoring of Microsoft Team Foundation Server 2010. Monitors TFS components, such as application tier server instances, team project collections, build servers, and proxy servers.	• Microsoft Team Foundation Server 2010 • Operations Manager 2007 R2 • System Center 2012 – Operations Manager • Operations Manager in System Center 2012 Service Pack 1 (SP1)	Microsoft Download Center
Microsoft Visual Studio 2012 Team Foundation Server Monitoring Management Pack for Microsoft System Center	Monitors TFS infrastructure. Provides both proactive and reactive monitoring of Microsoft Team Foundation Server 2012. Monitors TFS components, such as application tier server instances, team project collections, build servers, and proxy servers.	• Microsoft Team Foundation Server 2012 • Operations Manager 2007 R2 • System Center 2012 – Operations Manager • Operations Manager in System Center 2012 SP1	Microsoft Download Center

Management Pack	Description	Use with …	Where to get it
System Center Management Pack for Microsoft Visual Studio Team Foundation Server 2010 Work Item Synchronization	Provides synchronization with Microsoft Team Foundation Server 2010. Monitors its own synchronization infrastructure only. Use this if you are running System Center 2012 – Operations Manager without SP1.	• Microsoft Team Foundation Server 2010 • System Center 2012 – Operations Manager • Operations Manager in System Center 2012 SP1	Microsoft Download Center
Team Foundation Server Work Item Synchronization Management Pack	Provides synchronization with Microsoft Team Foundation Server 2010 and Microsoft Team Foundation Server 2012. Monitors its own synchronization infrastructure only.	• Microsoft Team Foundation Server 2010 • Microsoft Team Foundation Server 2012 • Operations Manager in System Center 2012 SP1	Operations Manager in System Center 2012 SP1 media

Note

If your environment contains TFS 2010 and TFS 2012, you can use both monitoring packs together (Microsoft Visual Studio 2010 Team Foundation Server Monitoring Management Pack for Microsoft System Center and Microsoft Visual Studio 2012 Team Foundation Server Monitoring Management Pack for Microsoft System Center). Also, you can use these management packs without enabling synchronization between Operations Manager alerts and TFS work items to get visibility into the health of the TFS environment.

See Also

How to Configure Integration with TFS in System Center 2012 SP1

Monitoring with Microsoft Monitoring Agent

Microsoft Monitoring Agent is a new agent that replaces the Operations Manager Agent and combines .NET Application Performance Monitoring (APM) in System Center with the full

functionality of IntelliTrace Collector in the Microsoft Visual Studio development system for gathering full application-profiling traces. Microsoft Monitoring Agent can collect traces on demand or can be left running to monitor applications and collect traces. You can limit the disk space that the agent uses to store collected data. When the amount of data reaches the limit, the agent begins to overwrite the oldest data and store the latest data in its place.

You can use Microsoft Monitoring Agent together with Operations Manager or as a stand-alone tool for monitoring web applications that were written on the Microsoft .NET Framework. In both cases, you can direct the agent to save application traces in an IntelliTrace log format that can be opened in Microsoft Visual Studio Ultimate. The log contains detailed information about application failures and performance issues.

You can use Windows PowerShell commands to start and stop monitoring and collect IntelliTrace logs from web applications that are running on Internet Information Services (IIS). To open IntelliTrace logs that are generated from APM exceptions and APM performance events, you can use Visual Studio. For information about supported versions of IIS and Visual Studio, see Microsoft Monitoring Agent Compatibility.

Monitoring with Microsoft Monitoring Agent Topics

- Installing Microsoft Monitoring Agent
- Monitoring Web Applications with Microsoft Monitoring Agent
- Comparing Monitoring Approaches for .NET Applications
- Microsoft Monitoring Agent Compatibility

Installing Microsoft Monitoring Agent

You can obtain and install Microsoft Monitoring Agent in several ways. You can manually install it from the System Center 2012 R2 Operations Manager media or the Microsoft Download Center, or you can deploy it automatically by using the **Administration** pane of the Operations Manager console. Additionally, you can opt in to automatically get the latest updates of the agent from Microsoft Update. Local collection is a lightweight monitoring solution that does not require any special configuration. You do not need databases or special accounts.

Important
Microsoft Update will not upgrade the Operations Manager agent from System Center 2012 Service Pack 1 (SP1) – Operations Manager to Microsoft Monitoring Agent. For more information, see Microsoft Monitoring Agent Compatibility to make sure that a compatible version of the agent is running in your environment.

Note

System Center versions before System Center 2012 R2 Operations Manager delivered the agent as the MOMAgent.msi file. You can still find the file that has the same name on the System Center 2012 R2 Operations Manager installation media. However, the file now installs Microsoft Monitoring Agent. If you get Microsoft Monitoring Agent from the Download Center, you can download either the 32-bit (MMASetup-i386.exe) version or the 64-bit (MMASetup-AMD64.exe) version of the agent.

To install Microsoft Monitoring Agent from the Operations Manager installation media, see Install Agent Using the MOMAgent.msi Setup Wizard.

To install Microsoft Monitoring Agent from the **Administration** pane in Operations Manager, see Install Agent on Windows Using the Discovery Wizard.

To install Microsoft Monitoring Agent from the Download Center for stand-alone monitoring

1. Open the Microsoft Monitoring Agent download page in the Microsoft Download Center.

   Important
   Local collection requires Microsoft .NET Framework 3.5 and the Windows PowerShell 2.0 command-line interface. Some features, such as downloadable Help and pre-imported monitoring Windows PowerShell modules, are not available unless you have Windows PowerShell 3.0.

2. Choose whether to install the 32-bit (MMASetup-i386.exe) or 64-bit (MMASetup-AMD64.exe) version of Microsoft Monitoring Agent, and follow the instructions to download the file.
3. When the download is complete, run the file and follow the instructions.
4. On the **Agent Setup Options** page, you can choose whether you want to connect the agent to Operations Manager. When you connect the agent with Operations Manager, you can manually choose the management group that this agent will participate with in monitoring. If you do not select this option, the agent can still collect Application Performance Monitoring data locally. You can change your selection in the **Monitoring Agent** item in Control Panel.

   Important
   If you connected this installation of the agent to Operations Manager, your System Center administrator must allow manual agent installations on the management server. This setting is controlled in the Operations Manager console. Additionally, before System Center begins to accept monitoring traffic from your agent, the System Center administrator must approve the agent in the Pending Management view in the **Administration** pane of the Operations Manager console.

Monitoring Web Applications with Microsoft Monitoring Agent

When Microsoft Monitoring agent is used together with System Center Operations Manager, it adds value for IT Operations by providing real-time alerting, operational reporting, and centralized management of configuration. Microsoft Monitoring Agent without connection to System Center can be used as a lightweight Application Performance Monitoring (APM) solution for Microsoft .NET Framework applications that does not require heavy infrastructure from IT Operations, so you can begin monitoring applications within a few minutes.

You can download Microsoft Monitoring Agent for stand-alone use or for use with Operations Manager from the Microsoft Download Center. You can also install it from the System Center 2012 R2 Operations Manager media. Downloading Microsoft Monitoring Agent from the Download Center gives you the latest version of the agent with the latest monitoring capabilities. After you install Microsoft Monitoring Agent for use without Operations Manager, you can use it to collect application traces locally. Microsoft Monitoring Agent adds the following new Windows PowerShell commands that control local monitoring:

- **Start-WebApplicationMonitoring** starts monitoring an Internet Information Services (IIS) web application.
- **Stop-WebApplicationMonitoring** stops monitoring an IIS web application and creates a Microsoft IntelliTrace file by using data that is collected during monitoring.
- **Checkpoint-WebApplicationMonitoring** creates a snapshot of the IntelliTrace file and continues monitoring.
- **Get-WebApplicationMonitoringStatus** gets the monitoring status of all monitored web applications.

Monitoring by Using Local Collection

To start and stop monitoring by using local collection

1. Start Windows PowerShell as an administrator. Your account must be a member of the Local Administrators group to perform this task, or you must run Windows PowerShell as a user who belongs to the Local Administrators group.
2. If you are using Windows PowerShell 2.0, you must manually import the monitoring module Microsoft.MonitoringAgent.PowerShell.dll from the Microsoft Monitoring Agent installation location. By default, the module is located at C:\Program Files\Microsoft Monitoring Agent\Agent\PowerShell\Microsoft.MonitoringAgent.PowerShell\. For example, to import the module, at the Windows PowerShell command prompt, type `import-module "C:\Program Files\Microsoft Monitoring Agent\Agent\PowerShell\Microsoft.MonitoringAgent.PowerShell\Microsoft.MonitoringAgent.PowerShell.dll".`

   Important

If you are using Windows PowerShell 2.0 and close Windows PowerShell, you must repeat this step to use any Windows PowerShell commands in Microsoft Monitoring Agent.

If you are using Windows PowerShell 3.0, the module will already be imported and you do not need to import it manually as described in this step.

3. At the Windows PowerShell command prompt, type `Start-WebApplicationMonitoring` and then specify the web application name, the monitoring mode, and the output location. For example, type `Start-WebApplicationMonitoring Fabrikam/FabrikanFiber.Web Monitor c:\outputlogs`.

   - To find the web application name, use the **Get-WebSite** and **Get-WebApplication** Windows PowerShell commands.
   - To limit the amount of space that is allocated for traces, use the *MaximumFileSizeInMegabytes* parameter and allocate enough space.
   - The monitoring mode can be Trace, Monitor, or Custom. These monitoring modes use a *collection plan*, which determines how an application is monitored (such as custom namespaces to monitor, all or only critical exceptions, and application-specific exception handlers). When you use Trace, you can use Microsoft Monitoring Agent in the same way that you might have used an IntelliTrace collector, and you can use collection plans in the form of the IntelliTrace collector that was part of Microsoft Visual Studio 2010 and Visual Studio 2012 and is available in Visual Studio 2013. The Monitor option uses the default monitoring collection plan that is preconfigured with Microsoft Monitoring Agent. The default collection plan is located in the same folder as the monitoring module. You can use this default collection plan by using the Monitor option, or you can copy it to a different file and customize it and use it with the Custom monitoring mode.

   Warning
   Starting and stopping monitoring might restart or recycle your application IIS pool.

4. To stop monitoring, type `Stop-WebApplicationMonitoring`. For example, type `Stop-WebApplicationMonitoring Fabrikam\FabrikamFiber.Web`. For more information about using Windows PowerShell commands, see these Windows PowerShell topics: Microsoft.MonitoringAgent.PowerShell.Start-WebApplicationMonitoring, Microsoft.MonitoringAgent.PowerShell.Stop-WebApplicationMonitoring, Microsoft.MonitoringAgent.PowerShell.Checkpoint-WebApplicationMonitoring, Microsoft.MonitoringAgent.PowerShell.Get-WebApplicationMonitoringStatus.

5.

   To learn more, see Monitor your app with Microsoft Monitoring Agent.

Using Local Monitoring and the .NET APM Template in System Center at the Same Time

If you configured application monitoring by using the .NET Application Performance Monitoring template in Operations Manager, you can still use Windows PowerShell commands in Microsoft Monitoring Agent local monitoring to monitor applications. The Windows PowerShell commands in Microsoft Monitoring Agent have higher priority than the APM monitoring configuration and will temporarily override the APM monitoring configuration when you use them to start local collection. For more information, see Microsoft Monitoring Agent Compatibility.

Customizing Local Collection

To get useful results from your monitoring, you might need to customize default collection settings, such as namespaces and thresholds that specify your application-specific service level agreements (SLAs). This customization is controlled in your collection plan. After you edit the collection plan, you must restart monitoring.

Comparing Monitoring Approaches for .NET Applications

A general best practice is to always monitor your Microsoft .NET Framework applications (continuous monitoring) because this gives you information about baseline performance, and you receive timely notifications of application failures before many customers are affected. At times, however, you might need to start monitoring only to troubleshoot specific application problems (on demand). System Center provides a powerful monitoring solution that includes alerting and reporting that are not available when you use local collection. However, using System Center usually requires an administrator and a heavier infrastructure. Local collection is a lightweight monitoring solution that does not require any special configuration before you can start monitoring. For instance, you do not need to set up special databases or special accounts. Less data is collected, and you receive no real-time alerts about application problems. Locally collected traces do not have performance counters or other diagnostic information that is available when you use Microsoft Monitoring Agent together with System Center 2012 – Operations Manager.

Choosing How to Monitor Your .NET Framework Applications

Comparing monitoring approaches

Monitoring approach	When to use	How to control monitoring
Continuous monitoring with System Center Application Performance Monitoring (APM)	Use this approach when you have System Center Operations Manager. Typically, IT Operations uses this approach to receive alerts about application performance or failures. IT Operations can convert data from APM alerts into Microsoft IntelliTrace format or can automatically route alerts to Microsoft Visual Studio Team Foundation Server (TFS) work items by using TFS synchronization. IT Operations owns the environment. For more information, see How to Configure Integration with TFS in System Center 2012 R2.	Use the .NET Application Performance Monitoring template. For more information, see .NET Application Performance Monitoring Template
Continuous monitoring with Microsoft Monitoring Agent local collection	Use this approach when your computer is still monitoring by using System Center and when you have other applications	Use Windows PowerShell cmdlets **Start-WebApplicationMonitoring** and **Checkpoint-WebApplicationMonitoring**. **Start-WebApplicationMonitoring** starts monitoring. **Checkpoint-WebApplicationMonitoring** collects a snapshot

Monitoring approach	When to use	How to control monitoring
	configured for APM monitoring. You are the owner of an environment. You control when to start and stop monitoring and know the best times to collect traces.	of the IntelliTrace file and continues monitoring. **Checkpoint-WebApplicationMonitoring** does not affect your application and does not require a restart of your application. After you start monitoring, the monitoring will continue even if your application or computer restarts. **Stop-WebApplicationMonitoring** stops monitoring. For more information, see Microsoft.MonitoringAgent.PowerShell.Start-WebApplicationMonitoring and Microsoft.MonitoringAgent.PowerShell.Checkpoint-WebApplicationMonitoring.
On-demand local collection that temporarily overrides the settings of continuous monitoring with System Center APM	Use this approach when you want to collect more data at certain times for troubleshooting. You will need to define your collection plan by using application-specific settings, and this might take more system resources for monitoring (CPU and memory). Output will be an IntelliTrace log that includes all events that are collected during the override, on-demand session. IT Operations still owns the environment, but you must collect more data at certain times and you have the flexibility.	Use Windows PowerShell cmdlets **Start-WebApplicationMonitoring** and **Stop-WebApplicationMonitoring** to enable local collection. When you stop monitoring, the trace is written to a local file and your System Center APM monitoring settings are restored.
On-demand local collection that	Use this approach when you have	Use Windows PowerShell cmdlets **Start-WebApplicationMonitoring** and **Stop-**

Monitoring approach	When to use	How to control monitoring
temporarily overrides settings of continuous monitoring with Microsoft Monitoring Agent local collection	already monitored an application, but you need to troubleshoot a particular application issue and want to run monitoring by using more refined settings that might take more system resources for monitoring (CPU and memory). Output will be an IntelliTrace log that includes all events that are collected during the override, on-demand session. IT Operations still owns the environment, but you must collect more data at certain times and you have the flexibility.	**WebApplicationMonitoring**. When you stop monitoring, the trace is written to a local file in the location that you specified when you started monitoring.

Microsoft Monitoring Agent Compatibility

The following table details the compatibility of Microsoft Monitoring Agent and versions of System Center and the Microsoft Visual Studio development system.

Microsoft Monitoring Agent compatibility

Service	Build	Supported versions of System Center	Supported versions of Visual Studio	Interoperability information
Microsoft Monitoring Agent	September 2013 release	• System Center 2012 R2 Operations Manager	• Microsoft Visual Studio Ultimate 2013 RC • Microsoft	If you want to use local monitoring with Application Performance Monitoring in

Service	Build	Supported versions of System Center	Supported versions of Visual Studio	Interoperability information
		• System Center 2012 Service Pack 1 (SP1) – Operations Manager (only when you are multihoming by using System Center 2012 R2 Operations Manager or during upgrades to System Center 2012 R2 Operations Manager) • System Center 2012 – Operations Manager (only when you are multihoming by using System Center 2012 R2 Operations Manager or during upgrades to System Center 2012 R2 Operations Manager)	Visual Studio Ultimate 2013 Preview • Microsoft Visual Studio Ultimate 2012 Update 2	System Center 2012 SP1, you must be running Update 4.

Service	Build	Supported versions of System Center	Supported versions of Visual Studio	Interoperability information
		• System Center 2012 R2 Operations Manager (only when you are multihoming by using System Center 2012 R2 Operations Manager or during upgrades to System Center 2012 R2 Operations Manager)		

Index to Security-Related Information for System Center 2012 - Operations Manager

Security information for System Center 2012 – Operations Manager is documented with the function or task to which it applies. This index identifies security-related information for Operations Manager and links to the relevant topics.

Type of information	Location
Firewall	• Firewall exceptions required by Operations Manager features in Supported Configurations for System Center 2012 - Operations Manager • Using a Firewall in the Deployment Guide • How to Configure the Operations Manager Database to Listen on a Specific TCP/IP

Type of information	Location
	Port in the Deployment Guide • How to Configure the Reporting Data Warehouse to Listen on a Specific TCP/IP Port in the Deployment Guide
Secure Sockets Layer (SSL)	• Web Console Security in Operations Manager in the Deployment Guide • How to Configure the Operations Console to Use SSL When Connecting to a Reporting Server in the Deployment Guide
Operations Manager accounts	• Deploying System Center 2012 - Operations Manager in the Deployment Guide • Security Considerations in the Deployment Guide • Topics explain how to change credentials for Operations Manager accounts in Account Information for Operations Manager section of Deployment Guide • Operations Manager Accounts in the Operations Guide • How to Create a New Action Account in Operations Manager in the Operations Guide • How to Manage the Report Server Unattended Execution Account in Operations Manager in the Operations Guide
Certificates	• Authentication and Data Encryption for Windows Computers in the Deployment Guide • How to Obtain a Certificate Using Windows Server 2008 Stand-Alone CA in the Deployment Guide • How to Obtain a Certificate Using Windows Server 2008 Enterprise CA in the Deployment Guide • How to Configure an HTTPS Binding for a Windows Server 2008 CA in the Deployment Guide

Type of information	Location
	• How to Remove Certificates Imported with MOMCertImport • Managing Certificates for UNIX and Linux Computers
Authentication and access	• Security Considerations in the Deployment Guide • Monitoring Across Untrusted Boundaries in the Operations Guide • Authentication and Data Encryption for Windows Computers in the Deployment Guide • Accessing UNIX and Linux Computers in Operations Manager in the Operations Guide • Troubleshooting UNIX and Linux Monitoring: Certificate Issues in the Operations Guide • Implementing User Roles in the Operations Guide • Control Access by Using the Health Service Lockdown Tool in Operations Manager in the Operations Guide • Managing Run As Accounts and Profiles in the Operations Guide
Network monitoring	Security for Servers Performing Network Discovery in the Operations Guide
Audit Collection Services (ACS)	• Deploying ACS and ACS Reporting in the Deployment Guide • Collecting Security Events Using Audit Collection Service in Operations Manager in the Operations Guide • Audit Collection Services Security in the Operations Guide
Internet proxy settings	How to Configure the Internet Proxy Settings for a Management Server in the Deployment Guide
Data sent to Microsoft	• System Center 2012 - Operations Manager Privacy Statement • Customer Experience Improvement

Type of information	Location
	Program (CEIP) • Operational Data Reporting (ODR) • Error Reporting • Client Monitoring Using Agentless Exception Monitoring in Operations Manager in the Operations Guide
Monitoring .NET applications	Working with Sensitive Data for .NET Applications in the Operations Guide

Related Resources

- TechNet Library main page for Operations Manager
- What's New in Operations Manager
- Operations Manager Release Notes
- Deployment Guide for Operations Manager
- Operations Manager Supported Configurations
- Operations Guide for Operations Manager

Authoring for System Center 2012 - Operations Manager

The Authoring Guide for System Center 2012 – Operations Manager provides information on creating custom monitoring for your application.

Prerequisites

This guide assumes that you have a basic knowledge of Operations Manager and understand all of the concepts presented in the Operations Guide for System Center 2012 - Operations Manager.

Not included in this guide

While the following topics are relates to authoring, they are covered in the Operations Guide for System Center 2012 - Operations Manager instead of this guide. This is because these features are available to users from the **Monitoring** workspace of the Operations console and may be used by a user without Author privileges or custom monitoring requirements.

- Overrides

- Views and Dashboards

More Information

For more information about creating management packs for different versions of Operations Manager and for other options for automating System Center components, see the System Center Authoring Hub.

Author's Guide Topics

- Key Concepts for Authors

  Describes basic concepts related to authoring. You should understand the concepts in this section before reviewing the other content in the guide.
- Targets and Objects

  Describes basic concepts and procedures related to targets and objects.
- Management Pack Templates

  Describes each of the standard management pack templates which provide complete monitoring scenarios with minimal effort.
- Monitors and Rules

  Describes the structure of monitors and rules and provides details for creating different kinds monitoring scenarios.
- Distributed Applications

  Describes how distributed applications work and how to create one using the Distributed Applications Designer.

Downloadable Documentation

You can download a copy of this technical documentation from the Microsoft Download Center. Always use the TechNet library for the most up-to-date information.

Key Concepts for Authors

This section of the Author's Guide to Operations Manager provides general concepts that an author should understand. The subsequent sections of the guide assume familiarity with these core concepts.

Key Concepts Topics

- What is an Author?

  Describes the concept of authoring and the tools and permissions required for the author.

- Authoring Tools

  Provides an overview of the different tools that are available to the author with an explanation of who should use which tools under different conditions.
- Structure of a Management Pack

  Describes the basic structure of a management pack and the different kinds of management packs that are available.
- Sealed Management Pack Files

  Describes the implications of sealing a management pack and the procedure for sealing one.
- Understanding Classes and Objects

  Provides an overview of the concepts of classes and objects.

What is an Author?

A variety of management packs are available that include complete monitoring for particular applications. You can monitor these applications by installing and configuring the appropriate management pack.

Operators can customize certain settings in existing monitoring configurations by using overrides. Overrides can perform such actions as disabling a particular rule, controlling how often a rule runs, or changing the threshold on a monitor. However, overrides cannot be used to create any additional monitoring.

There are times where you might have to add additional monitoring scenarios to an existing management pack or create monitoring for an application or device that has no management pack. When you create new monitoring for an application, you are acting as a *Management Pack Author*. As an author, you can create additional monitoring scenarios for an application with an existing management pack or create an entirely new management pack for an application that does not have a management pack.

What tools do I use?

Because management packs are implemented in .xml files, any XML editor can create and modify the XML code, however, this is the most complex method. Generally, you can create any monitoring that you require by using much simpler methods in the Operations console. When using the console, you have to select which management pack file you want to use to store any elements that you create, but there are few other details about the management pack that you have to consider.

For more information about the tools that you can use to create a management pack, see Authoring Tools.

What permissions do I require?

The permissions that you require to perform authoring depend on the method that you are using. Permissions in Operations Manager are controlled through user roles. All authoring performed in the Operations console requires access to the **Authoring** workspace. To access this workspace, you must have the **Author** or **Administrator** user role. Your authoring credentials might be limited to particular target classes depending on the author scope of the user role. If this is the case, you only can author elements against these classes. For more information about user roles, see Implementing User Roles.

If you are using one of the offline methods for authoring, the Authoring console or an XML editor, you do not require any permissions because you are simply creating a file offline. In contrast, to install the management pack, you must have the **Administrator** user role.

See Also

Authoring Tools

Understanding Classes and Objects

Implementing User Roles

Authoring Tools

There are multiple tools available for creating new monitoring in System Center 2012 – Operations Manager. The choice you make will depend on your requirements and experience with Operations Manager. Each of the available tools is described below.

Operations Console

The **Authoring** workspace of the Operations console contains templates and wizards that let you create monitoring scenarios that require minimal knowledge of authoring concepts.

Specific characteristics of the Operations console include the following:

- Creates or changes a management pack file in an existing management group. Changes are committed and deployed to agents immediately.
- Creates predefined monitoring scenarios by using templates and wizards. Cannot create custom monitoring scenarios.
- Cannot create custom classes or discoveries except for specific cases that the template provides.

The primary advantage of the Operations console is the ability to create new monitoring scenarios with minimal complexity. The Operations console provides the following approaches for creating monitoring scenarios.

Management Pack Templates

Management Pack templates let you create complete monitoring scenarios with minimal input. A single template can create different monitors, rules, and even new target classes without requiring you to know any of the details. If a template is available for the monitoring scenario that you want to create, this method is typically your easiest and most effective solution.

Distributed Application Designer

The Distributed Application Designer lets you create a single application that is comprised of multiple objects. It does not let you create new monitoring for these objects. The health of each object included in the distributed application is based on the monitors already running against that object. The health of the distributed application is based on the health of the individual objects that are included in it.

Authoring Wizards

Wizards let you create new monitors, rules, and tasks. You have to know the details of what data the workflow uses and what action are performed with that data. Wizards are available for a variety of different data sources and monitoring scenarios. You cannot create a new target with the monitoring wizards. You can use a suitable wizard that is available in an existing management pack, or you can create a wizard by using a template or by editing the management pack in the Authoring console.

Use of the Operations console is documented in this guide.

Visio Management Pack Designer

The Visio Management Pack Designer (VMPD) is an add-in for Microsoft Visio 2010 that allows you to create a management pack using graphical shapes. You can create a custom model representing your application based on a set of common patterns. Standard monitoring scenarios can be added to the model by simply setting properties on shapes that are added to the diagram. You can use the VMPD to create a complete management pack for an application with basic monitoring requirements or use it as a starting point for a management pack that can be edited using other tools.

Specific characteristics of the Visio Management Pack Designer include the following:

- Graphical tool that allows you to create sophisticated management packs while requiring minimal knowledge of the models and monitoring being created.
- Create new classes representing your application that cannot be created in the Operations console.
- Creates predefined monitoring scenarios. Cannot create custom monitoring scenarios.
- Generate a management pack file that can be installed in a management group or used as a starting point for additional modification using other authoring tools.
- Cannot import the management pack back into Visio once it has been generated.

- Creates or changes a management pack on disk without requiring access to the management group.

Documentation for the Visio Management Pack Designer is available at Visio Management Pack Designer for System Center 2012 - Operations Manager.

System Center Operations Manager 2007 R2 Authoring Console

The System Center Operations Manager 2007 R2 Authoring console can be used to create management packs for both System Center Operations Manager 2007 R2 and System Center 2012 – Operations Manager. It is intended for management pack authors with significant knowledge of the structure of management pack elements and lets them create and modify all elements in a management pack. It is not limited to a specific set of scenarios, although it does require deeper technical knowledge than the Operations console.

The Authoring console provides many of the same wizards as the Operations console, except that the Authoring console wizards can provide access to additional options. The Authoring console provides custom dialog boxes similar to the Operations console to help you configure management pack elements where they are available. For those elements where no dialog box is available, you must edit the XML code of the management pack directly. To help edit, the Authoring console starts an external editor. You use the editor to edit the XML code of the specific element and, when it is closed, the editor returns the completed element back to the management pack. You can specify the editor that the Authoring console starts.

Specific characteristics of the Operations console include the following:

- Creates or changes a management pack on disk without requiring access to the management group. Optionally, loads management packs from a management group and installs them after modification.
- Provides custom ID for each management pack element.
- Creates all management pack elements including custom classes, relationships, and discoveries that cannot be created in the Operations console.
- Creates predefined monitoring scenarios by using wizards. Creates custom monitoring scenarios with the assistance of the user interface.

Use of the System Center Operations Manager 2007 R2 Authoring Console is documented in the System Center Operations Manager 2007 R2 Authoring Guide.

Visual Studio Authoring Extensions

Because management packs are .xml files, any XML editor can create and modify them. While this is more complex than using the other authoring options, editing the XML gives you complete control over all elements in a management pack.

An XML editor is required for the following scenarios that cannot be performed in the consoles:

- Management pack elements cannot be copied by using the other consoles. For example, you might want to create a management pack element by copying a similar element in the same

management pack, or you might want to copy an element from another management pack into the current one. This functionality can only be performed with an XML editor.

- The consoles do not let an existing management pack element be modified if it affects the configuration of another element. For example, a rule might use a custom module that requires values for one or more parameters. You might want to modify this module and add an additional parameter to it. Because the rule would not provide a value for this required parameter after the module was modified, the changed module cannot be saved. To make this change in the Authoring console, you must delete the rule and create it again after changing the module. By using an XML editor, you can change the module and rule at the same time.
- The ID of a management pack element cannot be changed with the Authoring console after it has been created. You must perform this task with an XML editor. The ID of the element cannot only be changed, but you must search for the old ID and replace it with the new ID across the management pack because the element's ID might be used multiple times in the XML code.

The Visual Studio Authoring Extensions allow you to work with the XML of a management pack in System Center 2012 – Operations Manager directly using Microsoft Visual Studio. It provides the following advantages over using a standard XML editor:

- Provides XML templates and IntelliSense for different management pack elements so that you don't have to have detailed knowledge of the schema.
- Allows you to create XML fragments containing different management pack elements. The fragments can be copied within the management pack, to another management pack, and combined to build the final management pack.
- Allows multiple authors to work on a single management pack project at the same time.

Documentation for the Visual Studio Extensions is available at Visual Studio Authoring Extensions for System Center 2012 - Operations Manager.

See Also

System Center Operations Manager 2007 R2 Authoring Resource Kit

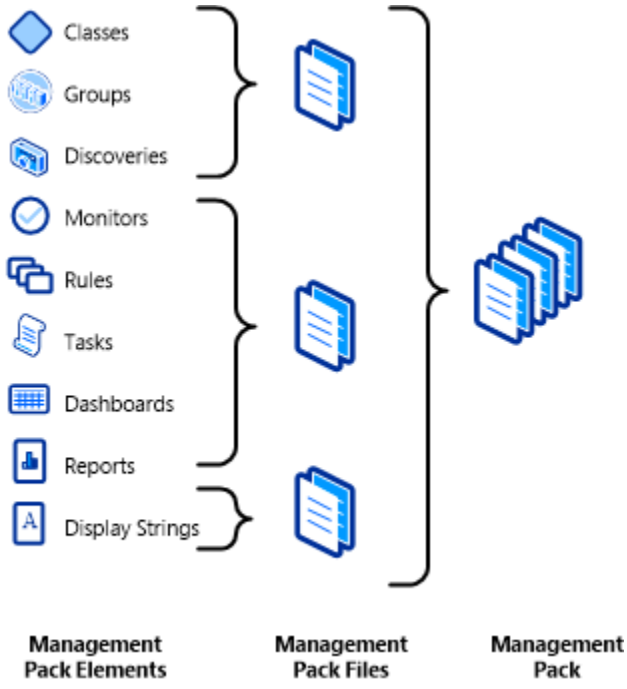
Structure of a Management Pack

Management packs to Operations Manager are the equivalent of games to a video game console. The main function of the console is to provide the basic functionality required to run the game, but the game provides the true value of the overall system. A variety of games are available that each provides a distinct entertainment experience. Similarly, Operations Manager provides basic functionality such as deployment of agents to managed computers and central collection, and analysis of collected information. A management pack is then required for each application that you want to monitor. The management pack only has to provide logic specific to the application and can take advantage of the platform provided by Operations Manager.

Management Pack Files

A single management pack is comprised of one or more *management pack files*. A management pack file is either an .xml file that can be viewed and edited, or an .mp file which is a sealed .xml file that cannot be changed. When you download a management pack from the management pack catalog, it typically includes a set of management pack files that each contains a specific set of elements. When you create a new element in the Operations console, you must select a management pack file to store it in.

Conceptual view of management pack files and elements



Management Pack Elements

A *management pack element* is a single item in a management pack such as a class, monitor, dashboard, or report. There are reasons that management pack authors group different elements in a particular file, but you can ignore the reasons until you get to more advanced concepts. For now, just understand that the word element refers to one of these items.

Compatibility with Operations Manager 2007

Operations Manager supports management packs that use a later version of the XML schema than Operations Manager 2007. Management packs written for Operations Manager 2007 work without changes in Operations Manager. However, management packs written by using new

Operations Manager elements or using the updated schema do not work in Operations Manager 2007. This includes management packs that are created in the Operations Manager 2012 Operations console because they are based on the new schema.

Types of Management Packs

All management packs use the same schema and can contain any elements that are used in Operations Manager. Management packs with a specific set of elements are referred to with a more specific term as described below.

Monitoring Pack

Monitoring packs are management packs intended to perform general monitoring scenarios. These are the primary management packs obtained from the management pack catalog. They also are the primary management pack that you create with the Operations console and Authoring console.

Feature Pack

Feature packs contain additional features for a monitoring pack. These can be features that are optional. You can select which set of features you want to install. Another reason for a feature pack is that it can contain elements specific to Operations Manager so that the monitoring pack can be used in Operations Manager 2007 and Operations Manager with the additional features only used in Operations Manager.

Dashboard Packs

Dashboard packs are feature packs that contain dashboards which are a new feature to Operations Manager, so they cannot be imported into an Operations Manager 2007 management group. Dashboards are not included in monitoring packs so that the monitoring pack can be used with both version of Operations Manager.

Security Packs

Security Packs are feature packs that monitor the security of an application.

Language Packs

Any text displayed by a management pack in the Operations Console is defined in a *display string*. Wizards populate the display strings, so you do not have to distinguish them from the elements that they are associated with. Some management pack files contain only display strings in a particular language. These are referred to as *language packs*. If you require a management pack in alternate languages, you can download the appropriate language packs for the languages that you require. If you are creating your own management pack, you can use the Authoring console or XML code to define display strings in any languages that you require.

Management Pack Schema

Knowledge of the schema for a management pack is only required if you edit the management pack directly by using an XML editor. You are never exposed to this schema when using the Operations console and only rarely with the Authoring console. Wizards are available for creating common elements, and custom user interface pages are available for common modules. Direct XML editing is only required for configuring modules and workflows that do not have custom UI pages. The XML for defining complex data types might be required, and the schema for these data types is provided in the Schema Type Reference.

See Also

Sealed Management Pack Files

Sealed Management Pack Files

When a management pack file is sealed, it is converted to a binary file that has an .mp extension. Either the sealed or the unsealed version of a management pack file can be installed to a management group, but both cannot be installed at the same time.

Important
Sealing a management pack is not a valid strategy for hiding information from users. You can export any sealed management pack from the management group by giving you full access to its XML code. A management pack should never contain sensitive information such as passwords.

Characteristics of Sealed Management Pack Files

Sealed management pack files have the following characteristics:

The contents of the management pack file cannot be modified

Sealed management pack files cannot be changed. Changes must be made to the .xml file which is then sealed again with the same certificate. Such an update can only be installed in the same management group if the updated management pack is backward compatible.

Enforce version control

Only sealed management pack files enforce version control when an updated version of the management pack is installed. If the management pack is unsealed, the new version is always installed regardless of its backward compatibility.

Enable the management pack to be referenced by other management packs

Management packs can only reference an element in another management pack if the management pack that is referenced is sealed. This requirement ensures that a modification to a management pack cannot break other management packs that reference it. Because sealed management packs maintain version control, any referencing management packs ensures that updates to the sealed management pack are backward compatible.

When to Seal a Management Pack File

Management pack files do not all have to be sealed. You can install the unsealed version of a management pack file in a management group, and it behaves exactly as the sealed version of the same management pack file. The following criteria list when a management pack file must be sealed:

- Management pack files that are referenced by other management pack files must be sealed. You might want to create common elements such as groups or modules that are used by other management packs for different applications. The application management packs do not have to be sealed, but the management pack files that contain the shared elements must be.
- Any management packs that are sent to external customers must be sealed. In addition to ensuring that the customer cannot modify the contents of the management pack, it ensures that any modifications they make are made through overrides in a different management pack file. This lets you provide updates to the management pack without affecting the customer's modifications.
- Management pack files that are shared by multiple business units in your organization should be sealed. This ensures that each business unit makes any modifications through overrides in their own management pack files. Each business unit cannot make modifications that affect the other group.

Sealing a Management Pack File

Management pack files are sealed by using the MPSeal tool that is located in the SupportTools folder of the Operations Manager 2007 R2 distribution media. Sealing requires a client certificate to validate the identity of the author.

You can use the Strong Name tool (Sn.exe) included with the Microsoft .NET Framework SDK to create a certificate sufficient for sealing management packs for testing. For production, use a client certificate from the correct certification authority (CA) appropriate for signing code for sealing management packs.

For information about the process for sealing a management pack file, see How to Seal a Management Pack File.

See Also

How to Seal a Management Pack File

Structure of a Management Pack

How to Seal a Management Pack File

Management packs are sealed by using the MPSeal tool that is located in the SupportTools folder of the Operations Manager 2007 R2 distribution media. This is a command-line tool that creates a sealed .mp file from an unsealed .xml file. After performing the sealing process, you can install the sealed management pack in your management group.

Note

If you created the management pack in the Operations console, you must export it to an .xml file before performing the sealing process. You must then uninstall the management pack before installing the sealed version.

MPSeal Syntax

MPSeal.exe uses the following syntax:

MPseal.exe *Management Pack File Name* [**/I** *Include Path*]* **/Keyfile** *Key File Path* **/Company** *Company Name* [**/Outdir** *Output Directory*] [**/DelaySign**] [**/Copyright** *Copyright text*]

Each of the command-line options are described in the following table.

Option	Description
Management Pack File Name	The full name of the .xml file to seal. If the file is not in the current directory, you must include the full path to the file. If the path includes a space, you must enclose it in quotes.
Include Path	The path to a directory containing .mp files that are referenced by the management pack that you are sealing. For more information, see Management Pack References.
Key File Path	The file containing the private and public key. For more information, see Key File.
Company Name	The name of your company. If it includes a space, you must enclose it in quotes.
Output Directory	The directory to store the output file. If not specified, the current directory is used.

Option	Description
DelaySign	If this option is used, only the public key is used. For more information, see Delayed Signing.
Copyright text	Text to include for copyright information. While this option is functional, the text is not currently accessible from Operations Manager.

Example

The following example seals a management pack file named Contoso.MyApp.xml. It creates a file called Contoso.MyApp.mp in the current directory.

```
mpseal Contoso.MyApp.xml /I c:\mp /Keyfile contoso.snk /Company "Contoso"
```

Management Pack References

In addition to sealing the management pack, MPSeal verifies the management pack file and reports any errors that prevents it from installing. All of these errors must be corrected before the sealing finishes successfully. The MPVerify tool performs the same verification . To perform this function, MPSeal requires access to any management packs referenced by the management pack that is in the process of being sealed. These must be the sealed versions of the files with an .mp extension and must be at least the version specified by the management pack that is being sealed.

You specify a directory to search .mp files with the **/I** command-line option. You can use multiple **/I** options if the required files are in multiple directories. You can obtain the standard library management pack files included with Operations Manager 2007 R2 from the installation directory on the management server. You must obtain other management pack files separately. If you import a management pack directly into your management group from the management pack catalog, you have to download it separately to obtain the .mp file.

Note
If you are unsure of the management packs referenced by the management pack that you are sealing, you can run MPSeal by using any directory. A list of the required management packs are returned.

For more information about management pack references, see the **Management Pack References** section of this guide.

Key File

Sealing requires a key file that contains a private and public key. The key pair validates the identity of the signing party and ensures that a malicious user cannot provide a sealed

management pack by impersonating someone else. This is the same key pair used for signing .NET assemblies and can be created with the Strong Name tool (sn.exe) included with the Microsoft Windows SDK.

Important
You should protect any key file that is used to seal a management pack. If someone else were to obtain this key file, they could seal a management pack by impersonating the original author.

For information about the complete use of the Strong Name tool, see Sn.exe (String Name Tool). The following example is sufficient for most management packs and creates a key file called contoso.snk in the local directory.

```
sn -k contoso.snk
```

Delayed Signing

For added security of their private key, organizations often implement a delayed process for signing assemblies. This allows access to the private key to only a few individuals. Using this process, you sign the assembly with only the public key, and then complete the signing with the private key just before a release.

If your organization has an existing process for performing delayed signing of assemblies, you should use this process to seal your management pack for production. You can perform the initial partial sealing of the management pack by using the **/DelaySign** option.

For more information about delayed signing of assemblies, see Delay Signing an Assembly.

Management Pack Files Created in the Operations Console

Management pack files created in the Operations console are unsealed. You can use the following procedures if you have to seal a management pack that you created in the Operations console.

To seal a management pack file that was created in the Operations console

1. Export the management pack file to an .xml file. For more information, see How to Export an Operations Manager Management Pack.
2. Seal the XML code. For more information, see MPSeal Syntax.
3. Delete the management pack file from the management group. For more information, see How to Remove an Operations Manager Management Pack.
4. Import the .mp file created by MPSeal. For more information, see How to Import an Operations Manager Management Pack.

See Also

Sealed Management Pack Files

Selecting a Management Pack File

When you create any monitoring in the Operations console, you have to specify a management pack file for the elements that you are creating. This topic describes a basic strategy that you can follow and provides additional details to help you understand the logic of the recommended strategy.

General Strategy

For applications that already have a sealed management pack installed, typically management packs installed from the Management Pack Catalog:

- Create a separate management pack file to store overrides and new monitoring for that application.

For applications that do not have a sealed management pack installed, typically management packs that you created yourself:

- Create a separate management pack file for each application. Use this file to store overrides and any new monitoring for that application.

For common elements that are used by other management pack files, such as groups:

- Create a separate management pack file for each logical set of elements. Seal this management pack file before installing it.

  Note
  If you created the management pack file in the Operations console, you must export it to an .xml file, and then seal it. You must then uninstall the unsealed management pack file from the management group before you install the sealed management pack file.

Default Management Pack

The **Default Management Pack** file contains common elements such as views at the top level of the **Monitoring** workspace. This is an unsealed management pack file so that you can create views and folders at this level. It should not be used for any other purpose. For creating elements such as monitors and rules, create a new management pack file.

Logically Grouping Elements

Although you could simply create a single management pack file to store all custom elements that you create, it is not a best practice. While management pack elements are treated individually by

the agents that run them, the management group works with the management pack file. When a management pack file is installed in the management group or removed from it, it includes all of its management pack elements.

When you determine how to group different elements, take the following considerations into account:

- Management pack files are delivered to any agent computer that requires at least one element in the file. If you use a single management pack file for different applications, elements might be delivered to agents that do not require them. The agent only actually loads the elements for the applications that it has installed, but the entire management pack file is delivered. Breaking up management pack files according to the elements that are relevant to a single application ensures the most efficient delivery of the files to agents.
- You can remove an application from your environment and no longer require its management pack. Or you can obtain a new management pack for an application and want to remove custom monitoring that you implemented. In cases like these, you can uninstall all of the elements for a particular application by removing any of its management pack files. If you combine elements for multiple applications, you limit your ability to manage the monitoring logic for a single application.
- You can develop and test some monitoring logic in a lab environment before moving it into a production management group. Combining elements for a particular application into a single management pack lets you manage that file through the different environments without affecting the monitoring for other applications.

By following the recommend strategy for logically grouping management pack elements, you can ensure that your management group runs as efficiently as possible and can most effectively handle future changes.

Sealed and Unsealed Management Pack Files

When selecting a management pack file, you must consider the implications of sealed and unsealed management packs. An element in one management pack file cannot refer to an element in another file if the file being referenced is not sealed. For this reason, you might have to group-related elements in a single management pack file or seal management pack files meant for general use. For more information about the effects of sealing a management pack, see Sealed Management Pack Files.

Because a sealed management pack file cannot be modified, you can only store new management pack elements in unsealed files. Any management pack created in the Operations console is unsealed, and any dialog box prompting you for a management pack only includes unsealed files.

For example, you might create a set of groups that represent different aspects of your computing environment such as the data center that certain computers reside in, the support personnel that manage particular computers, or the applications that different computers support. You want to use those groups to override monitors and rules that you created in different management pack files.

If you used the Operations console to create the groups in this example in an unsealed management pack file, you could not use them with other management pack files. You have to use one of the following two strategies to implement this solution:

- Create groups in each management pack file with the overrides. This has the advantage of being easy to implement without any requirement to seal a management pack file, but it has the disadvantage of requiring you to potentially create multiple copies of the same group.
- Create a separate management pack file for the groups. After you create the groups in the Operations console, export the management pack to an .xml file, and then seal the .xml file by using the process described in Selecting a Management Pack File. You can then install the sealed version of the management pack file so that the groups are available to any other management pack.

See Also

Management Pack Templates

Monitors and Rules

Targets and Objects

An *object* is the basic unit of management in Operations Manager. An object typically represents something in your computing environment, such as a computer, a logical disk, or a database. A *class* represents a kind of object, and every object in Operations Manager is considered an *instance* of a particular class. A *target* in the Operations console represents all instances of a particular class.

The following sections provide further detail on these concepts and guidance for selecting target and created new classes.

Targets and Objects Topics

- Understanding Classes and Objects

  Basic concepts for understand classes and objects that are required for basic and advanced authoring.
- Selecting a target

  Guidance for selecting a target when you create a monitor
- Creating a new target

  Strategies for creating a simple class to use as a target for custom monitors and rules.
- Attributes

  Concepts of how attributes are used and procedure for adding new attributes to an existing class.

Understanding Classes and Objects

To start authoring in Operations Manager, you should understand some basic concepts and terminology about how monitored objects are implemented. If you have used the Operations Manager for monitoring, you are already familiar with using these objects, but for authoring, you should understand them at a deeper level.

Object

An *object* is the basic unit of management in Operations Manager. An object typically represents something in your computing environment, such as a computer, a logical disk, or a database. It could also represent something more abstract, such as an application, an Active Directory domain, or a DNS zone. An object can also be referred to as an *instance* of a particular Class.

Objects must be discovered before they appear in the Operations console. Management packs include *discoveries* that inspect information about the agent computer to determine whether an object should be created and what the values for its properties should be. These discoveries are typically run on a schedule, and different management packs define different schedules for different objects. One discovery might run one time per day whereas another might run every few hours.

For more information about discoveries for advanced authors, see Discovery in the System Center Operations Manager 2007 R2 Authoring Guide.

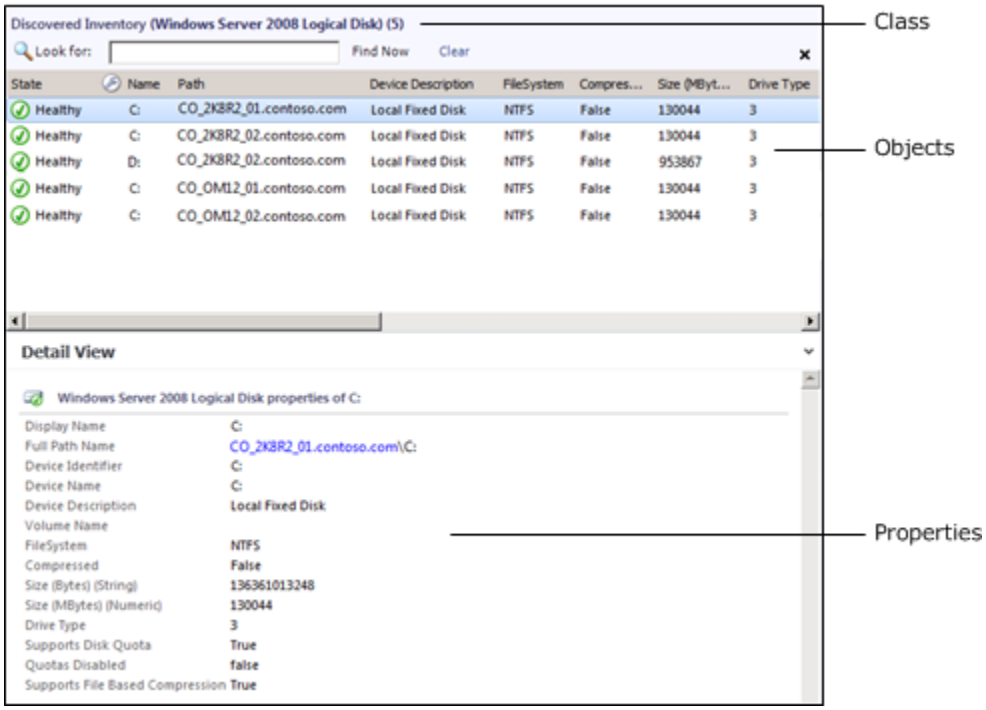
Class

A *class* represents a kind of object, and every object in Operations Manager is considered an *instance* of a particular class. All instances of a class share a common set of properties. Each object has its own values for these properties which are determined when the object is discovered. Most management packs define a set of classes that describe the different components that make up the application that is being monitored and the relationships between those classes.

A *target* in the Operations console represents all instances of a particular class. For example, a view lists all of the objects that are instances of the class that is used as the target class for the view, and a monitor is applied to all objects that are instances of the monitor's target class.

The following screenshot shows an example of **Windows Server 2008 Logical Disk** class and objects in the **Discovered Inventory** view in the Operations console.

Sample Class and Objects



Base Classes

You only have to understand the concept of base classes if you are performing advanced authoring. For more information, see **Classes and Relationships**. For basic authoring, you only have to understand how base classes affect targeting.

Every class in Operations Manager has a *base class*. A class has all the properties of its base class and potentially adds more. All of the classes from the different management packs installed in your management group can be arranged in a tree with each class positioned under its base class. If you start at any class, and then walk up the tree following its base class, and then the base class of that class, and so on, you eventually reach the **Object** class which is the *root* of the System Center class library.

Note

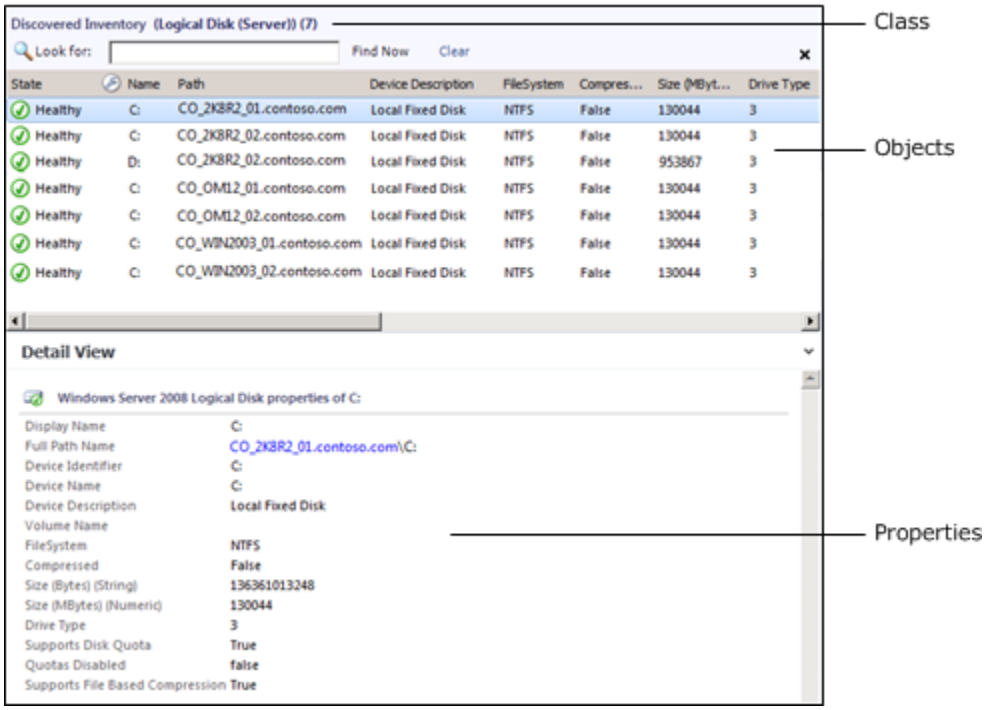
The *Entity* class is the root of the class library in Operations Manager 2007. The **Entity** class is the same class as **Object**. It has been renamed in Operations Manager 2012.

When you select a class as a target that is a base class for other classes, the monitor or rule applies to all instances of each of those classes. For example, if you use **Windows Operating System** as the target for a monitor, then the monitor applies to all instances of **Windows Client Operating System** and **Windows Server Operating System**. This is because those two classes use **Windows Operating System** as their base class. If you use Operating System as the target, the monitor applies to all those classes and also to any instance of **Unix Operating System**.

For information about how to view the complete class library in your management group from the **Distributed Application Designer**, see Distributed Applications.

The following screenshot shows an example of **Logical Disk (Server)** class and objects in the **Discovered Inventory** view in the Operations console. This is the base class for **Windows Server 2008 Logical Disk** which is shown earlier in this section. Note that this includes the same set of objects, but adds instances of **Windows Server 2003 Logical Disk** which also uses **Logical Disk (Server)** as its base class.

Sample Base Class and Objects



Hosting Classes

Most classes are *hosted* by another class. When one class hosts another, the hosting class is called the *parent*, and the class being hosted is called the *child*. Instances of the child class cannot exist without a parent. For example, several classes are hosted by **Windows Computer** because they are components on a computer. It would not make sense to have a logical disk if there was no computer for the disk to be installed on. Therefore, **Logical Disk** is hosted by **Windows Computer**. This means that every instance of **Logical Disk** must have one instance of **Windows Computer** as its parent.

Hosting classes can be important because the properties of the host of a target class are available in rules and monitors. An object might also have the health of its child objects available in its Health Explorer.

You can typically determine the hosting parent of an object by viewing its **Path Name** property. This includes the name of the object's parent. In the Operations console, you can click this name to open a state view for the parent object. In the previous screenshots, the name of the computer hosting the selected logical disk is included in the selected object's path name.

Group

A *group* is a collection of objects. They can be instances of the same class or of different classes. Groups have population criteria that define what objects are added to them. This can be dynamic criteria that adds objects as they are discovered or explicit criteria where you manually add specific objects to the group.

Groups are used to scope overrides, views, and user roles and to set the scope of monitoring for certain templates. They are not used to target monitors and rules. For more information, see Targeting a group,

Viewing Classes and Objects

Use the following procedure to walk through the examples illustrated earlier in this section in your own Operations Manager environment. This shows the concepts of objects, classes, and base classes by using the **Logical Disk** classes in the **Windows Server Operating System Management Pack**. You must have this management pack installed in your management group to complete this procedure.

To view a class in the Operations console

1. Start the Operations console.
2. In the navigation pane, click **Monitoring**, and then select **Discovered Inventory**.
3. In the **Actions** pane, click **Change Target Type**. In the **Select Items to Target** dialog box, select **View all targets**.

   This list consists of all the classes included in all the management packs that are currently installed in the management group. Any of these classes can be selected to view a list of all its discovered instances and their properties. Any new classes included in a management pack that is installed later in the management group will be included in this list.
4. Select **Windows Server 2008 Logical Disk**, and then click **OK**.

   This view shows a listing of logical disks on Windows Server 2008 computers that were discovered in the current environment.
5. Select one of the instances.

   Take note of the properties in the **Detail View** pane. This shows the values for each property that were collected by the discovery process. Notice also the **Path name** property that is built from the key property of the current class and its parents. In this case, the key properties include the computer name and the device name.

6. In the **Actions** pane, again select **Change Target Type**.
7. In the **Select Items to Target** dialog box, select **View all targets**.
8. Select **Logical Disk (Server)**, and then click **OK**.

   This is the class that is the base class for **Windows Server 2008 Logical Disk**. The view resembles the previous one, but includes objects from both Windows Server 2003 and Windows Server 2008, assuming both are installed in your environment. The properties are identical to the previous view, because the **Windows Server Logical Disk** class has the same properties that are inherited by **Windows Server 2008 Logical Disk**.
9. In the **Actions** pane, again select **Change Target Type**. In the **Select Items to Target** dialog box, select **View all targets**.
10. Select **Logical Disk**, and then click **OK**.

    This is the class that is the base class for **Logical Disk (Server)**. The instances are identical to the previous view, but fewer properties are shown. This is because the **Logical Disk** class has only the properties directly assigned to it, and inherits only its single property from **Object**. The other properties are not visible because they are associated with a class further down the tree.
11. Select one of the disks and then click the link on the computer name part of the **Path Name** property shown in the **Detail View**.

    This opens a state view for the hosting object of the disk object that you selected. You can see in the **Detail View** that this is an instance of **Windows Computer**.

See Also

Selecting a target

Creating a new target

Selecting a target

Every time you create a monitor or rule, you must select a target for it. The target determines where the monitor or rule will run and how its information will be organized in the Operations console. It is important to understand how targets work so that you can select the most appropriate one for the monitor or rule that you are creating.

If you are creating a monitor or rule for an application or device that already has a management pack installed, then you can most likely use a target that already exists in your management group. If you are creating a monitor or rule for a new application then you may need to create a new target specifically for this purpose. Creating a new target is covered in Creating a new target.

You do not select specific objects to target in Operations Manager 2012 but rather you select a particular class of object. The monitor or rule will apply to all instances of the target class. For more information on classes and instances of classes, see Understanding Classes and Objects.

Quick Logic

If you do not have a full understanding of the logic behind the selection of a target, you can use the following quick logic. Refer to the rest of this section for a complete explanation of the effects of a target and how to select an appropriate one.

Examples

- If you want the monitor or rule to run on all Windows computers in your management group, then select **Microsoft Windows Computer**.
- If you want the monitor or rule to run on all Unix computers in your management group, then select **Unix Computer**.
- If you want the monitor or rule to run on all computers running SQL Server 2008 in your management group, then select **SQL 2008 DB Engine**.
- If you want the monitor or rule to run on all computers running any version of SQL Server in your management group, then select **SQL DB Engine**.
- If you want the monitor or rule to run against all logical disks on all Windows servers in your management group, then select **Logical Disk (Server)**.

Effects of a target

The target of a monitor or rule determines the following:

- Where the monitor or rule will run
- How many copies of the monitor or rule will run on the agent
- What object the data will be associated with
- What properties will be available for the expression and the alert description

Where the monitor or rule will run

The monitor or rule will run on each agent that has at least one instance of the target class. You should select a target that only includes those agents where you want the rule or monitor to run.

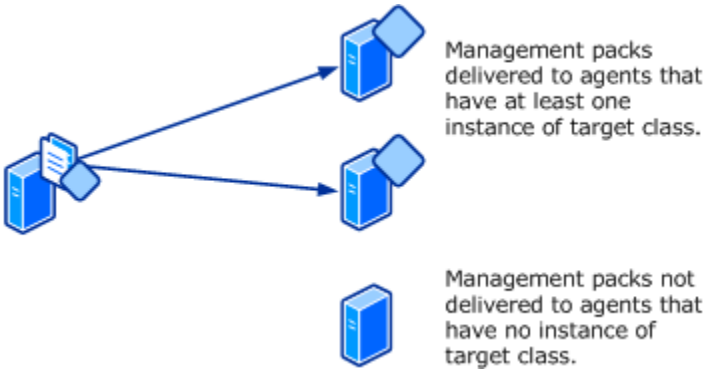
When a management pack is installed or changed, it is delivered to any agent that manages at least one instance of a class that is used as a target on at least one included workflow. Only workflows targeted at classes that have discovered instances on the agent are actually loaded.

You must ensure that the data that the monitor or rule is accessing will be available in the agent where it is running. For example, if you are creating a monitor that looks for a particular event, you must ensure that the event will be written to the event log where the monitor is running. If you are creating a rule that collects a performance counter, you must ensure that the performance counter is available on that agent. If you are creating a monitor that runs a script, then the script will run on that agent and any resources that it access must be available on the local computer.

If you select a very broad class such as **Windows Computer**, then the monitor or rule will probably run on the agents that you need, but it will also probably run on additional agents where

it is not needed. If a broad class such as this is the only one that includes the agents that you need, then consider creating a new target as described in Creating a new target.

Management pack delivery

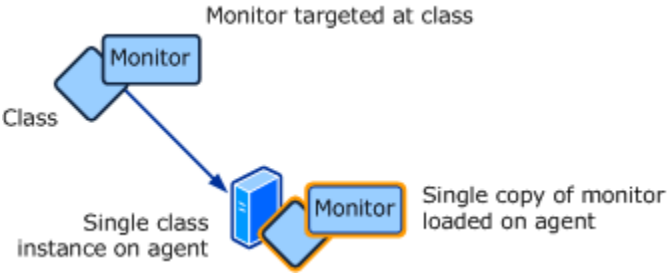


How many copies of the monitor or rule will run on the agent

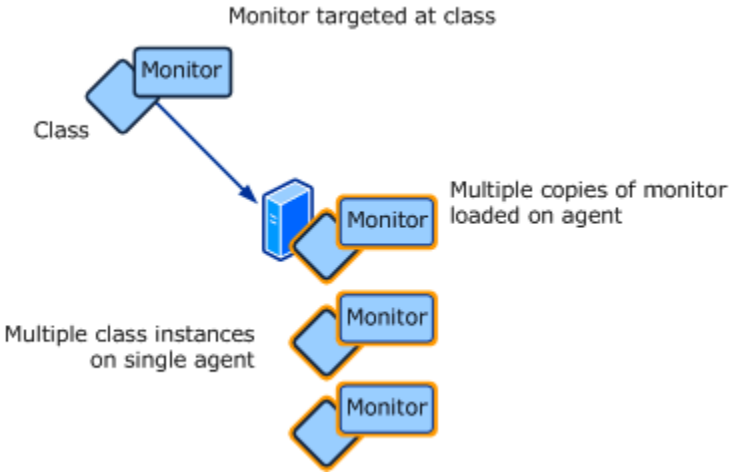
One copy of the monitor or rule will run for each instance of the target. If there is more than one instance of the target on an agent, then more than one copy of the monitor or rule will run on that agent. You can determine how many objects are running on each agent in your environment using the procedure in Viewing Classes and Objects.

For targets such as **Windows Computer**, you can be assured that they will only have a single object on a particular agent. Other targets such as **Logical Disk** may have only object but could have multiple depending on the configuration of the agent computer.

Workflow targeted at a single instance



Workflow targeted at multiple instances



If you do target a class that may have multiple instances on a single agent, then you need to include criteria in the expression to unique identify each instance.

What object the data will be associated with

Monitors are included in the Health Explorer of their target object. This has implications beyond just the user interface. Any downtime from the monitor would be included in the availability of the target object. For example, while using **Windows Computer** as a target might cause a monitor to run on the agent computers that you want, any downtime from the monitor would result in downtime for the entire computer, which may not be valid. It would be better to use a target more specific to the component that you want to monitor.

Alerts and data collected by rules will be associated with their target object. When you right-click an open alert and select **Health Explorer**, you will open the Health Explorer of the target object. When you right -click an object and select **Performance View**, you will open a view with performance data for the target object. To achieve optimum functionality from the monitors and rules that you create, you should select or create a target that most accurately represents the component that you want to monitor.

What properties will be available for the expression and the alert description

Properties of the target object are available for both any expressions that are used in the monitor or rule and in the description of the resulting alert.

Viewing Classes and Objects

You can use the **Discovered Inventory** view in the Operations Console to assist in selecting an appropriate target for a particular monitor or rule. This view will list all instances of a specified class with its entire set of properties. This shows which instances of the class are managed by

different agents, how many instances each agent is managing, and what properties the class has available. Any workflows targeted at the selected class will be run against each of the objects listed in the view. If no instances are listed for a particular class, then none have been discovered on any agents. Any workflows targeted at these classes would not be run.

You can view the discovered inventory for a particular class using the following procedure.

1. In the Operations console, click the **Monitoring** button.
2. In the **Monitoring** pane, select **Discovered Inventory**.
3. In the **Actions** pane click **Change Target Type**.
4. In the **Select Items to Target** dialog box, select the class to view, and then click **OK**.

Targeting a group

Groups are included in the dialog box for selecting a target, but you will receive a warning if you select one. The reason for this is that there is rarely a case where you will want to select one. Monitors and rules run on the agent that manages their target object. The workflow will not enumerate the contents of the group but will attempt to run against the group object itself. Since groups are managed by the management server currently running the Root Management Server services, any workflows targeted at them will be loaded only on that server.

If you do want to have a monitor or rule run only on the members of a particular group, then you can use the following procedure. Note that this is not an ideal strategy, and under most circumstances it would be more effective to create a target for your application as described in Creating a new target.

To create a monitor or rule that runs on agents in a group

1. Create the monitor or rule and use Windows Computer for the target.
2. Disable the monitor or rule that you just created.
3. Create an override to enable the monitor or rule for the group.

Selecting a group for a monitoring wizard

Certain monitoring wizards will require a group to be specified. This specifies the group of computers that will be searched to determine if they have the component that the wizard is monitoring. For example, if you run the Windows Service monitoring wizard, you specify the name of a service to monitor. The wizard will search all computers in the target group that have the service installed. Only those computers with the service will be monitored.

Examples

- If you want the wizard to include all Windows agents in your management group, select **All Windows Computers**.
- If you want the wizard to include all Unix agents in your management group, select **Unix Computer Group**.

- If you want the wizard to include all computers running SQL Server 2008 in your management group, then select **SQL 2008 Computers**.
- If you want the wizard to include all computers running any version of SQL Server in your management group, then select **SQL Computers**.

Creating a new target

There are multiple methods that you can use to create a new class that can be used as a target for monitors and rules in System Center 2012 – Operations Manager. Any classes in a management pack created by the Visio Management Pack Designer can be used as a target. Advanced authors can refer to the Service Model section of the System Center Operations Manager 2007 R2 Authoring Guide for detailed information on creating a complex class model for their application. This advanced information is not required though to create a basic class that can act as a target for monitors and rules specific to a particular application.

Management Pack Templates

The following management pack templates in the Operations console create a class that can be used as a target for monitors and rules:

Windows Service Template

If your application has service a Windows installed on each server, then you should use the Windows Service Template. This will create a new class and discover an instance on all agent computers with the service installed. If any monitors or rules use this class as a target, then they will run on those same agents.

Process Monitoring Template

If your application does not have a Windows service but does have a process that is running on the agent computer, then you should use the Process Monitoring Template. This will create a new class and discover an instance on all computers in a specified group. If any monitors or rules use this class as a target, then they will run on those same agents.

Unix/Linux Service

If your application has a service on a Unix or Linux server, then you should use the UNIX or Linux Process template. This will create a new class and discover an instance on all agent computers with the service installed.

Simple class using Authoring Console

The System Center Operations Manager 2007 R2 Authoring Console is typically used by advanced users for custom management packs. It can be used though to create a simple class and discovery that you can then install in your management group and perform further authoring using the Operations console.

In addition to the class, you must create a discovery so that instances of the class can be created on agents where the application is installed. The Authoring Console provides a wizard that creates a discovery based on the Windows registry. This will allow you to specify criteria such as the name of a registry key. If the key is present, then the application is installed, and an instance of the class should be created.

To create a class and discovery in the Authoring Console

1. Open the Authoring Console.
2. Select **File** and then **New**.
3. On the **Management Pack Template** page, do the following:
   a. In the **Select a Management Pack Template** pane, select **Windows Application (Registry)**.
   b. For the **Management Pack Identity**, type a name such as **Contoso.MyApplication**.

      Note
      This name may not contain spaces and should start with the name of the management pack.

   c. Click **Next**.
4. On the **Name and Description** page, type a **Display Name** such as **Contoso My Application** for the management pack and click **Next**.
5. On the **Windows Application** page, do the following:
   a. In the **ID** box, type a unique ID for the new class such as *Contoso.MyApplication.MyTarget*.

      Note
      This name may not contain spaces and should start with the name of the management pack.

   b. In the **Display Name** box, type a display name for the new class such as *My Application Target*
   c. Click **Next**.
6. On the **Discovery Schedule** page, set the schedule to 1 hour or more and click **Next**.

   Note
   This is the frequency that registry criteria on the agent computer will be evaluated to determine if an instance of the class should be created.
7. On the **Registry Probe Configuration** page, do the following:

Note
On this page, you specify the registry keys and values that your criteria will use.

a. Click **Add**.
b. Leave the **Object Type** set to **Key**.
c. In the **Name** box, type a name such as **KeyExists**.

Note
You can use any name that is descriptive. The name is not displayed to the user and is only used on the next page of the wizard.

d. In the **Path** box, type the path of the registry key to check such as **SOFTWARE\MyApplication**.
e. In the **Attribute Type** box, select **Check if exists**.
f. Click **Next**.

8. On the **Expression Filter** page, do the following:

Note
On this page, you specify the criteria for evaluating the registry data collected on the previous page.

a. Click **Insert**.
b. Click the ellipse button next to **Parameter Name** and select **KeyExists**.
c. In the **Operator** box, select **Equals**.
d. In the **Value** box, type **True**.
e. Click **Create**.

To install the management pack from the Authoring Console

1. Select **Tools** and then **Export MP to Management Group**.
2. Select or type in the name of a management server for your management group.
3. Click **Connect**.

See Also

Understanding Classes and Objects

Selecting a target

Management Pack Templates

Attributes

Attributes in Operations Manager are properties of a class. Each instance of the class has the same set of attributes, but each instance can have its own value for each attribute. These values are populated when the object is discovered.

Uses for Attributes

The following table lists different ways that attributes can be used.

Management Pack Element	How attributes can be used
Views and Dashboards	A view or dashboard can include all objects with a particular value for an attribute.
Groups	A group can define criteria for dynamic membership that populates the group with all objects that have a particular value for an attribute.
Monitors and Rules	The value of an attribute can be used in the definition of the monitor or rule. For example, a monitor may run a script that requires information from the target object. An attribute could be used as a command line parameter sent to the script.
Alert Descriptions	An alert description created by a monitor or rule can include values from the data or from the attributes of the target object.

Custom Attributes

You may want to add custom attributes to existing classes so that you can collect additional information supporting views and groups in your environment. You can add attributes to any class and populate it with data retrieved from the registry or from a WMI query.

When you create a new attribute, a new class is created based on the existing class. The new class has the new attribute and inherits all of the attributes from the original class, so that it is interchangeable with the original class. In order to use the new attribute, you must select the new class. An instance of the new class will be discovered for each member of the original class and the new attribute populated only on those agents where the specified data is found.

Warning

When you create a new attribute in the Operations console, a new class is created for each custom attribute that you create. Even if you create multiple attributes on the same class, a new class will be created for each one. Too many classes can result in excessive overhead. If you create more than a few custom attributes for a class, you should use another tool such as the System Center Operations Manager 2007 R2 Authoring Console that will allow you to create a single class with multiple attributes.

Wizard Options

When you run the **Create Attribute Wizard**, you will need to provide values for options in the following tables. Each table represents a single page in the wizard.

General Properties

The **General Properties** page includes the name and description of the attribute.

Option	Description
Name	The name of the attribute that will be displayed in the Operations console.
Description	Optional description of the attribute.

Discovery Method

The **Discovery Method** page includes the method for populating the attribute and the class that it will target.

Option	Description
Discovery Type	Specifies if the value of the attribute will be populated from the registry or from a WMI query.
Target	The class to which to add the attribute.
Management Pack	Management pack to store the attribute. For more information on management packs, see Selecting a Management Pack File.

Registry Probe Configuration

The **Registry Probe Configuration** page includes the details of the registry key or value used to populate the attribute. This page is only displayed if the **Discovery Type** is **Registry**.

Option	Description
Key Or Value Type	Specifies if a registry key or registry value will be used. The data in a registry value can be used for the attribute, while it can only return a true or false indicating if a registry key exists.
Path	The path to the registry key or value.
Attribute Type	The type of data stored in the registry value. **Check if exists** can be selected if you only want to determine if a registry key or registry value exists.
Frequency	Specifies how often the discovery of the attribute should run. This should typically be a value of an hour or higher since the values of attributes rarely change.

WMI Configuration

The **WMI Configuration** page includes the details of the WMI query used to populate the attribute. This page is only displayed if the **Discovery Type** is **WMI Query**.

Option	Description
WMI Namespace	The WMI namespace with the class used in the query.
Query	The WMI query to run.
Property Name	The name of the property from the WMI query with the value to populate the attribute.
Frequency	Specifies how often the discovery of the attribute should run. This should typically be a value of an hour or higher since the values of attributes rarely change.

Creating custom attributes

The following example procedure creates an attribute with the following details:

- New attribute named **Location** on all instances of **Windows Computer**.
- Value populated from a registry key at HKLM\SOFTWARE\Contoso\Location.

To create a new attribute using the registry

1. If you don't have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. In the Operations console, select the **Authoring** workspace, and then expand **Management Pack Objects**.
3. Right-click Attributes and select **Create a new attribute**.
4. On the **General** page, do the following:
   a. In the **Name** box, type **Location**.
   b. Click **Next**.
5. On the **Discovery Method** page, do the following:
   a. In the **Discovery Type** dropdown, select **Registry**.
   b. Click **Browse** to select the target class.
   c. Select **Windows Computer** and then click **OK**.
   d. In the Management Pack box, select the management pack from step 1.
   e. Click **Next**.
6. On the **Registry Probe Configuration** page, do the following:
   a. For **Key or Key Value Type** select **Value**.
   b. In the **Path** box, type **SOFTWARE\Contoso\Location**.
   c. In the **Attribute Type** dropdown, select **String**.
   d. In the **Frequency** box, type **3600** seconds.
   e. Click **Finish**.

The following example procedure creates an attribute with the following details:

- New attribute named **Manufacturer** on all instances of **Windows Computer**.
- Value populated from a WMI query using the **Win32_ComputerSystem** class.

To create a new attribute using WMI

1. If you don't have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. In the Operations console, select the **Authoring** workspace, and then expand **Management Pack Objects**.
3. Right-click Attributes and select **Create a new attribute**.
4. On the **General** page, do the following:
   a. In the **Name** box, type **Location**.
   b. Click **Next**.
5. On the **Discovery Method** page, do the following:
   a. In the **Discovery Type** dropdown, select **WMI Query**.
   b. Click **Browse** to select the target class.

c. Select **Windows Computer** and then click **OK**.
d. In the Management Pack box, select the management pack from step 1.
e. Click **Next**.

6. On the **WMI Configuration** page, do the following:
   a. In the **WMI Namespace** box, type **root\cimv2**.
   b. In the **Query** dropdown, type **select * from win32_computersystem**.
   c. In the **Property Name** box, type **Manufacturer**.
   d. In the **Frequency** box, type **3600** seconds.
   e. Click **Finish**.

See Also

Base Classes

Script Monitors and Rules

Alerts

Management Pack Templates

Management Pack Templates provide *Monitoring wizards* that let you create complete monitoring scenarios with minimal input. The wizard creates the required monitors, rules, and even targets to implement the particular scenario. There is no requirement for you to understand the management pack elements that are created. You can modify the configuration of the wizard itself if you want to change the way that monitoring is being performed.

Conceptual view of a monitoring wizards

If a management pack template is available for your particular monitoring requirement, using the template most likely is your best strategy. In many cases, you could create the individual rules and monitors yourself, but this exercise is significantly more complex than using an available template. In addition, some templates perform actions that you cannot perform in any other way in the Operations console.

The following table lists the management pack templates that are part of the standard Operations Manager installation. You can install other management packs that might provide additional templates. Each of these templates is covered in detail in subsequent sections of this guide.

Template	Description
.NET Application Performance Monitoring Template	Monitor .NET applications to get details about application performance and reliability.
OLE DB Data Source Template	Monitor a database accessible with OLE DB.
Process Monitoring Template	Discover and monitor instances of a particular Windows process.
TCP Port Template	Monitor the availability of an application that is listening on a specific port.
UNIX or Linux Log File	Monitor a UNIX or Linux log file for a specific entry.
UNIX or Linux Process	Monitor a UNIX or Linux process.
Web Application Availability Monitoring Template	Monitor the availability of one or more web application URLs and run these monitoring tests from internal locations.
Web Application Transaction Monitoring Template	Monitor the availability, operation, and performance of a web application.
Windows Service Template	Discover and monitor instances of a particular Windows service.

See Also

Creating Management Pack Templates

Watcher Nodes

Creating Management Pack Templates

Use the following procedure to create and modify management pack templates.

To create a management pack template

1. Start the Operations console with an account that has Author credentials in the management group.
2. Open the **Authoring** workspace.
3. In the **Authoring** navigation pane, right-click the **Management Pack Templates** node, and then click **Add Monitoring Wizard**.
4. Select the management pack template that you want to create, and then click **Next**.

5. Follow the instructions for the template that you selected. You can use the links in the table above to access this content.

To edit an existing management pack template

1. Start the Operations console with an account that has Author credentials in the management group.
2. Open the **Authoring** workspace.
3. In the **Authoring** navigation pane, expand the **Management Pack Templates** node.
4. Right-click the template to edit and then select **Properties**.

To view the elements created by the management pack template

1. Start the Operations console with an account that has Author credentials in the management group.
2. Open the **Authoring** workspace.
3. In the **Authoring** navigation pane, expand the **Management Pack Templates** node.
4. Right-click the template to view, select **View Management Pack Objects**, and then select the kind of element that you want to view.

See Also

Management Pack Templates

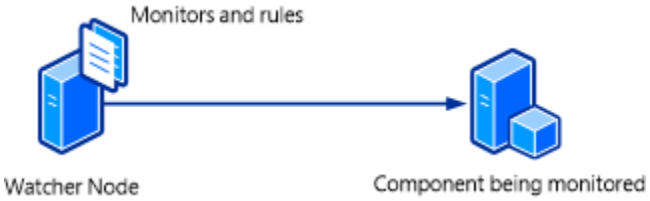
Watcher Nodes

A *watcher node* is an agent that runs monitors and rules that test an application or feature on another computer. The following management pack templates use watcher nodes:

- **OLE DB Data Source**
- **TCP Port**
- **Web Application Transaction Monitoring**

When you use one of these templates, you must specify one or more watcher nodes to run the monitor.

Conceptual view of watcher nodes



A watcher node can either be the agent with the application or feature installed, or it can be a separate agent. If the watcher node is a separate computer, in addition to ensuring that the application or feature is healthy, the watcher node can validate that clients can connect to it and test such additional features as security, network availability, and firewalls.

You can best ensure availability of an application or feature by specifying watcher nodes in different network segments. For example, a database might be accessed from application servers in each of two different network segments. While the database might be available to one set of servers, an issue such a problem with a network device could make it inaccessible to servers on the other segment. If you use the **OLE DB Data Source** template to create a monitor for the database with a watcher node in each segment, you are assured that any problem accessing the database is detected.

You can also specify the computer with the application or feature itself as a watcher node. This watcher node performs the test without relying on any external features.

See Also

TCP Port Template

OLE DB Data Source Template

Web Application Transaction Monitoring Template

.NET Application Performance Monitoring Template

The **.NET Application Performance Monitoring** (APM) template in System Center 2012 – Operations Manager lets you monitor Internet Information Services (IIS)-hosted .NET applications from server- and client-side perspectives to get details about application performance and reliability that can help you pinpoint root causes of incidents. (For System Center 2012 SP1 only: You can also monitor Windows Services.) When you specify settings, the types of events to collect, the performance goals to measure, and servers to monitor, .NET Application Performance Monitoring reveals how applications are running. You can see how frequently a problem is occurring, how a server was performing when a problem occurred, and the chain of events related to the slow request or method that is raising exceptions. This information is required to partner with software developers and database administrators to help ensure that applications perform correctly and reliably for your customers.

This template lets you monitor applications and web services that are hosted in Internet Information Services (IIS) 7.0. You can select one or more applications or services discovered by the IIS 7.0 management pack and configure monitoring of performance and exception events. You must have the Windows Server 2008 Internet Information Services (IIS) 7.0 management pack installed to monitor applications and web services.

For System Center 2012 SP1, you can use the template to monitor applications and web services that are hosted in Internet Information Services (IIS) 8.0. You can select one or more applications or services discovered by the IIS 8.0 management pack and configure monitoring of performance and exception events. You must have the Windows Server 2012 Internet Information Services (IIS) 8.0 management pack installed to monitor applications and web services.

For more information, see Before You Begin Monitoring .NET Applications

Scenarios

Monitoring Performed by the .NET Application Performance Monitoring Template

Viewing Monitoring Data

Wizard Options

Server-Side Configuration

Advanced Settings for Server-Side Monitoring

Server-Side Customization

Server-Side Modifying Settings

Transaction Properties: Add ASP.NET Web Page

Transaction Properties: Add ASP.NET Web Service

Transaction Properties: Add ASP.NET MVC Page

Transaction Properties: Add WCF Method

Transaction Properties: Add Function

Client-Side Configuration

Advanced Settings for Client-Side Monitoring

Enable Client-Side Monitoring

Client-Side Modifying Settings

Summary

Creating and Modifying .NET Application Performance Monitoring Templates

Viewing .NET Application Performance Monitoring Monitors and Collected Data

Scenarios

Use the **.NET Application Performance Monitoring** template in scenarios where you have to monitor web-based applications. These scenarios include the following monitoring processes:

Server-Side Monitoring: Single- or Multi-Tier Web Applications

You might have applications that must be running at all times. Use the **.NET Application Performance Monitoring** template to ensure that your applications are reliable, have no exceptions, and meet service level agreements (SLAs), in short, that they perform correctly on the computers where they are installed.

Client-Side Monitoring: Browser Performance and Reliability

You want to ensure that your customers are having quality web experiences. By creating or editing existing templates, you can extend your server-side monitoring by adding client-side monitoring that measures the browser experience of your customers.

Monitoring Performed by the .NET Application Performance Monitoring Template

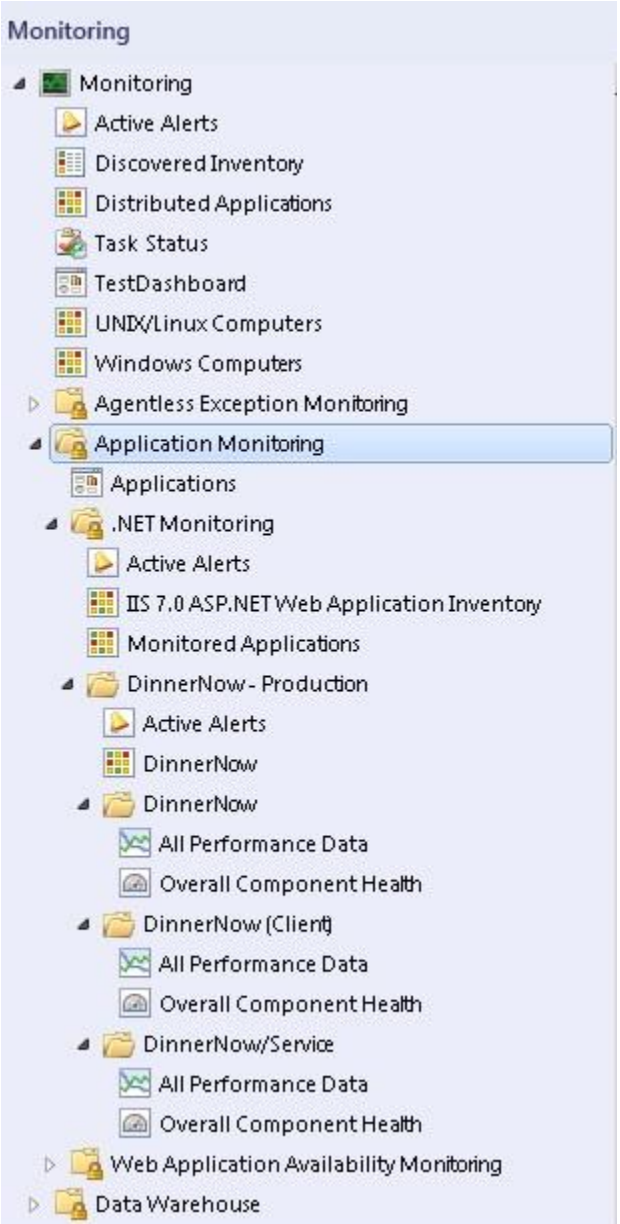
By default, the **.NET Application Performance Monitoring** template configures the following monitoring. You can be enable, disable, and modify monitors in the **Advanced Configuration** page of the **.NET Application Performance Monitoring** template.

Monitor description	Default values
Percentage of exception events per monitored requests	Enabled, Threshold=15%, Interval=5 minutes
Percentage of performance events per monitored requests	Enabled, Threshold=20%, Interval=5 minutes
Average Request Time	Enabled, Threshold=10,000 ms, Interval=5 minutes

Viewing Monitoring Data

All data collected by the **.NET Application Performance Monitoring** template appears in the **.NET Monitoring** folder in the **Application Monitoring** folder in the **Monitoring** navigation pane. For each of the application groups that you create by using the **.NET Application Performance Monitoring** template, the template creates a folder under **.NET Monitoring**. The **Application Monitoring** folder contains the default views and subfolders that provide health state, Performance views, and alerts related to the application components in the application group. By using the top-level Application Group State view, you can see the health of the individual components and the monitoring configurations that have been enabled. The state of each object matches the state of the targeted object that has the worst health state so that you see the worst state of the monitors that are running. If one or more of the components are shown with an error while at least one other component is healthy, it could indicate a problem with that particular component, such as a credential issue. If all of the components are unhealthy, it could indicate a problem with the infrastructure, such as network connectivity issues.

Application Monitoring folders

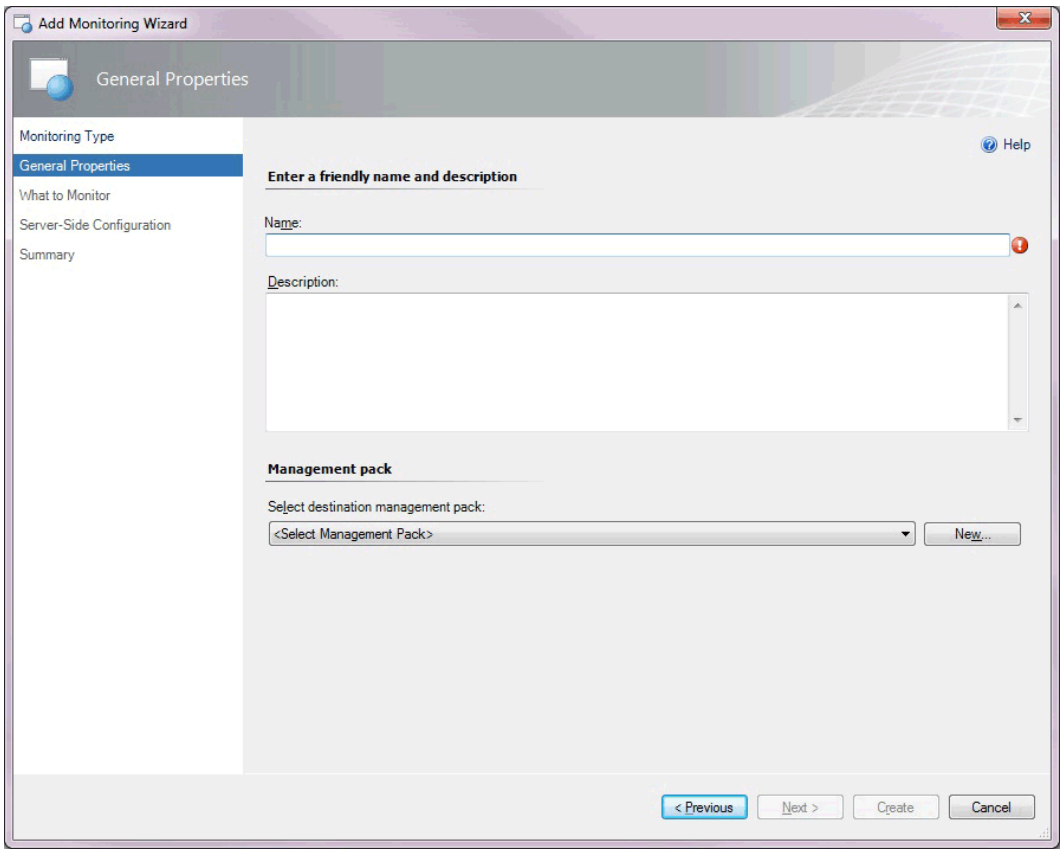


To view the state of the individual monitors, open the Health Explorer for each component. Drill down to the unhealthy monitors to see what is making your application unhealthy. For more information, see Monitoring .NET Applications

Wizard Options

When you run the **.NET Application Performance Monitoring** template, you have to provide values for options as listed in the following tables. Each table represents a single page in the wizard.

General Properties

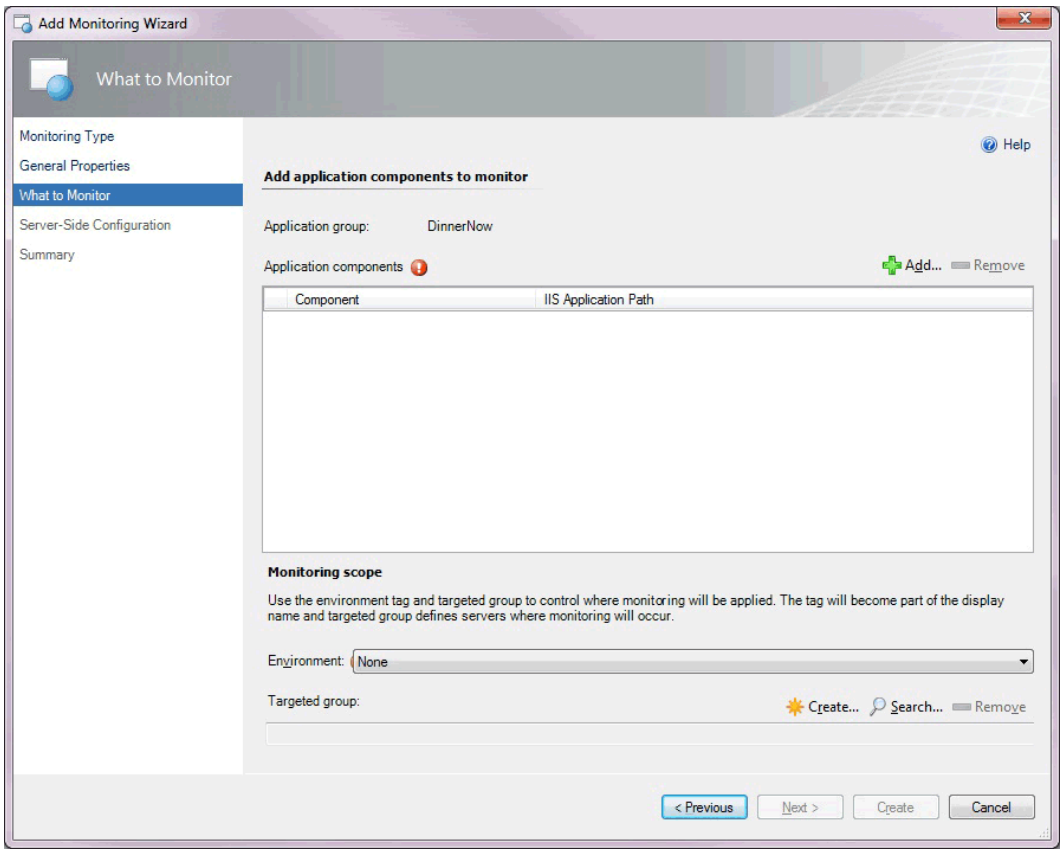


The following options are available on the **General Properties** page of the wizard.

Option	Description
Name	Enter the friendly name used for the template and application group that you are creating. This name is displayed in the Operations console and used for the folder under the **.NET Monitoring** folder. **Note** After you have given the template a name and saved the template, this name cannot be edited without deleting and re-creating the template instance.
Description	Describe the application group. (Optional)
Select destination management pack	Select the management pack to store the views and configuration created by the template. Use

Option	Description
	the same name for your new management pack as the application group so you can easily pair the two names. You can use an existing management pack or create a new management pack. For more information about management packs, see Selecting a Management Pack File.

What to Monitor



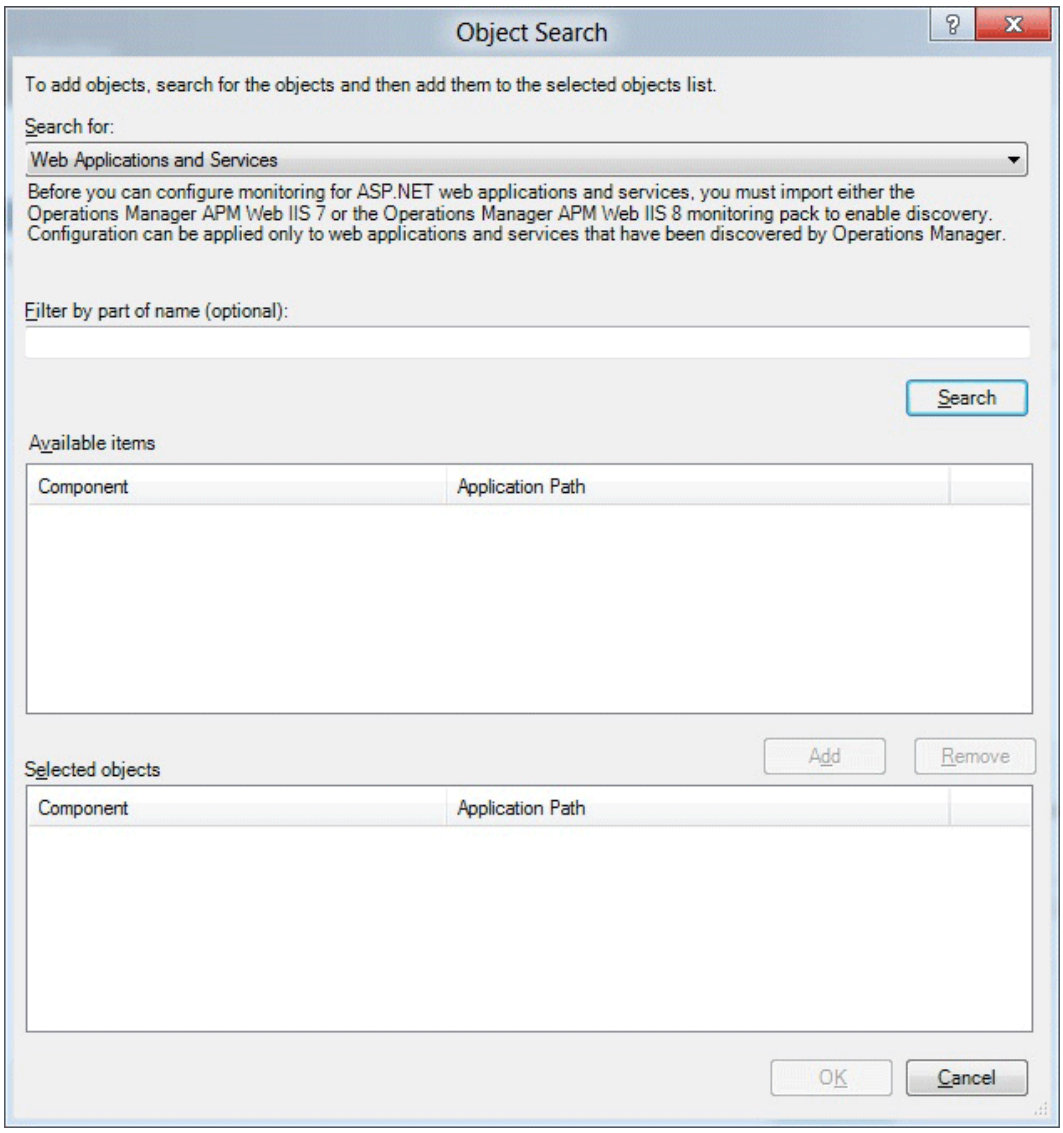
The following options are available on the **What to Monitor** page of the wizard.

Option	Description
Application components, Add	Search for and add or remove the application components to monitor. When you click **Add**, the Object Search page

Option	Description
	opens, which lets you select whether you want to monitor Web Applications and Services. For System Center 2012 SP1 only: You can monitor Windows Services. **Note** For System Center 2012 SP1 only: Before you begin monitoring Windows Services, you need to configure Windows Services using the Windows Service template. Once you do this, the.NET Application Performance Monitoring template can discover the Windows Services that are running. For more information, see Authoring the Windows Service Template.
Environment	Select the environment in which you want to monitor your application: **None**, **Production**, **Staging**, **Test**, **Development**, or use **New** to create a new tag. Typically, you want to pair the environment tag with the server group that you are monitoring. The tag is appended to the application group name and component names, letting you differentiate the event data in Application Diagnostics and Application Advisor. From a monitoring perspective, the environment tag lets you separate the same application into multiple virtual applications. **Note** After you have selected an environment tag and saved the template, the tag cannot be edited without deleting and re-creating the template instance.
Targeted group	Select specific servers to limit monitoring to this specific set of servers. This is optional. Targeted group scoping only becomes necessary when you have the same application running in multiple environments, such as production and staging, and you intend to run

Option	Description
	the template multiple times, one for each environment. In this scenario, group which machines belong to production and which belong to the staging environment, and then use the targeted groups to restrict where the configuration is propagated. You can also use groups to apply configuration to a subset of your servers. Otherwise, it is not necessary to specify targeted group scoping if you just want to monitor all instances of a given application.

Object Search

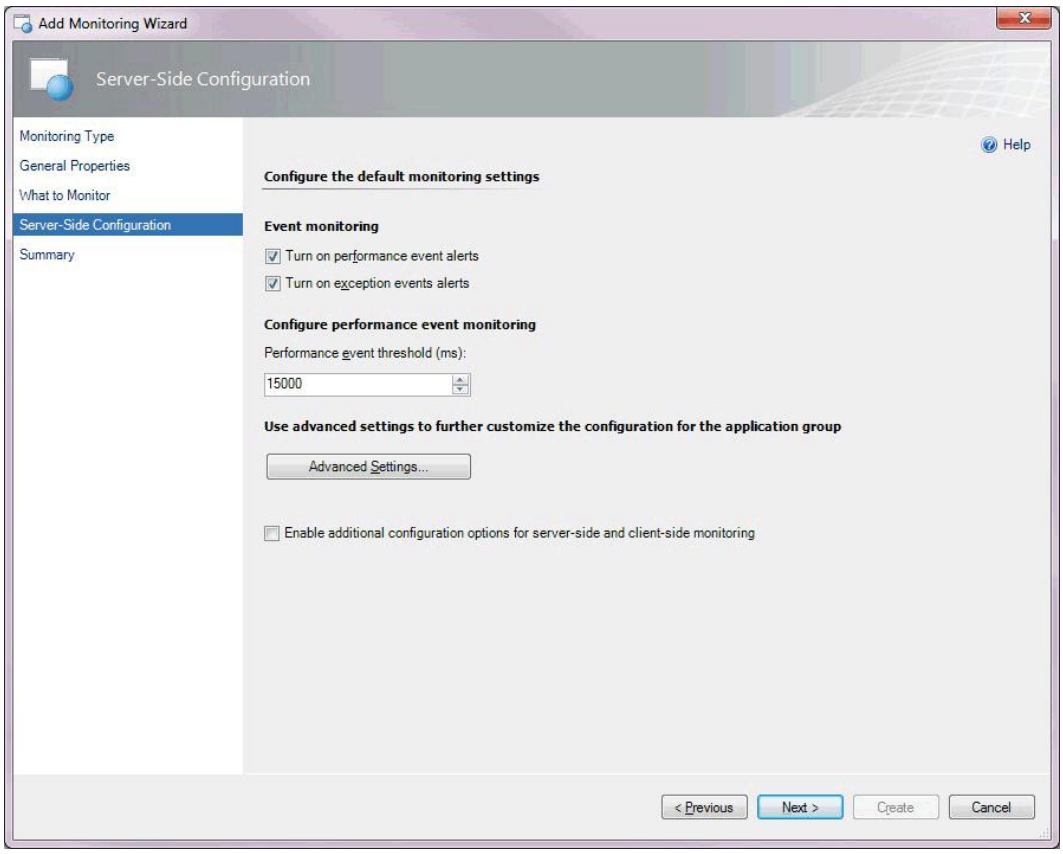


The following options are available on the **Object Search** page of the wizard.

Option	Description
Search for	Select Web Applications and Services. For System Center 2012 SP1 only: You can also select Windows Services. **Note** For System Center 2012 SP1, before you begin monitoring Windows

Option	Description
	Services, you need to configure Windows Services using the Windows Service template. Once you do this, the.NET Application Performance Monitoring template can discover the Windows Services that are running. For more information, see Authoring the Windows Service Template
Filter by part of name (optional)	Enter part of the name of Web Application and Services that you want to select. For System Center 2012 SP1 only: You can also enter part of the name of a Windows Service that you want to select.
Available items	Displays the Windows Web Application and Services that are available for monitoring. For System Center 2012 SP1 only: Also displays the Windows Services that are available for monitoring.
Selected objects	Displays the application components that you have selected to monitor.

Server-Side Configuration

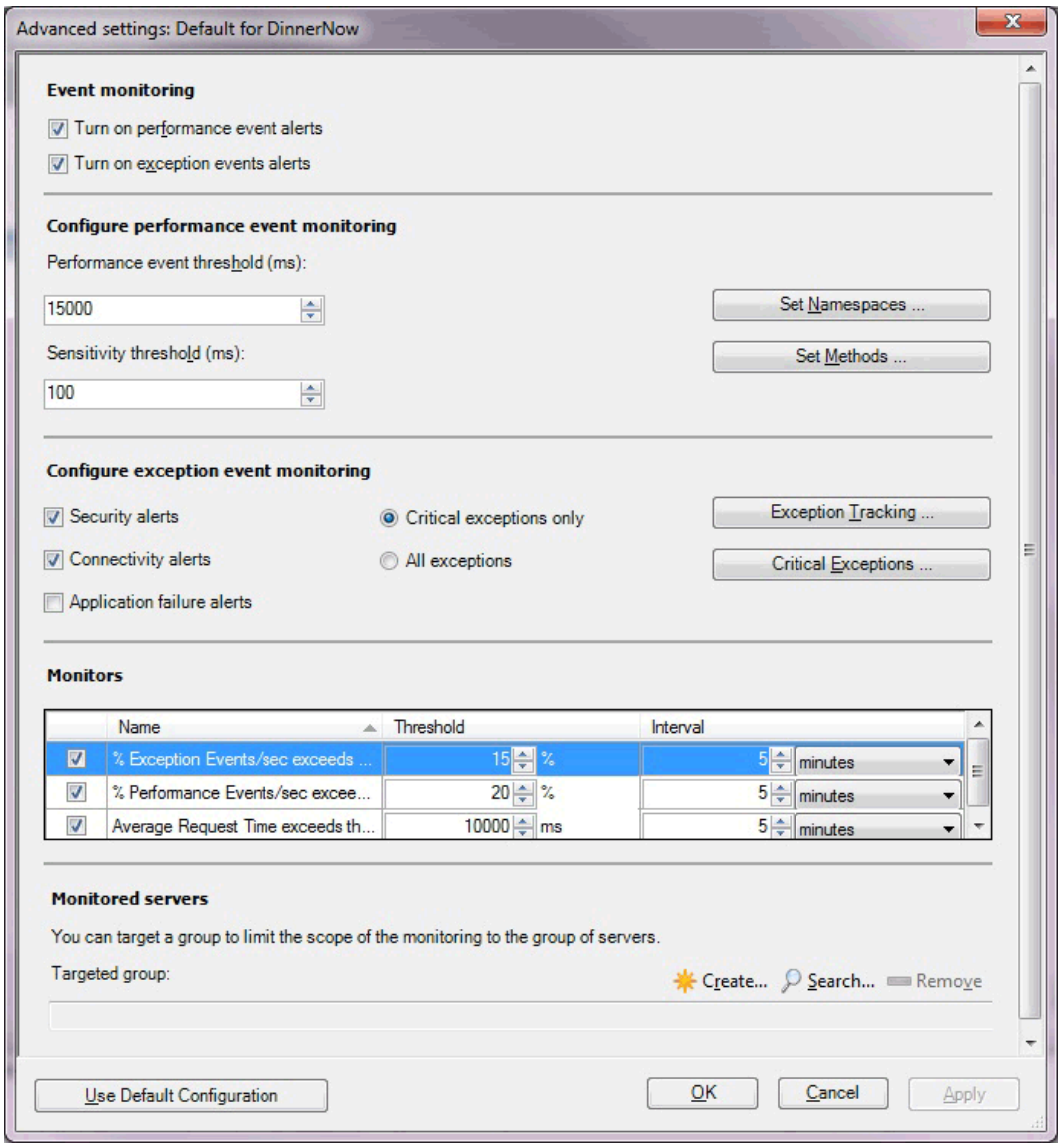


The following options are available on the **Server-Side Configuration** page of the wizard.

Option	Description
Turn on performance event alerts	Turn performance event alert reporting for the application group on or off within the Operations console for server-side monitoring. Performance events are still logged to the Application Diagnostics console. You have the option whether to raise alerts after an Application Performance Monitoring event is generated.
Turn on exception event alerts	Turn the exception event alert notification for the application group on or off within the Operations console for server-side monitoring. Exception events are still logged to the Application Diagnostics console. You have the option whether to raise alerts after an

Option	Description
	Application Performance Monitoring event is generated.
Performance event threshold (ms)	Set the threshold in milliseconds (ms) that a user transaction must exceed before it raises a performance event.
Advanced Settings	Set advanced configurations, including sensitivity (restricting the collection of fast functions), namespaces (that define where you want to collect data from custom applications), methods (specific functions where you want to start monitoring), custom exception handlers (that define critical exceptions), and customize the configuration of the monitors that affect the component health state.
Enable additional configuration options for server-side and client-side monitoring	Specify additional options in the wizard to customize monitoring for individual application components and client-side monitoring.

Advanced Settings for Server-Side Monitoring



The following options are available on the **Advanced Settings** for server-side monitoring page of the wizard.

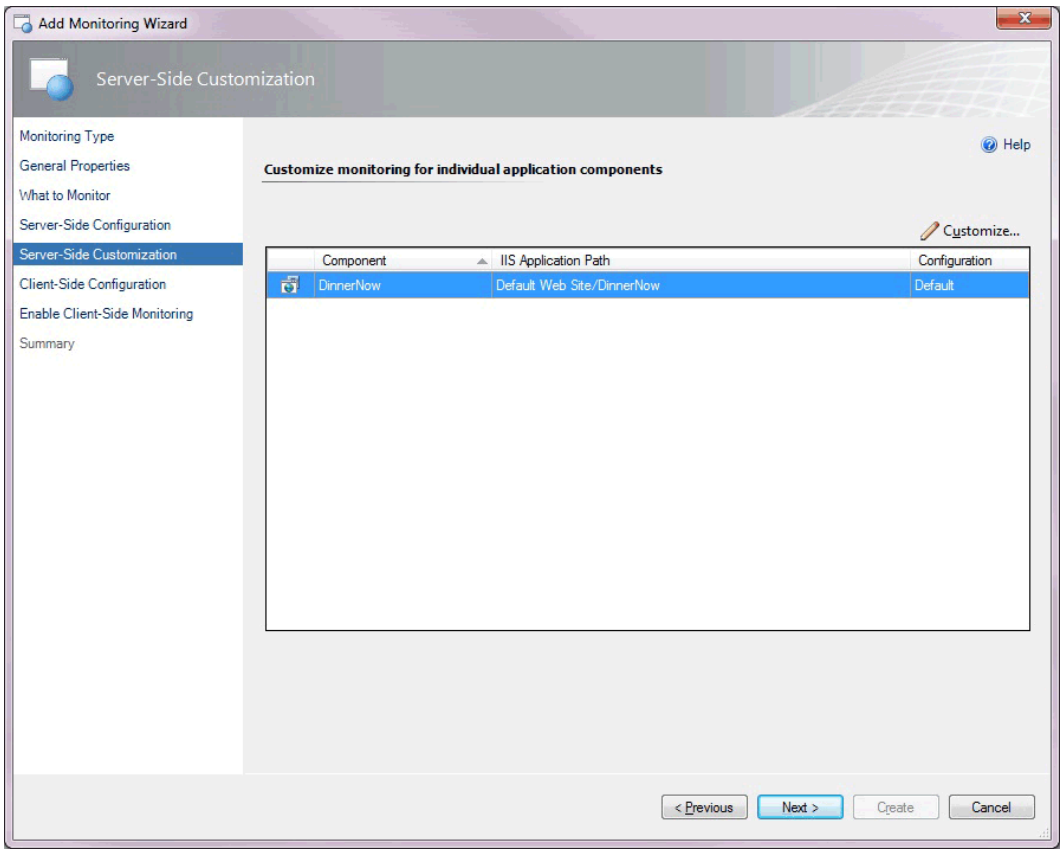
Option	Description
Turn on performance event alerts	Turn performance event alert reporting for the application group on or off within the Operations console for server-side monitoring. Performance events are still logged to the Application Diagnostics console. You have the option whether to raise alerts after an

Option	Description
	Application Performance Monitoring event is generated.
Turn on exception event alerts	Turn the exception event alert notification for the application group on or off within the Operations console for server-side monitoring. Exception events are still logged to the Application Diagnostics console. You have the option whether to raise alerts after an Application Performance Monitoring event is generated.
Performance event threshold (ms)	Set the threshold in milliseconds (ms) that a request must be processed in before it causes a performance event.
Sensitivity threshold (ms)	Specify to filter out fast-running methods to reduce overall “noise” by reducing the size of the call stack by gathering less data for each event. For more information, see Authoring Strategies for .NET Application Monitoring
Set Namespaces	Specify namespaces and classes where to start measuring for performance events and performance threshold violations, and define which namespaces should be treated by default as entry points. For more information, see How to Add, Enable, and Disable Namespaces
Set Methods	Specify how deep in the call stack to drill down to collect more detailed information, such as parameters and variables, for specific methods. For more information, see How to Add, Edit, and Remove Methods
Security alerts	Turn alerting of exceptions on or off that are classified as security alerts for the application group, with errors such as “Access Denied” or “Login Failed”. Security events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.

Option	Description
Connectivity alerts	Turn alerting of exceptions on or off that are classified as connectivity alerts for the application group, with errors such as “Connection timed out”. Connectivity events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Application failure alerts	Turn alerting of exceptions on or off that are classified as application, or code, failures for the application group. By default, this option is turned off to reduce the “noise” of alerts raised due to code failures that typically only development teams can resolve. For more information, see Authoring Strategies for .NET Application Monitoring Exception events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Critical exceptions only	Specify whether the exception is considered relevant by the Application Performance Monitoring agent and whether an event is created. An event is created if the exception raised is one of those in the list of critical exception handlers. For more information, see Using Exception Handlers to Define Critical Exceptions
All exceptions	Specify whether all exceptions are considered relevant by the Application Performance Monitoring agent and events are created when exceptions are detected in monitored namespaces and classes.
Exception Tracking	Select to add namespace or classes where you track exception parameters or variables, and collect additional information about each exception that a namespace or class raised.

Option	Description
	For more information, see How to Add, Edit, and Remove Exception Tracking
Critical Exceptions	Select to add items to the Exception handlers list. Define exception handlers that catch critical exceptions that an application raised. For more information, see Using Exception Handlers to Define Critical Exceptions
Monitors: Exception Events/sec exceeds	Monitor that watches the .NET App/% Exception Events/sec performance counter.
Monitors: Performance Events/sec exceeds	Monitor that watches the .NET Apps/% Performance Events/sec performance counter.
Monitors: Average Request Time exceeds	Monitor that watches the .NET Apps/Average Request Time performance counter.
Targeted group	Select specific servers to limit monitoring to this specific set of servers. This is optional. Targeted group scoping only becomes necessary when you have the same application running in multiple environments, such as production and staging, and you intend to run the template multiple times, one for each environment. In this scenario, group which machines belong to production and which belong to the staging environment, and then use the targeted groups to restrict where the configuration is propagated. You can also use groups to apply configuration to a subset of your servers. Otherwise, it is not necessary to specify targeted group scoping if you just want to monitor all instances of a given application.

Server-Side Customization

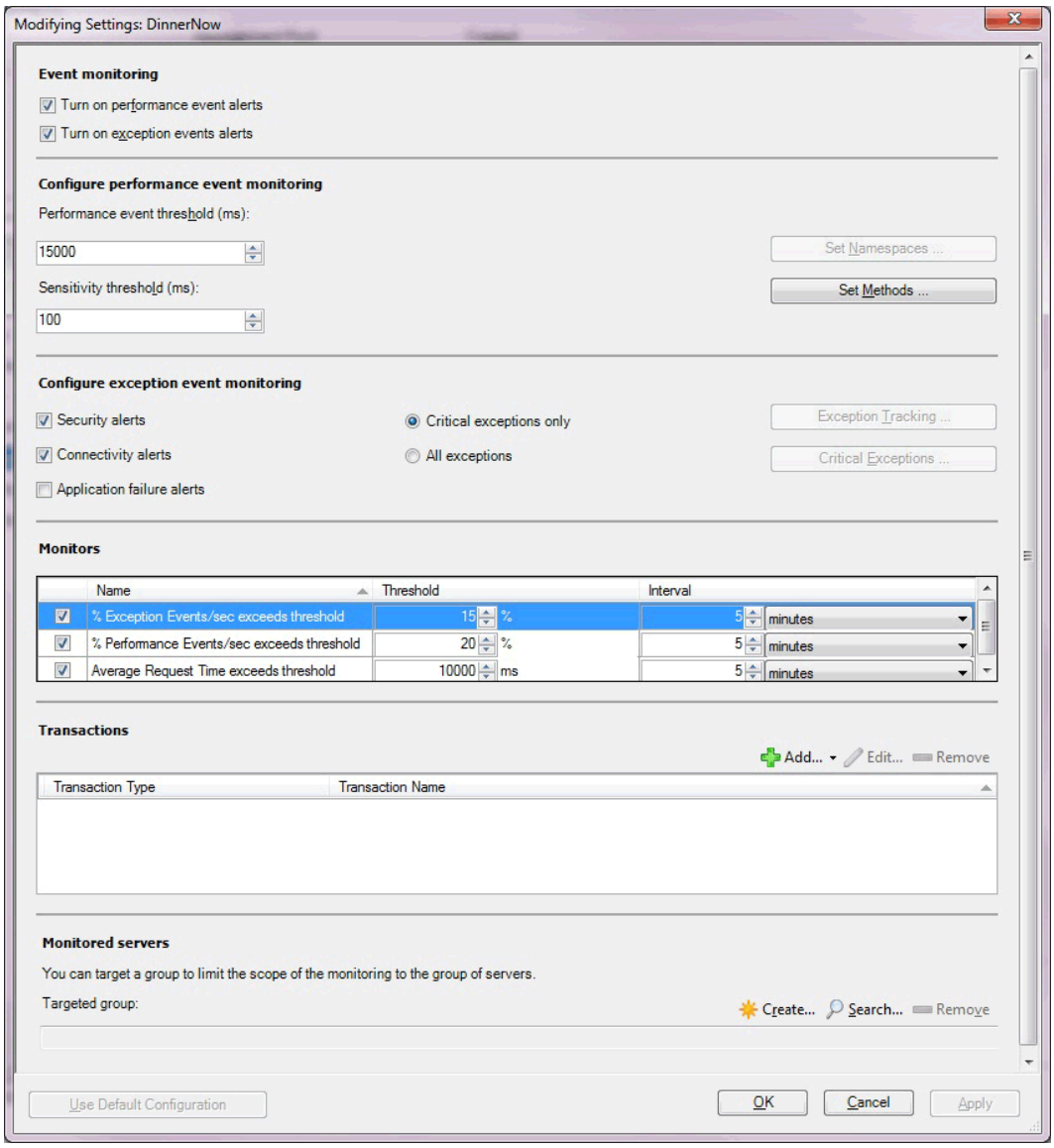


For System Center 2012 SP1, the following options are available on the **Server-Side Customization** page of the wizard.

Option	Description
Component	Select the component you want to customize for monitoring individual application components.
Customize	Modify the settings for the selected application component. This opens the **Modifying Settings** page. The settings on this page are the same as those on the **Advanced Settings for Server-Side Monitoring** page, except you can create individual transaction monitoring for ASP.NET webpages, ASP.NET web services, or individual functions in an assembly. These are described in the Transaction Properties: Add ASP.NET Web Page sections that follow.

Option	Description
	Note The buttons for namespaces, exception tracking, and critical exceptions are unavailable because these can only be set at the application-group level, not at the component level. For System Center 2012 SP1 only: you can customize these settings if you are configuring monitoring for Windows Services.
Modifying Settings page	Customize settings for the application component and/or specify monitoring for a specific webpage, web method, or function within the application component.

Server-Side Modifying Settings



The following options are available on the **Server-Side Modifying Settings** page of the wizard.

Option	Description
Turn on performance event alerts	Turn performance event alert reporting for the application group on or off within the Operations console for server-side monitoring. Performance events are still logged to the Application Diagnostics console. You have the option whether to raise alerts after an Application Performance Monitoring event is

Option	Description
	generated.
Turn on exception event alerts	Turn the exception event alert notification for the application group on or off within the Operations console for server-side monitoring. Exception events are still logged to the Application Diagnostics console. You have the option whether to raise alerts after an Application Performance Monitoring event is generated.
Performance event threshold (ms)	Set the threshold in milliseconds (ms) that a request must be process in before it causes a performance event.
Sensitivity threshold (ms)	Specify to filter out fast-running methods to reduce overall “noise” by reducing the size of the call stack by gathering less data for each event. For more information, see Authoring Strategies for .NET Application Monitoring
Set Methods	Specify how deep in the call stack to drill down to collect more detailed information, such as parameters and variables, for specific methods. For more information, see How to Add, Edit, and Remove Methods
Security alerts	Turn on or off alerting of exceptions classified as security alerts for the application component, with errors such as “Access Denied” or “Login Failed”. Security events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Connectivity alerts	Turn on or off alerting of exceptions classified as connectivity errors for the application component, such as “Connection Timed Out”. Connectivity events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is

Option	Description
	generated.
Application failure alerts	Turn on or off alerting of exceptions classified as application, or code, failures for the application component. By default, this option is turned off to reduce the “noise” of alerts raised due to code failures that typically only development teams can resolve. For more information, see Authoring Strategies for .NET Application Monitoring Exception events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Critical exceptions only	Specify whether the exception is considered relevant by the Application Performance Monitoring agent and whether an event is created. An event is created if the exception raised is one of those in the list of critical exception handlers. For more information, see Using Exception Handlers to Define Critical Exceptions
All exceptions	Specify whether all exceptions are considered relevant by the Application Performance Monitoring agent and events are created when exceptions are detected in monitored namespaces and classes.
Monitors: Exception Events/sec exceeds	Monitor that watches the .NET App/% Exception Events/sec performance counter.
Monitors: Performance Events/sec exceeds	Monitor that watches the .NET Apps/% Performance Events/sec performance counter.
Monitors: Average Request Time exceeds	Monitor that watches the .NET Apps/Average Request Time performance counter.
Transactions: Add	Add transactions for ASP.NET web pages, ASP.NET Web services, and functions. See the following tables.
Targeted group	Select specific servers to limit monitoring to this

Option	Description
	specific set of servers. This is optional. Targeted group scoping only becomes necessary when you have the same application running in multiple environments, such as production and staging, and you intend to run the template multiple times, one for each environment. In this scenario, group which machines belong to production and which belong to the staging environment, and then use the targeted groups to restrict where the configuration is propagated. You can also use groups to apply configuration to a subset of your servers. Otherwise, it is not necessary to specify targeted group scoping if you just want to monitor all instances of a given application.

Note
The buttons for namespaces, exception tracking, and critical exceptions are unavailable because these can only be set at the application-group level, not at the component level. For System Center 2012 SP1 only: You can customize these settings if you are configuring monitoring for Windows services.

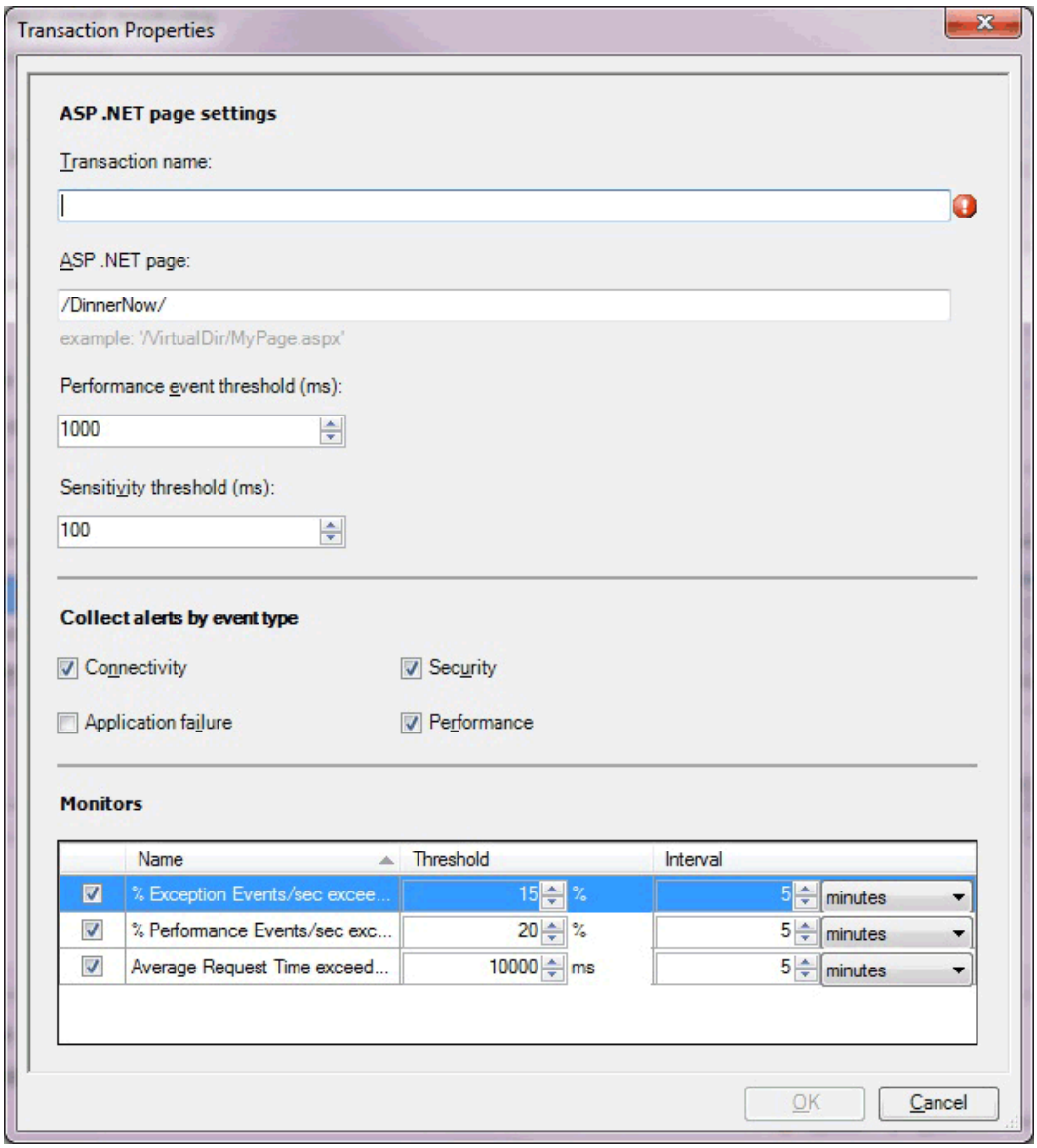
Application types and server-side transactions you can monitor

For each application type there are several transaction types you can choose to monitor. The following options are available:

Application type	Transaction types for System Center 2012	Transaction types for System Center 2012 SP1
ASP.NET Web application	• ASP.NET webpage • ASP.NET web service • Function	• ASP.NET webpage • ASP.NET MVC page • ASP.NET web service • WCF method • Function
ASP.NET Web service	• ASP.NET webpage • ASP.NET web service • Function	• ASP.NET webpage • ASP.NET MVC page • ASP.NET web service • WCF method • Function

Application type	Transaction types for System Center 2012	Transaction types for System Center 2012 SP1
WCF service	Not available	• ASP.NET webpage • ASP.NET MVC page • ASP.NET web service • WCF method • Function
Windows service	Not available	• WCF method • Function

Transaction Properties: Add ASP.NET Web Page



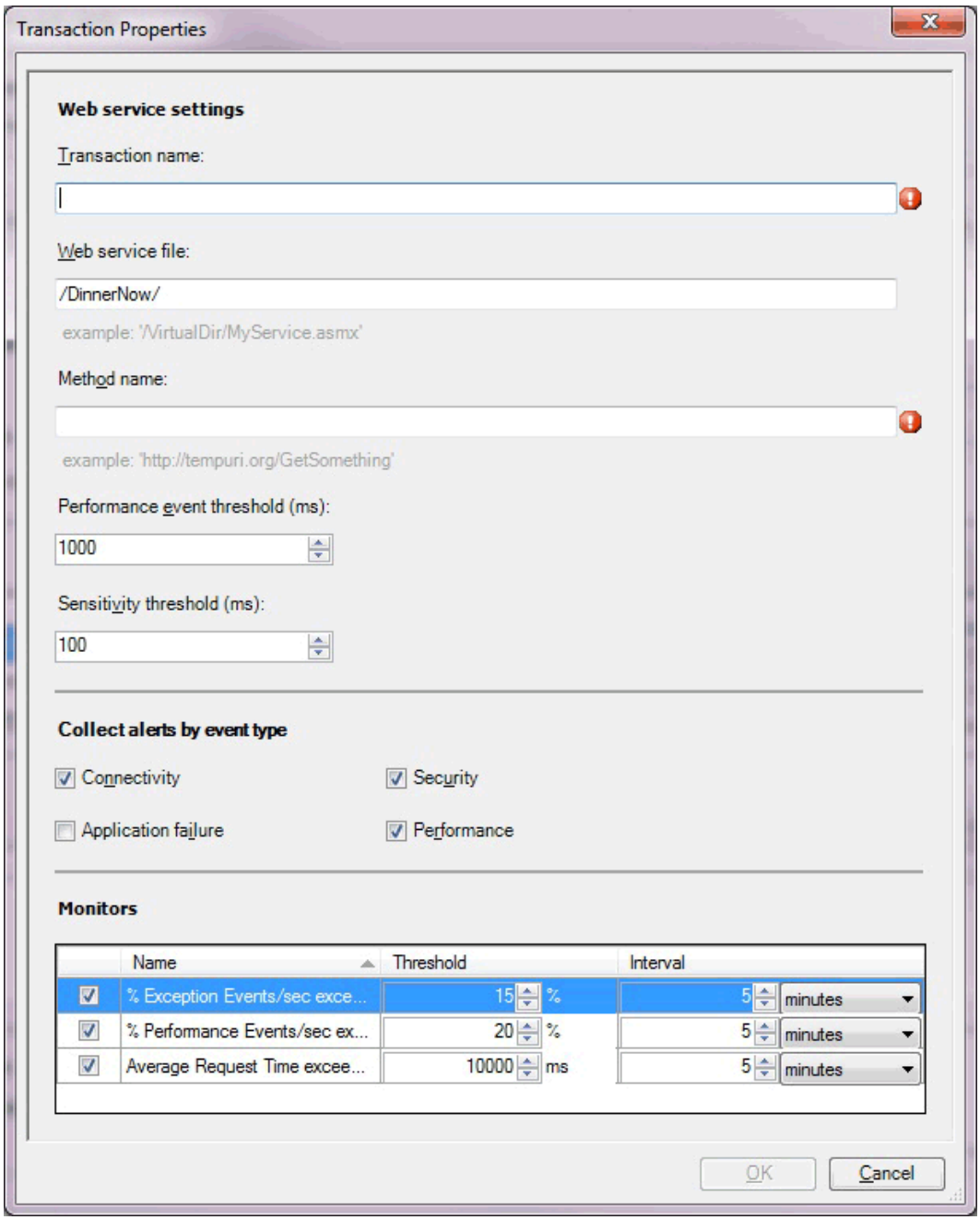
The following options are available on the **Transaction Properties** page for ASP.NET Web Page page of the wizard.

Option	Description
Transaction name	Enter the friendly name for the transaction as it will be displayed on the **Monitoring** tab, performance counters, and elsewhere.
ASP.NET page	Enter the path to the page that you are

Option	Description
	configuring these monitoring settings for.
Performance event threshold (ms)	Set the threshold in milliseconds (ms) that a user transaction must exceed before it raises a performance event. **Note** The application component continues to monitor the page specified in the transaction by using the performance threshold that is set for the application component. This threshold is used as a second measure on the same page in the application component. If you set this threshold higher than the application component threshold, you get a single event, but you might get two performance alerts for the transaction when the threshold is breached—one from the application component and one from the transaction, depending on your alerting settings. Transactions are typically used to monitor the individual page more aggressively than the parent application, at a lower threshold, or to monitor a page where alerting has been disabled on the parent.
Sensitivity threshold (ms)	Specify to filter out fast-running methods to reduce overall “noise” by reducing the size of the call stack by gathering less data for each event. An event is still generated if the threshold is surpassed. For more information, see Authoring Strategies for .NET Application Monitoring
Collect alerts by event type: Connectivity	Turn on or off alerting of events, classified as connectivity alerts with errors such as “Connection Timed Out”. Connectivity events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an

Option	Description
	Application Performance Monitoring event is generated.
Collect alerts by event type: Application failure	Turn on or off alerting of events classified as application, or code, failures. Turning this off reduces the “noise” of many alerts raised due to code failures. Because these alerts are raised from code failures, developers usually resolve these issues. For more information, see Authoring Strategies for .NET Application Monitoring Exception events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Collect alerts by event type: Security	Turn on or off alerting of events classified as security alerts, with errors such as “Access Denied” or “Login Failed”. Security events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Collect alerts by event type: Performance	Turn on or off alerting of events classified as performance alerts. Performance events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Monitors: % Exception Events/sec	Monitor that watches the .NET App/% Exception Events/sec performance counter.
Monitors: % Performance Events/sec	Monitor that watches the .NET Apps/% Performance Events/sec performance counter.
Monitors: Average Request Time	Monitor that watches the .NET Apps/Average Request Time performance counter.

Transaction Properties: Add ASP.NET Web Service



The following options are available on the **Transaction Properties** page for the **ASP.NET Web Service** page of the wizard.

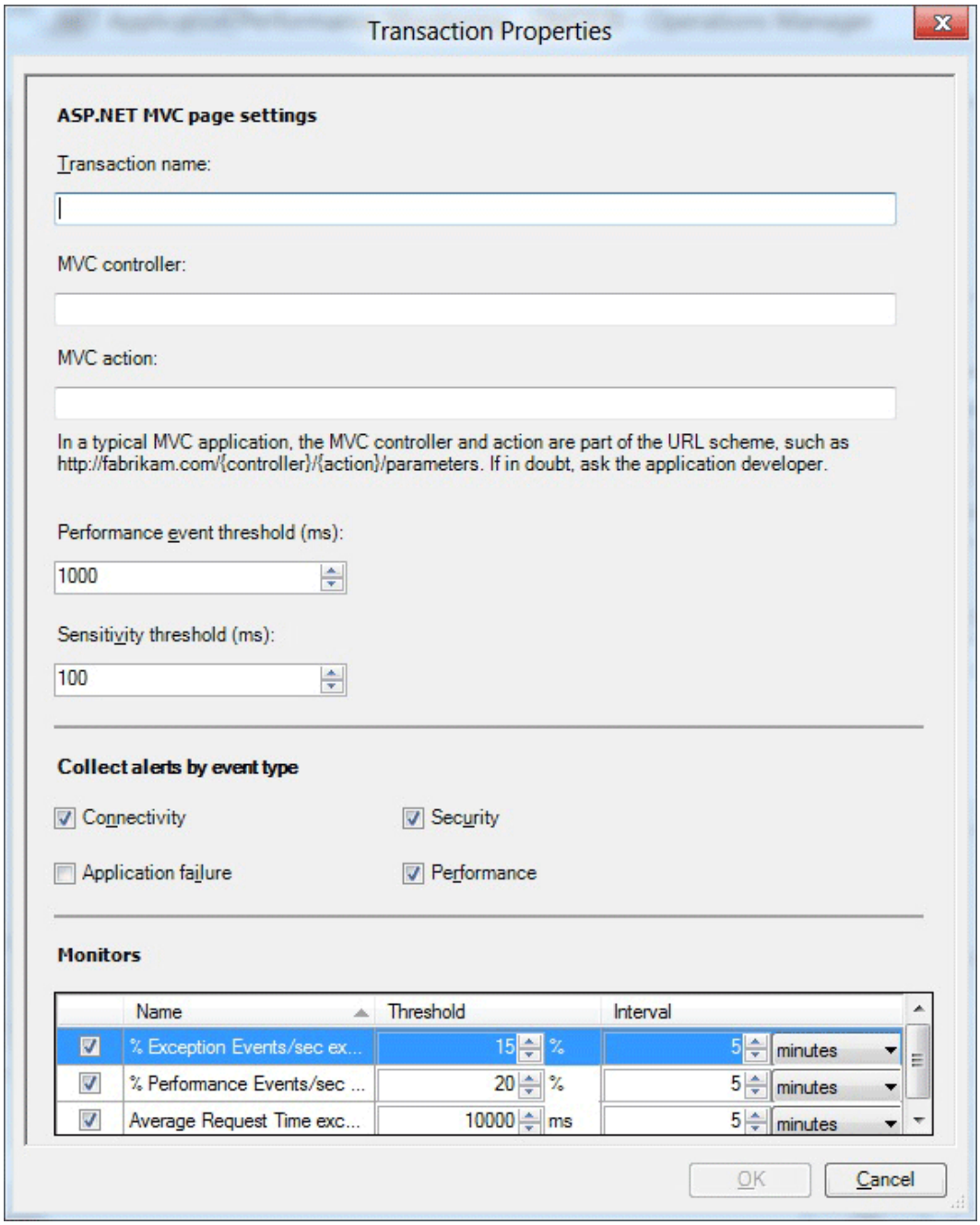
Option	Description
Transaction name	Enter the friendly name for the transaction as it

Option	Description
	will be displayed on the **Monitoring** tab, performance counters, and so on.
Web service file	Enter the path to the file for which you are configuring these monitoring settings.
Method name	Enter the URI of the web method that you want to monitor.
Performance event threshold (ms)	Set the threshold in milliseconds (ms) that a user transaction must exceed before it raises a performance event. **Note** The application component continues to monitor the page specified in the transaction by using the performance threshold that is set for the application component. This threshold is used as a second measure on the same page in the application component. If you set this threshold higher than the application component threshold, you get a single event, but you might get two performance alerts for the transaction when the threshold is breached—one from the application component and one from the transaction, depending on your alerting settings. Transactions are typically used to monitor the individual page more aggressively than the parent application, at a lower threshold, or to monitor a page where alerting has been disabled on the parent.
Sensitivity threshold (ms)	Specify to filter out fast-running methods to reduce overall “noise” by reducing the size of the call stack by gathering less data for each event. For more information, see Authoring Strategies for .NET Application Monitoring
Collect alerts by event type: Connectivity	Turn on or off alerting of events classified as connectivity alerts, with errors, such as

Option	Description
	“Connection Timed Out”. Connectivity events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Collect alerts by event type: Application failure	Turn on or off alerting of events classified as application, or code, failures. Turning this option off reduces the “noise” of many alerts raised due to code failures. Because these alerts are raised from code failures, developers usually resolve these issues. For more information, see Authoring Strategies for .NET Application Monitoring Exception events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Collect alerts by event type: Security	Turn on or off alerting of events classified as security alerts, with errors such as “Access Denied” or “Login Failed”. Security events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Collect alerts by event type: Performance	Turn on or off alerting of events classified as performance alerts. Performance events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Monitors: % Exception Events/sec	Monitor that watches the .NET App/% Exception Events/sec performance counter.
Monitors: % Performance Events/sec	Monitor that watches the .NET Apps/% Performance Events/sec performance counter.

Option	Description
Monitors: Average Request Time	Monitor that watches the .NET Apps/Average Request Time performance counter.

Transaction Properties: Add ASP.NET MVC Page



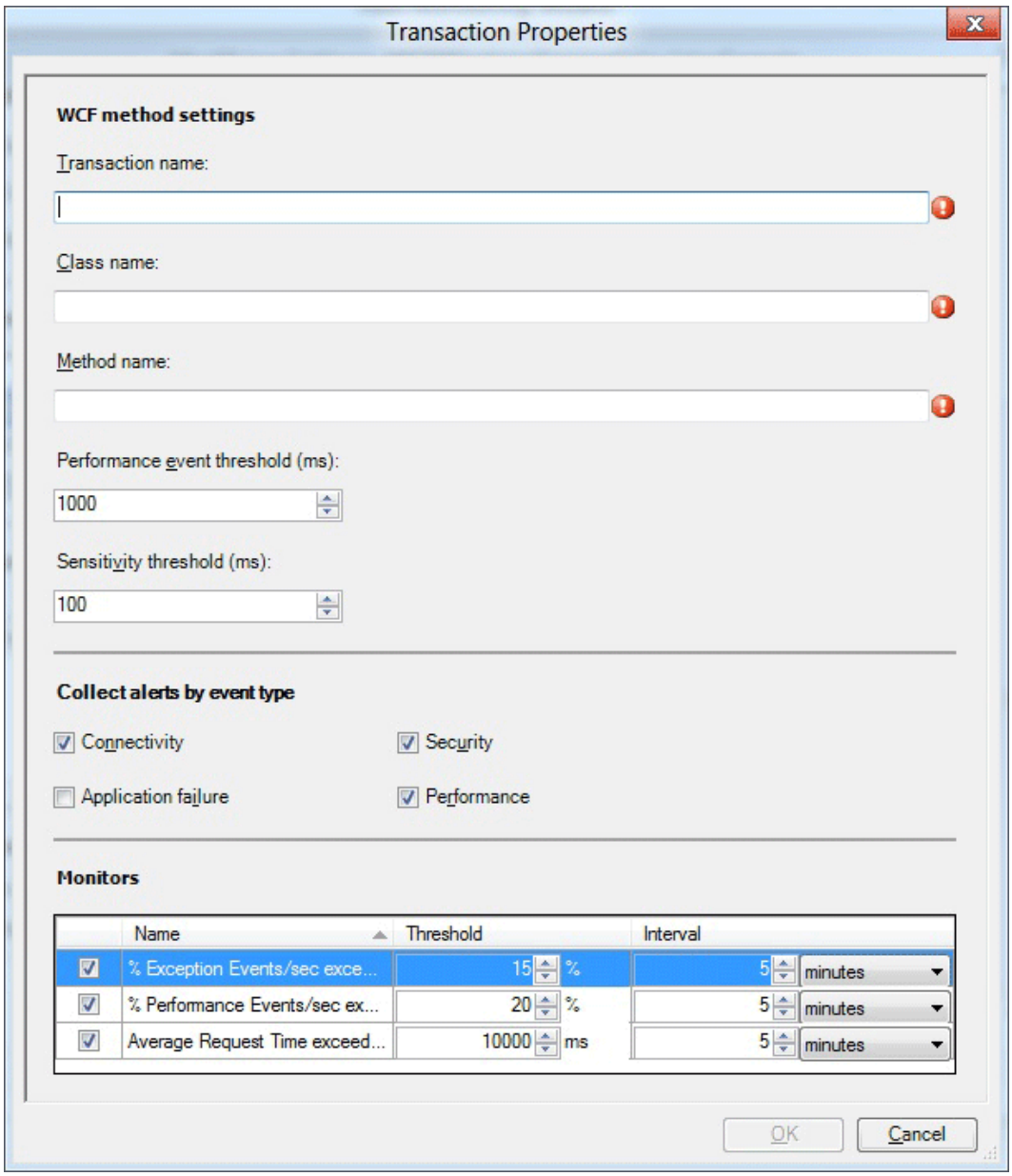
For System Center 2012 SP1 the following options are available on the **Transaction Properties** for the **ASP.MVC** page of the wizard.

Option	Description
Transaction name	Enter the friendly name for the transaction as it will be displayed on the Monitoring tab, performance counters, and so on.
MVC controller	Enter the name of the MVC controller for which you are configuring these monitoring settings.
MVC action	Specify the name of the MVC action for which you are configuring these monitoring settings.
Performance event threshold (ms)	Set the threshold in milliseconds (ms) that a user transaction must exceed before it raises a performance event. **Note** The application component continues to monitor the page specified in the transaction by using the performance threshold that is set for the application component. This threshold is used as a second measure on the same page in the application component. If you set this threshold higher than the application component threshold, you get a single event, but you might get two performance alerts for the transaction when the threshold is breached—one from the application component and one from the transaction, depending on your alerting settings. Transactions are typically used to monitor the individual page more aggressively than the parent application, at a lower threshold or to monitor a page where monitoring has been disabled on the parent.
Sensitivity threshold (ms)	Specify to filter out fast-running methods to reduce overall “noise” by reducing the size of the call stack by gathering less data for each event. For more information, see Authoring

Option	Description
	Strategies for .NET Application Monitoring
Collect alerts by event type: Connectivity	Turn on or off alerting of events classified as connectivity alerts, with errors such as “Connection Timed Out”. Connectivity events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Collect alerts by event type: Application failure	Turn on or off alerting of events classified as application, or code, failures. Turning this option off reduces the “noise” of many alerts raised due to code failures. Because these alerts are raised from code failures, developers usually resolve these issues. For more information, see Authoring Strategies for .NET Application Monitoring Exception events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Collect alerts by event type: Security	Turn on or off alerting of events classified as security alerts with errors such as “Access Denied” or “Login Failed”. Security events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Collect alerts by event type: Performance	Turn on or off alerting of events classified as performance alerts. Performance events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Monitors: % Exception Events/sec	Monitor that watches the .NET App/%

Option	Description
	Exception Events/sec performance counter.
Monitors: % Performance Events/sec	Monitor that watches the .NET Apps/% Performance Events/sec performance counter.
Monitors: Average Request Time	Monitor that watches the .NET Apps/Average Request Time performance counter.

Transaction Properties: Add WCF Method



The following options are available on the **Transaction Properties** for the **Add WCF method settings** page of the wizard.

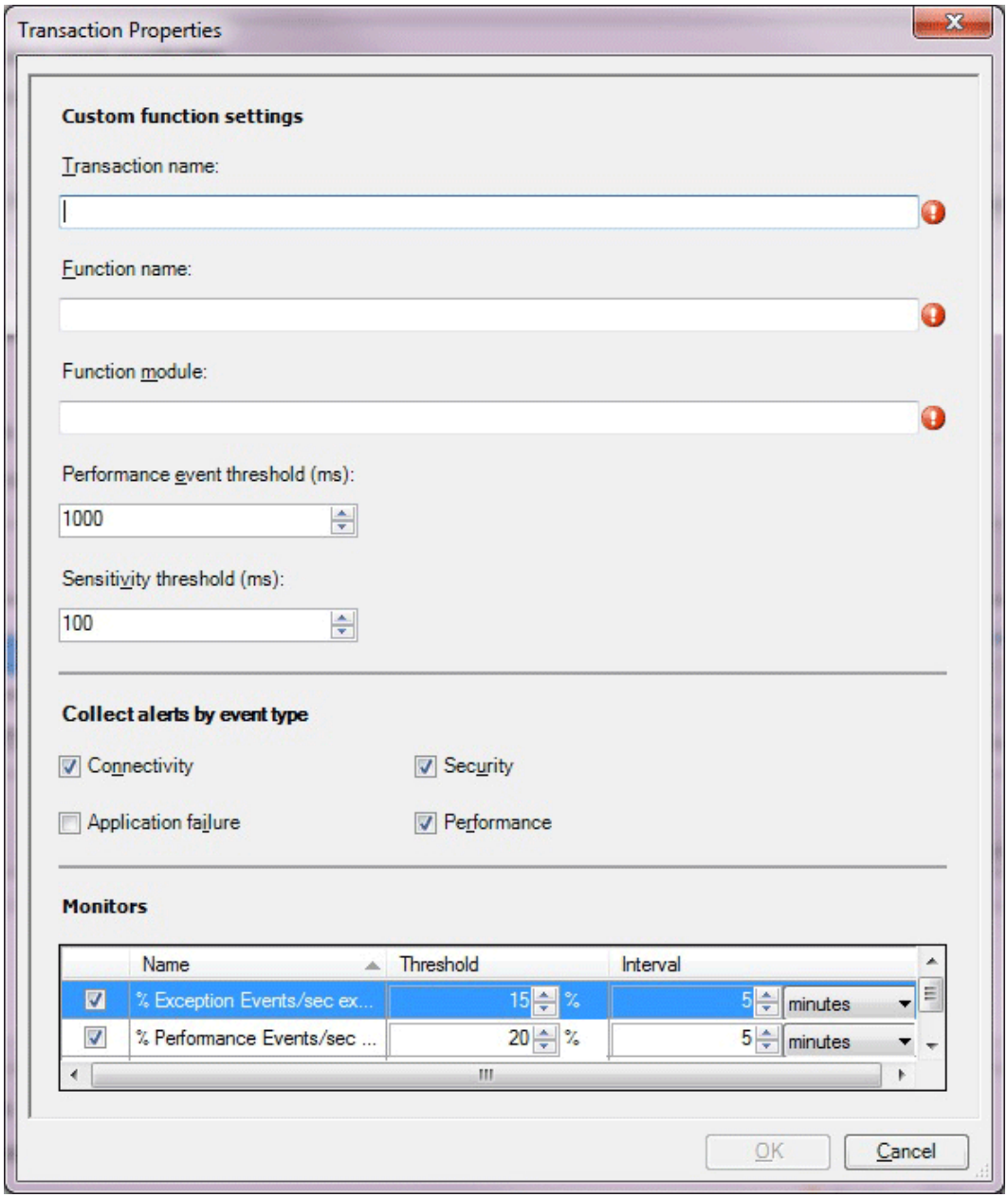
Option	Description
Transaction name	Enter the friendly name for the transaction as it will be displayed on the Monitoring tab, performance counters, and so on.

Option	Description
Class name	Enter the name of the class for which you are configuring these monitoring settings. The class name is in the format: Namespace.Class. For example: wcfservice.myclass.
Method name	Specify the name of the method that is expected to be in the class for which you are configuring these monitoring settings.
Performance event threshold (ms)	Set the threshold in milliseconds (ms) that a user transaction must exceed before it raises a performance event. **Note** The application component continues to monitor the page specified in the transaction by using the performance threshold that is set for the application component. This threshold is used as a second measure on the same page in the application component. If you set this threshold higher than the application component threshold, you get a single event, but you might get two performance alerts for the transaction when the threshold is breached—one from the application component and one from the transaction, depending on your alerting settings. Transactions are typically used to monitor the individual page more aggressively than the parent application, at a lower threshold or to monitor a page where alerting has been disabled on the parent.
Sensitivity threshold (ms)	Specify to filter out fast-running methods to reduce overall “noise” by reducing the size of the call stack by gathering less data for each event. For more information, see Authoring Strategies for .NET Application Monitoring
Collect alerts by event type: Connectivity	Turn on or off alerting of events classified as connectivity alerts, with errors such as

Option	Description
	“Connection Timed Out”. Connectivity events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Collect alerts by event type: Application failure	Turn on or off alerting of events classified as application, or code, failures. Turning this option off reduces the “noise” of many alerts raised due to code failures. Because these alerts are raised from code failures, developers usually resolve these issues. For more information, see Authoring Strategies for .NET Application Monitoring Exception events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Collect alerts by event type: Security	Turn on or off alerting of events classified as security alerts with errors such as “Access Denied” or “Login Failed”. Security events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Collect alerts by event type: Performance	Turn on or off alerting of events classified as performance alerts. Performance events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Monitors: % Exception Events/sec	Monitor that watches the .NET App/% Exception Events/sec performance counter.
Monitors: % Performance Events/sec	Monitor that watches the .NET Apps/% Performance Events/sec performance counter.

Option	Description
Monitors: Average Request Time	Monitor that watches the .NET Apps/Average Request Time performance counter.

Transaction Properties: Add Function



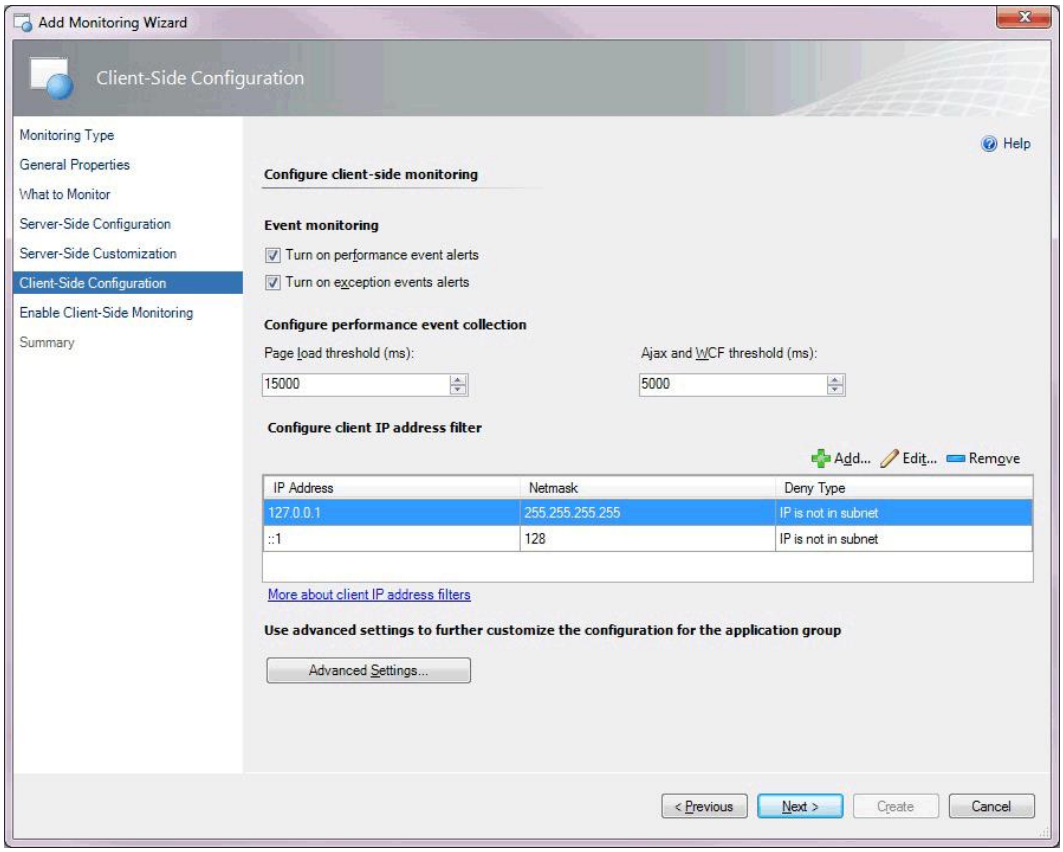
The following options are available on the **Transaction Properties** for the **Add Function** page of the wizard.

Option	Description
Transaction name	Enter the friendly name for the transaction as it will be displayed on the Monitoring tab, performance counters, and so on.
Function name	Enter the name of the function for which you are configuring these monitoring settings. The function name is in the format: **Namespace.Class.Method**. For example: **System.Web.UI.Page.ProcessRequest**.
Function module	Specify the name of the assembly, such as System.Web.dll, that defines the function for which you are configuring these monitoring settings.
Performance event threshold (ms)	Set the threshold in milliseconds (ms) that a user transaction must exceed before it raises a performance event. **Note** The application component continues to monitor the page specified in the transaction by using the performance threshold that is set for the application component. This threshold is used as a second measure on the same page in the application component. If you set this threshold higher than the application component threshold, you get a single event, but you might get two performance alerts for the transaction when the threshold is breached—one from the application component and one from the transaction, depending on your alerting settings. Transactions are typically used to monitor the individual page more aggressively than the parent application, at a lower threshold or to monitor a page where alerting has been

Option	Description
	disabled on the parent.
Sensitivity threshold (ms)	Specify to filter out fast-running methods to reduce overall “noise” by reducing the size of the call stack by gathering less data for each event. For more information, see Authoring Strategies for .NET Application Monitoring
Collect alerts by event type: Connectivity	Turn on or off alerting of events classified as connectivity alerts, with errors such as “Connection Timed Out”. Connectivity events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Collect alerts by event type: Application failure	Turn on or off alerting of events classified as application, or code, failures. Turning this option off reduces the “noise” of many alerts raised due to code failures. Because these alerts are raised from code failures, developers usually resolve these issues. For more information, see Authoring Strategies for .NET Application Monitoring Exception events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Collect alerts by event type: Security	Turn on or off alerting of events classified as security alerts with errors such as “Access Denied” or “Login Failed”. Security events are logged to the Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Collect alerts by event type: Performance	Turn on or off alerting of events classified as performance alerts. Performance events are logged to the

Option	Description
	Application Diagnostics console. You have the option to choose whether to raise alerts after an Application Performance Monitoring event is generated.
Monitors: % Exception Events/sec	Monitor that watches the .NET App/% Exception Events/sec performance counter.
Monitors: % Performance Events/sec	Monitor that watches the .NET Apps/% Performance Events/sec performance counter.
Monitors: Average Request Time	Monitor that watches the .NET Apps/Average Request Time performance counter.

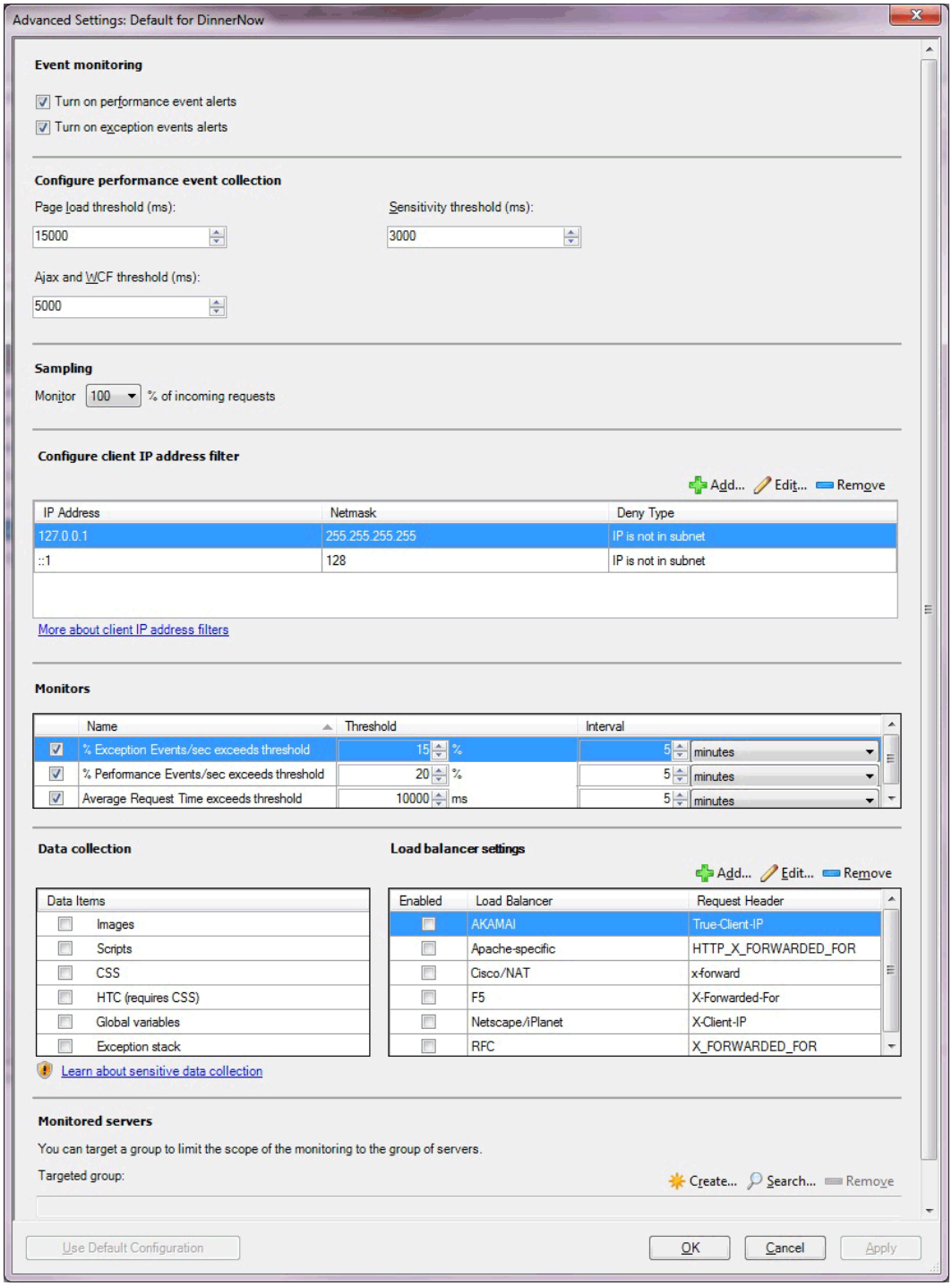
Client-Side Configuration



The following options are available on the **Client-Side Configuration** page of the wizard.

Option	Description
Turn on performance event alerts	Turn performance event alert reporting on or off within the Operations console for server-side monitoring. Performance events are still logged to the Application Diagnostics console. You have the option whether to raise alerts after an Application Performance Monitoring event is generated.
Turn on exception event alerts	Turn exception event alert reporting on or off within the Operations Manager console for server-side monitoring. Exception events are still logged to the Application Diagnostics console. You have the option whether to raise alerts after an Application Performance Monitoring event is generated.
Page load threshold (ms)	Set the threshold in milliseconds (ms) that a page load must exceed before it causes a performance event. You have the option whether to raise alerts after an Application Performance Monitoring event is generated. The event is only turned into an alert if you have selected **Turn on performance event alerts**.
IP address filter: IP Address	Specify the IP addresses that you want to exclude from monitoring. For more information, see How to Configure IP Address Exclusion Filters for Client-Side Monitoring
IP address filter: Netmask	The part of the filter IP address and user IP address that have to be compared for equality.
IP address filter: Comparison Type	Specify to exclude IP addresses that match the IP addresses in the subnet (**IP is in subnet**), or to exclude the user IP addresses that do not match the IP addresses in the subnet (**IP is not in subnet**).
IP address filter: Use IPv6	Add the IPv6 filter if the IPv6 protocol is enabled on the web server.
Advanced Settings	Specify settings, such as performance and event monitoring thresholds, exception event monitoring, Critical Exceptions, and monitors.

Advanced Settings for Client-Side Monitoring



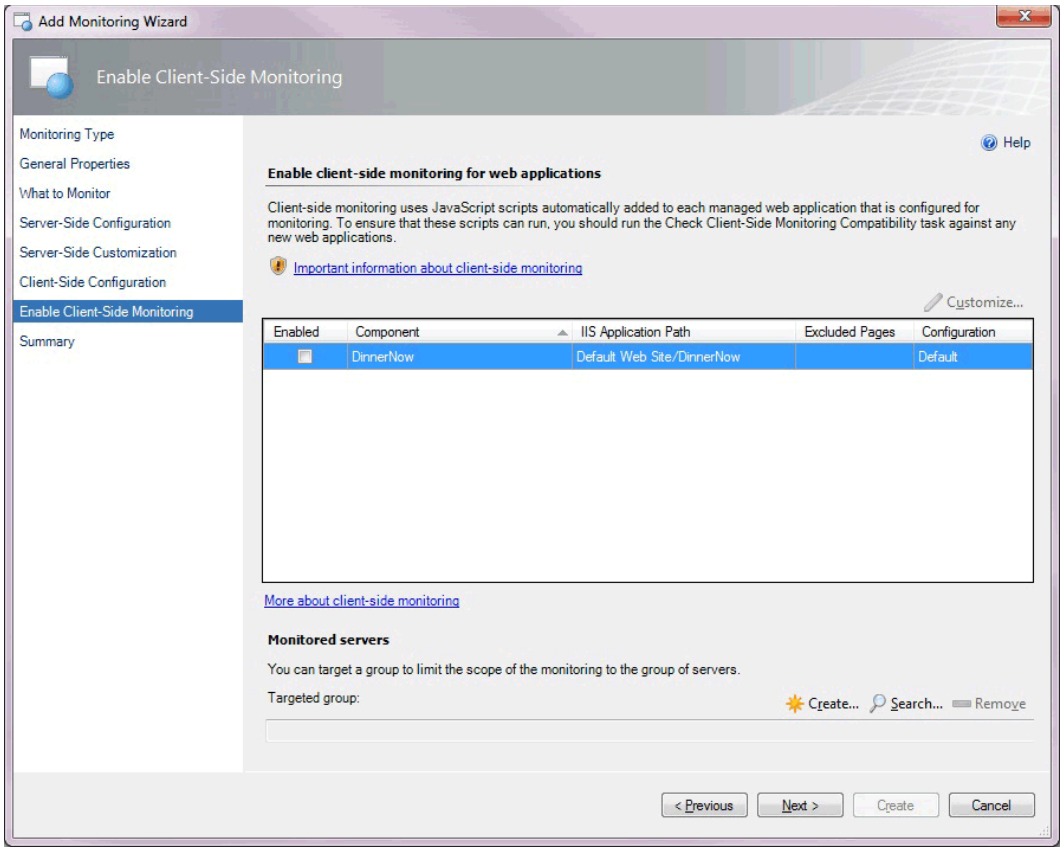
The following options are available on the **Advance Settings** for **Client-Side Monitoring** page of the wizard.

Option	Description
Turn on performance event alerts	Turn performance event alert reporting on or off within the Operations console for server-side monitoring. Performance events are still logged to the Application Diagnostics console. You have the option whether to raise alerts after an Application Performance Monitoring event is generated.
Turn on exception event alerts	Turn exception event alert notification on or off within the Operations console for server-side monitoring. Exception events are still logged to the Application Diagnostics console. You have the option whether to raise alerts after an Application Performance Monitoring event is generated.
Page load threshold (ms)	Set the threshold in milliseconds (ms) that a page load must exceed before it causes a performance event. You have the option whether to raise alerts after an Application Performance Monitoring event is generated. The event is only turned into an alert if you have selected **Turn on performance event alerts**.
Ajax and WCF threshold (ms)	Set the threshold in milliseconds (ms) that an Ajax or Windows Communications Foundation (WCF) call initiated from the page must exceed before it causes a performance event. The event is only turned to an alert if you have selected **Turn on performance event alerts**.
Monitor % of incoming requests.	Specify a sample size of incoming requests, defined as a percentage of the total number of incoming requests that you want to monitor. For more information, see Authoring Strategies for .NET Application Monitoring
IP address: IP Address	Specify the IP addresses that you want to exclude from monitoring. For more information, see How to Configure IP Address Exclusion

Option	Description
	Filters for Client-Side Monitoring
IP address: Netmask	Specify the part of the filter IP address and user IP address that have to be compared for equality.
IP address: Comparison Type	Specify to exclude IP addresses that match the IP addresses in the subnet (**IP is in subnet**), or to exclude the user IP addresses that do not match the IP addresses in the subnet (**IP is not in subnet**).
IP address: Use IPV6	Specify to add the IPv6 filter if the IPv6 protocol is enabled on the web server.
Monitors: Exception Events\sec exceeds	Monitor that watches the .NET CSM Apps/% Exceptions Events/sec performance counter.
Monitors: Performance Events\sec exceeds	Monitor that watches the .NET CSM Apps/% Performance Events/sec performance counter.
Monitors: Average Request Time exceeds	Monitor that watches the .NET CSM Apps/Average Page Load Response Time performance counter.
Data Items	Select the type of client-side data that you want to collect. For more information, see Working with Sensitive Data for .NET Applications
Load balancer settings	Select the type of load balancer that you are using with your application. You can also add your own load balancer, if it is not included in the list. For more information, see Client-Side Monitoring with Targeted Groups and Load Balancers
Targeted group	Select specific servers to limit monitoring to this specific set of servers. This is optional. Targeted group scoping only becomes necessary when you have the same application running in multiple environments, such as production and staging, and you intend to run the template multiple times, one for each environment. In this scenario, group which machines belong to production and which belong to the staging environment, and then

Option	Description
	use the targeted groups to restrict where the configuration is propagated. You can also use groups to apply configuration to a subset of your servers. Otherwise, it is not necessary to specify targeted group scoping if you just want to monitor all instances of a given application.

Enable Client-Side Monitoring

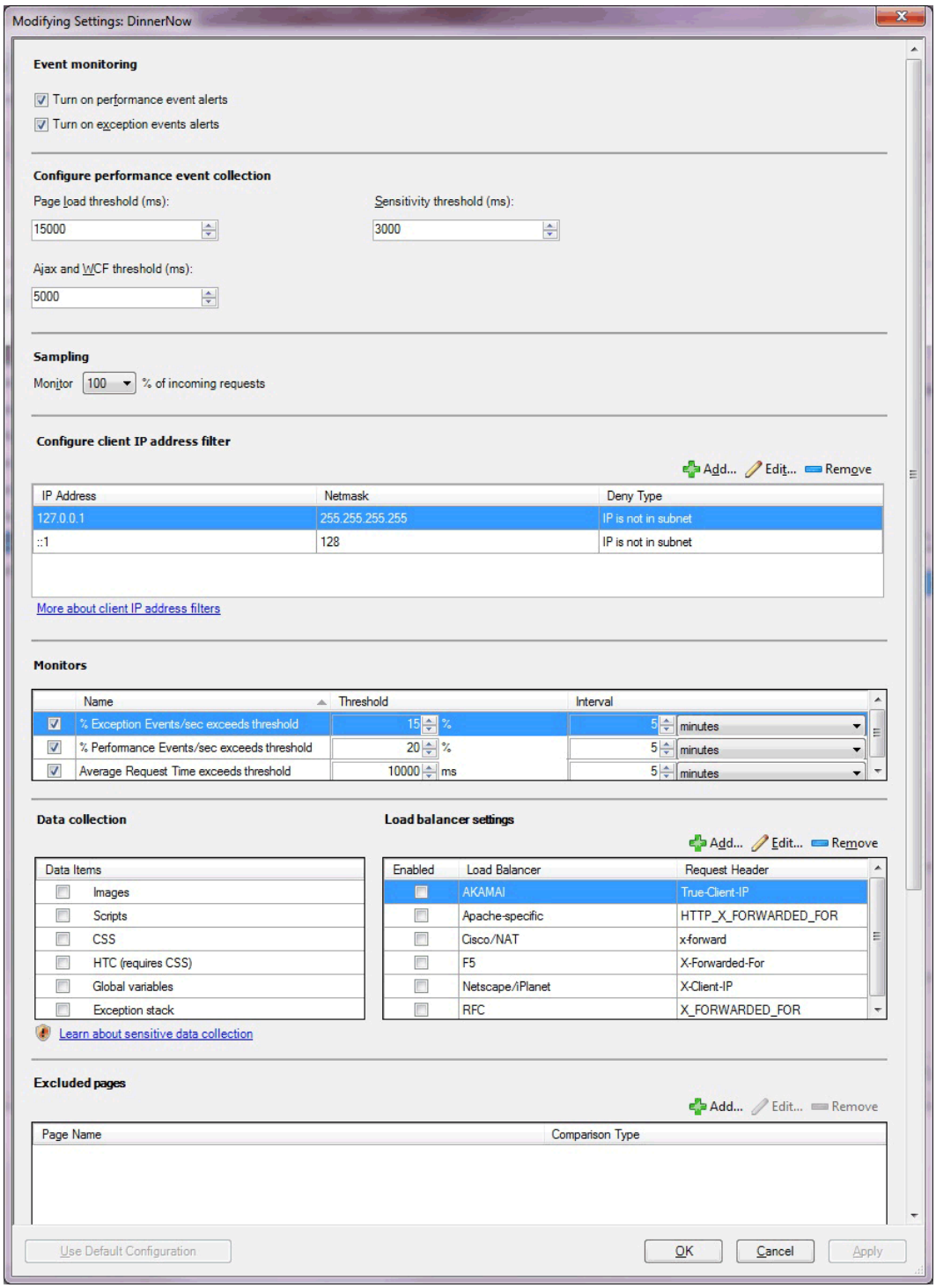


The following options are available on the **Enable Client-Side Monitoring** page of the wizard.

Option	Description
Component	Select the component you want to customize for monitoring individual application components. Only the components of the ASP.NET Web application type are displayed. Web Services and WCF Services do not serve

Option	Description
	HTML pages to browsers, so you cannot enable client-side monitoring for them. For System Center 2012 SP1 only: .NET applications hosted in Windows Services do not serve HTML pages to browsers, so you cannot enable client-side monitoring for them.
Customize	Modify the settings for the selected application component. This opens the **Modifying Settings** page. The settings on this page are similar to those on the **Advanced Settings for Client-Side Monitoring** page. On the **Modifying Settings** page, you can specify the pages to be excluded from monitoring.
Targeted group	Select specific servers to limit monitoring to this specific set of servers. This is optional. Targeted group scoping only becomes necessary when you have the same application running in multiple environments, such as production and staging, and you intend to run the template multiple times, one for each environment. In this scenario, group which machines belong to production and which belong to the staging environment, and then use the targeted groups to restrict where the configuration is propagated. You can also use groups to apply configuration to a subset of your servers. Otherwise, it is not necessary to specify targeted group scoping if you just want to monitor all instances of a given application.

Client-Side Modifying Settings



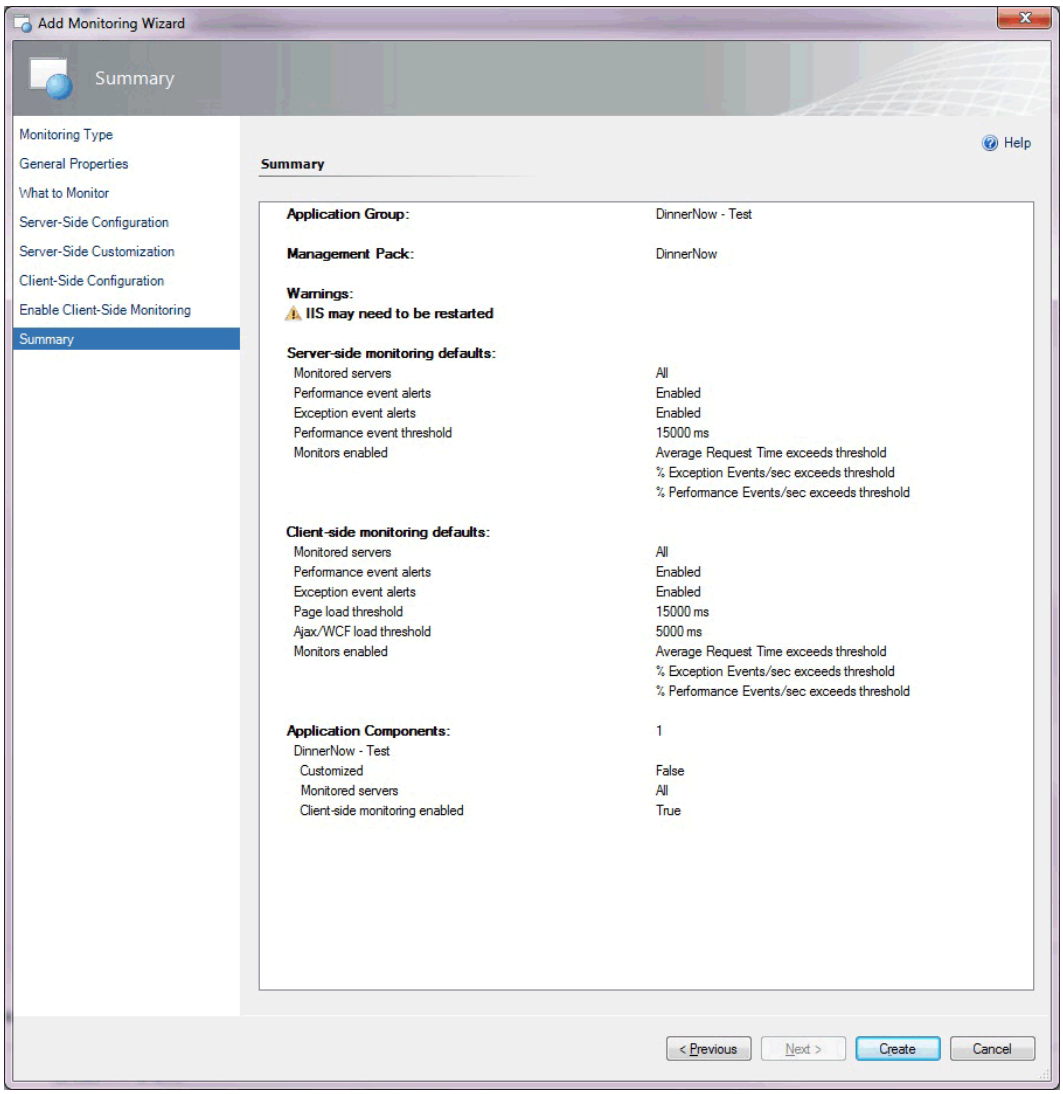
The following options are available on the **Client-Side Modifying Settings** page of the wizard.

Option	Description
Turn on performance event alerts	Turn performance event alert reporting on or off within the Operations console for server-side monitoring. Performance events are still logged to the Application Diagnostics console. You have the option whether to raise alerts after an Application Performance Monitoring event is generated.
Turn on exception event alerts	Turn exception event alert reporting on or off within the Operations console for server-side monitoring. Exception events are still logged to the Application Diagnostics console. You have the option whether to raise alerts after an Application Performance Monitoring event is generated.
Page load threshold (ms)	Set the threshold in milliseconds (ms) that a page load must exceed before it causes a performance event alert. You have the option whether to raise alerts after an Application Performance Monitoring event is generated. The event is only turned into an alert if you have selected **Turn on performance event alerts**.
Ajax and WCF threshold (ms)	Sets the threshold in milliseconds that an Ajax or Windows Communications Foundation (WCF) call initiated from the page must exceed before it causes a performance event. The event is only turned into an alert if you have selected **Turn on performance event alerts**.
Sensitivity threshold (ms)	Specify to filter out fast-running methods to reduce overall “noise” by reducing the size of the call stack by gathering less data for each event. For more information, see Authoring Strategies for .NET Application Monitoring
Monitor % of incoming requests.	Specify a sample size of incoming requests, defined as a percentage of the total number of incoming requests that you want to monitor. For more information, see Authoring Strategies for .NET Application Monitoring

Option	Description
IP address: IP Address	Enter the IP addresses that you want to exclude from monitoring. For more information, see How to Configure IP Address Exclusion Filters for Client-Side Monitoring
IP address: Netmask	Specify the part of the filter IP address and user IP address that have to be compared for equality.
IP address: Comparison Type	Specify to exclude IP addresses that match the IP addresses in the subnet (**IP is in subnet**), or to exclude the user IP addresses that do not match the IP addresses in the subnet **IP is not in subnet**).
IP address: Use IPV6	Specify to add the IPv6 filter if the IPv6 protocol is enabled on the web server.
Monitors: Exception Events\sec exceeds	Monitor that watches the .NET CSM Apps/% Exceptions Events/sec performance counter.
Monitors: Performance Events\sec exceeds	Monitor that watches the .NET CSM Apps/% Performance Events/sec performance counter.
Monitors: Average Request Time exceeds	Monitor that watches the .NET CSM Apps/Average Page Load Response Time performance counter.
Data collection	Select the type of client-side data you want to collect. For more information, see Working with Sensitive Data for .NET Applications
Load balancer settings	Select the type of load balancer that you are using with your application. You can also add your own load balancer, if it is not included in the list. For more information, see Client-Side Monitoring with Targeted Groups and Load Balancers.
Excluded pages: Add	Specify to add the pages to exclude from monitoring. You typically exclude pages that are considered unimportant for given metrics or that did not pass the compatibility check.
Transactions: Add	Specify transactions to add for ASP.NET web pages.

Option	Description
Targeted group	Select specific servers to limit monitoring to this specific set of servers. This is optional. Targeted group scoping only becomes necessary when you have the same application running in multiple environments, such as production and staging, and you intend to run the template multiple times, one for each environment. In this scenario, group which machines belong to production and which belong to the staging environment, and then use the targeted groups to restrict where the configuration is propagated. You can also use groups to apply configuration to a subset of your servers. Otherwise, it is not necessary to specify targeted group scoping if you just want to monitor all instances of a given application.

Summary



The **Summary** page of the wizard lists the settings you have configured for the **.NET Application Performance Monitoring** template. If you want to change any of these settings, click **Previous** or the template page until you reach the page with the settings that you want to change.

Creating and Modifying .NET Application Performance Monitoring Templates

For the procedure to run the .NET Application Performance Monitoring wizard, see How to Configure Monitoring for .NET Applications.

To modify an existing .NET Application Performance Monitoring template

1. Open the Operations console with a user account that has Author credentials in the

management group.

2. Click the **Authoring** workspace.
3. In the **Authoring** navigation pane, expand **Management Pack Templates**, and then select **.NET Application Performance Monitoring**.
4. In the **.NET Application Performance Monitoring** pane, locate the template to change.
5. Right-click the application group that you want to modify, and then select **Properties**.
6. Using the tabs to navigate the pages of settings, make the desired changes, such as adding customized monitoring for a specific application component or configuring and enabling client-side monitoring, and then click **OK**.

Viewing .NET Application Performance Monitoring Monitors and Collected Data

After you configure monitoring for an application, these three views will help you get started with the monitoring experience.

To view all .NET Application Performance Monitoring monitored applications

1. Open the Operations console.
2. Click the **Monitoring** workspace.
3. In the **Monitoring** navigation pane, expand **Application Monitoring**, expand **.NET Monitoring**, and then click **Monitored Applications**.

To view the state of each monitor

1. Open the Operations console.
2. Click the **Monitoring** workspace.
3. In the **Monitoring** navigation pane, expand **Application Monitoring**, expand **.NET Monitoring**, and then click **Monitored Applications**.
4. In the **Monitored Applications** view, right-click an object. Select **Open**, and then click **Health Explorer**.
5. Expand the **Availability** and **Performance** nodes to view the individual monitors.

To view the performance collected for an application component

1. Open the Operations console.
2. Click the **Monitoring** workspace.
3. In the **Monitoring** navigation pane, expand **Application Monitoring**, expand **.NET Monitoring**, and then click **Monitored Applications**.
4. In the **Monitored Applications** pane, right-click an object. Select **Open**, and then click **Performance View**.
5. In the **Legend** pane, select the counters that you want to view.
6. Use options in the **Actions** pane to modify the Performance view.

See Also

Before You Begin Monitoring .NET Applications

How to Configure Monitoring for .NET Applications

How to Start Monitoring a New Application

Authoring Strategies for .NET Application Monitoring

Before You Begin Monitoring .NET Applications

In System Center 2012 – Operations Manager, you can monitor web applications and web services from server- and client-side perspectives to get details about application availability and performance that can help you pinpoint problems. (For System Center 2012 SP1 only: You can also monitor Windows Services.) When you specify settings, the types of events to collect, the performance goals to measure, and which servers to monitor, Operations Manager .NET Application Monitoring provides insights into how web-based applications are running. You can see how frequently a problem is occurring, how a server was performing when a problem occurred, and the chain of events related to the slow request or a method that is unreliable. You have to have this information to partner with software developers and database administrators to help ensure that applications are available and perform at optimal levels.

Current AVIcode 5.7 customers: Operations Manager has .NET application monitoring capabilities that can replace AVIcode 5.7 for applications hosted in Internet Information Services (IIS) 7.0. (For System Center 2012 SP1 only: Also for applications hosted in Internet Information Services (IIS) 8.0.) If you are using AVIcode 5.7 to monitor applications and want to upgrade to Operations Manager, you must be running AVIcode 5.7 with System Center Operations Manager 2007 R2 with the latest cumulative updates. During the upgrade, the AVIcode 5.7 configuration is not converted to the .NET Application Performance Monitoring configuration, and the AVIcode agent is not replaced with the .NET Application Performance Monitoring agent. AVIcode agents continue to work as they did before the upgrade because the .NET Application Performance Monitoring configuration does not affect them. However, to continue to monitor applications by using AVIcode 5.7 after the upgrade, you must manually install these management packs: AVIcode.DotNet.SystemCenter.Enterprise.Monitoring.mpb and AVIcode.DotNet.SystemCenter.Client.Monitoring.mp. For more information, see Steps to import AVIcode 5.7 templates after upgrading and Notes for AVIcode 5.7 Customers

After the upgrade, we recommend that you configure all new application monitoring by using the .NET Application Performance Monitoring wizard and gradually replace the AVIcode 5.7 agents with the new .NET Application Performance Monitoring agents.

Before You Begin

To view Application Performance Monitoring event details, you must install the Operations Manager Web Console. For more information, see How to Install the Operations Manager Web Console

Import the IIS 7.0 management pack (Microsoft.Windows.InternetInformationServices.2008.mp) and the Operations Manager APM Web IIS 7 management pack (Microsoft.SystemCenter.Apm.Web.IIS7.mp). The Microsoft.SystemCenter.Apm.Web.IIS7.mp management pack is included in the download package in the Management Packs folder—it is not available on the management pack catalog.

For System Center 2012 SP1, to monitor Windows Server 2012, you also need to import the Microsoft.InternetInformationServices.2012.mp management pack (in the management pack catalog) and the Microsoft.SystemCenter.Apm.Web.IIS8.mp management pack. The Microsoft.SystemCenter.Apm.Web.IIS8 mp management pack is included in the download package in the Management Packs folder—it is not available on the management pack catalog.

For information about importing management packs, see How to Import an Operations Manager Management Pack. Additionally, ensure that websites, applications, and services have been discovered.

Important

When you try to import the .NET Monitoring management pack (Microsoft.SystemCenter.Apm.Web.IIS7.mp) from disc and resolve the references it has to Microsoft.Windows.InternetInformationServices.2008.mp, this IIS management pack in turn references the Windows Server 2008 Operating System (Discovery) management pack. If any of these management packs fail to import manually, update Microsoft.Windows.Server.Library.mp and import Microsoft.SystemCenter.Apm.Web.IIS7.mp again.

If you are running Windows Server 2008 R2, import the IIS 7.0 management packs.

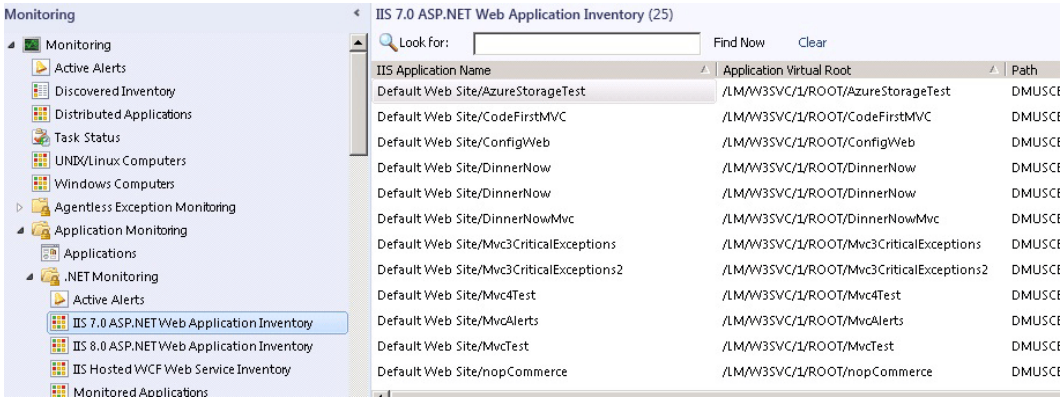
For System Center 2012 SP1 only: If you are running Windows Server 2012, import the IIS 8.0 management pack. If you are running both Windows Server 2008 R2 and Windows Server 2012, import IIS 7.0 and IIS 8.0 management packs.

Note

After you import the management packs, wait until the IIS Application Pools have been discovered and ASP.NET Web Applications start to appear in the ASP.NET Web Application Inventory view before you begin monitoring. For more information, see Configuring the Management Pack for Operations Manager APM Web IIS 7

Before you begin monitoring Windows Services, you need to configure Windows Services using the Windows Service template. Once you do this, the.NET Application Performance Monitoring template can discover the Windows Services that are running. For more information, see Authoring the Windows Service Template

ASP.NET Web Application Inventory view



Here are some questions to answer before you begin:

- What are the names of the applications that you want to monitor?
- Which servers host the applications that you want to monitor?
- Do you want to monitor performance events?
- Do you want to monitor exception events?
- What threshold signifies a performance issue with a request?
- Do you want to monitor both server and browser performance?

If you plan to monitor browser performance, check application compatibility before you begin to configure client-side monitoring of the ASP.NET application. To check compatibility, use the Check Client-Side Compatibility task. The information collected by this task tells you what pages should be excluded from monitoring. The list of excluded pages is entered during the configuration of client-side application monitoring in the wizard.

To check applications for compatibility with client-side monitoring

1. To see a view of all the ASP.NET web applications that Operations Manager finds, in the Operations console, in the navigation pane, click the **Monitoring** button, expand **Application Monitoring**, expand **.NET Monitoring**, and then click **ASP.NET Web Application Inventory**.
2. To check applications for compatibility with client-side monitoring, click an application name, and in the tasks pane, in the **IIS 7 ASP.NET Application Endpoint Tasks** section, click **Check Client Side Monitoring Compatibility**, and then click **Run**. This task does an analysis and lets you know if the application has compatibility issues with client-side monitoring.
3. The results page displays whether incompatibilities are found. If an application has incompatibilities, you should exclude the incompatible pages from client-side monitoring later when you are configuring client-side monitoring.

   You can change an application so that it becomes compatible with client-side monitoring by following the instructions in the output of the compatibility tool.

Note

For System Center 2012 SP1, you can only check applications for compatibility with client-side monitoring in the IIS 7.0 ASP.NET Web Applications and IIS 8.0 ASP.NET Web Applications views. You cannot check applications for compatibility with client-side monitoring in the IIS Hosted WCF Web Services view because client-side monitoring does not apply to this type of endpoint.

See Also

[How to Configure Monitoring for .NET Applications]

[How to Start Monitoring a New Application]

How to Configure Monitoring for .NET Applications

Configure .NET Application Performance Monitoring

The **.NET Application Performance Monitoring** template in System Center 2012 – Operations Manager lets you monitor .NET and WCF applications hosted in Internet Information Services (IIS) 7.0. For System Center 2012 SP1 only: You monitor applications hosted in IIS 8.0 and Windows Services. You can select one or more applications or services and configure monitoring of performance and exception events. Server-side monitoring lets you measure details about the performance and reliability of applications that are running in your datacenter. By monitoring client-side applications, you can measure details of the customer experience, such as how long it takes for a page to load. It is another way to monitor how your applications are working from the perspective of your customer. Client-side application monitoring helps you determine whether your users are experiencing problems. With both client-side and server-side monitoring in use, you can determine if a problem exists on your server, in the application, or is being caused by external factors, such as high network latency.

Tip

Client-side monitoring can be set up at the same time as server-side monitoring when you run the .NET Application Performance Monitoring wizard or by editing an existing instance of a template.

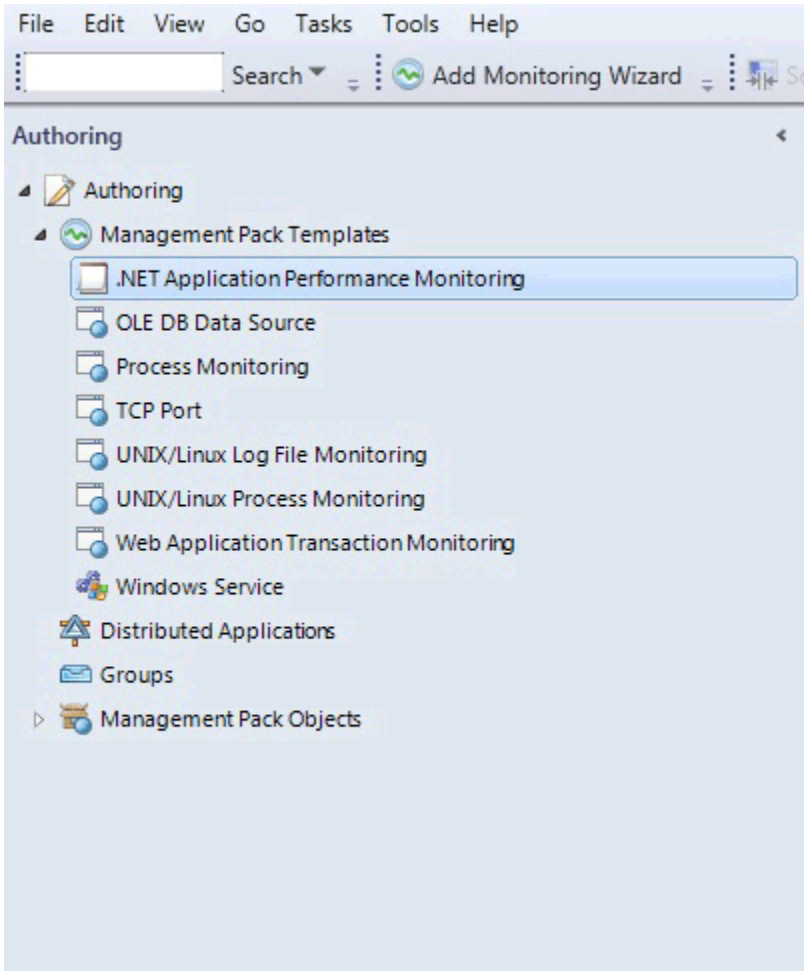
Important

You can only configure client-side monitoring for applications that have been configured for server-side monitoring.

To configure .NET Application Performance Monitoring (server-side perspective)

1. To open the **.NET Application Performance Monitoring** template, in the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Templates**, click **.NET Application Performance Monitoring**, and then, in the tasks pane, click the **Add Monitoring Wizard** where you name and configure the application group that you want to monitor.

   Location of .NET Application Performance Monitoring



2. In the **Add Monitoring Wizard** on the **Monitoring Type** page, select **.NET Application Performance Monitoring**, and then click **Next**. This template lets you monitor web applications and services hosted in IIS 7.0. (For System Center 2012 SP1 only: You can monitor applications hosted in IIS 8.0 and Windows Services.) You can select one or more applications or services discovered by the IIS 7.0 management pack and configure monitoring of performance and exception events. For System Center 2012 SP1 only: You can select one or more applications or services discovered by the IIS 8.0 management pack or Windows Services previously configured with the Windows Service Template.
3. On the **General Properties** page, enter a friendly name and description for the application group that you are creating.

   In the **Select destination management pack** menu, select the management pack to

store the settings that are specific to this instance of the template. To create a new management pack, click **New**. In the **Create a Management Pack** wizard, name your new management pack the same as the application group so you can easily pair the two, which is helpful later in the monitoring experience. Click **Next**. For more information, see Selecting a Management Pack File.

4. On the **What to Monitor** page, in the **Application components** section, click **Add**. On the **Object Search** page, on the **Search for** menu, use the **Filter by part of the name (optional)** box to narrow your search, and then click **Search** to view a list of the application components you can monitor. (For System Center 2012 SP1 only: You can monitor Windows Services.) From the search results, select the application components that you want to monitor, click **Add**, and then click **OK**. The application components you selected are now displayed as members of the application group that you are going to monitor. Click **Next**.

   On the **What to Monitor** page, on the **Environment** menu, select the environment you want to monitor your application in: **None**, **Production**, **Staging**, **Test**, **Development**, or **New**. Typically, you want to pair the environment tag with the server group you are monitoring.

   Tip
   If you do not have to monitor multiple versions of the same applications, such as production instances and staging instances, you can leave the environment tag set to **None**.

5. To limit the scope of monitoring to a group of servers, on the **What to Monitor** page, in the **Monitored Servers** section, click **Search**. On the **Group Search** page that opens, select the **Filter by** box and **Management pack** menu to find the server group that you want to use, and then click **Search**. Select the server group to which you want to limit monitoring in the **Available Groups** search results list, and click **OK** to add it to your targeted server group to monitor. Click **Next**.

   Tip
   The **Targeted servers** group lets you configure monitoring by using one set of thresholds for one set of application servers and a different set of thresholds for another set of application servers. To configure monitoring for the second set of application servers, run the template again, and use the alternate **Targeted servers** group and use a different environment tag for each template instance.

6. On the **Server-Side Configuration** page, decide how you want to configure your monitoring. You have options to:
   - Turn on or off performance event monitoring
   - Turn on or off exception event monitoring
   - Change the Performance Event Threshold
   - Configure Advanced Settings
   - Enable additional configuration options for server-side and client-side monitoring.
7. To further configure exception and performance event monitoring for the application

group, including settings for **Namespaces**, **Methods**, **Exception Tracking**, and **Critical Exception Handlers**, click **Advanced Settings**. Also on the **Advanced Settings** for **Server-Side Monitoring** page, you can reset monitor thresholds from the defaults and scope monitoring to a targeted group. If you want to use or return to the default **Advanced Settings**, click **Use Default Configuration**. When you are finished, click **OK**. For more information, see How to Start Monitoring a New Application and Application Monitoring Using the Default Settings

Warning

Gathering detailed performance and exception events can lead to collecting sensitive information that should not be passed on to the development team. For example, if you capture an exception from your billing system, you might also capture user names and other tokens that can be used to identify the person who is having problems making purchases and what they were trying to purchase. Before enabling the collection of parameters and local variables for performance and exception events, we recommend that you review your policies. For more information, see Working with Sensitive Data for .NET Applications

8. If you only want to configure server-side monitoring and do not want to customize additional server-side monitoring options or configure and enable client-side monitoring, click **Next**, and on the **Summary** page, review your monitoring configuration for your application group. To create the monitoring template, click **Create**.
9. You might have to restart IIS or recycle the application pools to finalize the configuration of the applications for monitoring. If a restart or recycle is required, you receive an alert and can use the task link in the knowledge base to perform the necessary action.

Note

After you restart the application it does not begin collecting information accessed by users.

10. If you do want to customize server-side monitoring settings further and to configure and enable client-side monitoring, select the **Enable additional configuration options for server-side and client-side monitoring** check box, and then click **Next**. This command adds pages to the wizard as described below.

Additional Customization for .NET Application Performance Monitoring (Server-Side Perspective)

Using the **Modifying Settings** page, you can customize server-side monitoring settings for specific application components.

To customize .NET Application Performance Monitoring for a specific application component (server-side perspective)

1. If you want to customize server-side monitoring settings further and to configure and enable client-side monitoring, on the **Server-Side Configuration** page, select the **Enable additional configuration options for server-side and client-side monitoring**

check box, and then click **Next**. This command adds pages to the wizard.

Warning
If you do not want to change settings of an application component monitor, click **Next**, and continue with **Client-Side Configuration**.

2. To select the specific application component for which you want to customize monitoring, on the **Server-Side Customization** page, click **Customize**. The **Modifying Settings** page lets you customize and specialize monitoring for the specific application component and create transactions for individual webpages, web methods, or functions within the application component. When you are finished, click **OK**, and then click **Next**. If you do not want to configure and enable client-side monitoring, click **Next** on the **Client-Side Configuration** page, and then click **Next** on the **Enable Client-Side Monitoring** page.
3. On the **Summary** page, review your monitoring configuration for your application group. To create the monitoring template, click **Create**.
4. You might have to restart IIS or recycle the application pools to finalize the configuration of the applications for monitoring. (For System Center 2012 SP1 only: You might have to restart the Windows Service.) If a restart or recycle is required, you receive an alert and can use the task link in the knowledge base to perform the necessary action.

Note
After you restart the application it does not begin to collect information until it is accessed by users.

Enable and Configure .NET Application Performance Monitoring (Client-Side Perspective)

Client-side application monitoring lets you measure details of the customer experience, such as how long it takes for a page to load. It is another way to monitor how your applications are working from the perspective of your customer. Client-side application monitoring helps you determine whether a problem exists on your server, in the application, or elsewhere.

Important
You can only configure client-side monitoring for applications that have been configured for server-side monitoring.

Important
When working with web applications configured using IIS Shared Configuration, the Operations Manager “Privileged Monitoring Account” Runas Profile associated with the Windows agents hosting the application must have read and write permissions on the shared directory that hosts the web application files to create the Client-Side Monitoring Collector web application, as well as local administrative privileges on each server in the farm to access the IIS metabase for discovery.

Tip

Client-side monitoring can be set up at the same time as server-side monitoring when you run the .NET Application Performance Monitoring wizard or through editing an existing instance of a template as described below.

To enable and configure .NET Application Performance Monitoring (client-side perspective)

1. You can either enable client-side monitoring as part of the .NET Application Performance Monitoring Wizard when you configure monitoring for server-side monitoring, or you can revise an existing template to include client-side monitoring. This procedure describes how to enable client-side monitoring while authoring the template.

   To enable client-side monitoring, on the **Server-Side Configuration** page, select the **Enable additional configuration options for server-side and client-side monitoring** check box and continue with the wizard.

   To revise the template to add client-side monitoring, see To add client-side monitoring to an existing .NET Application Performance Monitoring template
2. On the **Client-Side Configuration** page, you can select to turn on performance and exception event alerts, set page load thresholds and the Ajax and WCF threshold for the application group you are going to monitor. What you enter in the **Configure client IP address filter** section determines the client requests that are monitored. You can use client IP filters to select the networks that you want to exclude from monitoring. By applying filters, administrators can limit the scope of the monitored computers. By default, the filter is set to localhost, so only connections from browsers started on the local server are instrumented for monitoring. If the IP filter list is empty, all IP addresses are monitored. Any IP addresses that fit the filter definitions are excluded from client-side monitoring. For more information and filtering examples, see How to Configure IP Address Exclusion Filters for Client-Side Monitoring.
3. To configure more settings for this application group, click **Advanced Settings**. Here, in addition to settings on the previous page, you can set the sensitivity threshold, that lets you filter out fast-running methods, which reduces overall “noise”, making it easier for you to determine where the problem is and reduces network bandwidth usage. You can also choose to sample only a percentage of the incoming requests. Choosing to monitor only some of the incoming requests can help reduce the load on your monitoring server. Additionally, you can configure these settings:
   - In the **Monitors** section, you can change the default thresholds and intervals for the monitors.
   - In the **Data collection** section, you can select the type of data you want to collect.

     Warning
     Enabling the **Exception Stack** and **Global Variables** data collection sends application data to the monitored server. We recommend that you do not enable the data collection from **Exception Stack** and **Global Variables** unless the application is configured to use an HTTPS protocol.
   - **Load balancer settings** let you select the type of load balancers that you are using with your application. You can also add your own load balancer, if it is not included in

the list. For more information about load balancers, see Client-Side Monitoring with Targeted Groups and Load Balancers

- In the **Monitored Servers** section, you can target a group to limit the scope of the monitoring to a group of servers. To select a targeted group, click **Search** and use the **Group Search** page to search for the group by name and management pack, and then add them to the selected objects list. The targeted group you select consists of only the servers hosting the web application that set the application pages to return browser-side events. This group lets you limit client-side monitoring independent of server-side monitoring.

Tip

Only applications hosted on servers that are members of both the server-side and client-side targeted groups are monitored by client-side monitoring.

When you have made your changes, click **OK**, and then click **Next**.

4. To enable an application group for client-side monitoring, on the **Enable Client-Side Monitoring** page, select the application you want to enable for client-side monitoring. To customize settings for a selected application component, click **Customize**.
5. On the **Modifying Settings** page, you can configure the same settings for the application component that you did for the entire application group with the addition of **Excluded pages** and **Transactions**. In the **Excluded Pages** section, click **Add** to add the pages that you want to exclude from client-side monitoring. The pages you add to this list are the pages that the Check Client Side Monitoring Compatibility task found incompatible when you ran the task before configuring your application for monitoring. In the **Transactions** section, click **Add** to add transactions for ASP.NET webpages.
6. To review all of your monitoring configurations—both server-side configurations and client-side configurations—click the **Summary** tab. After you have reviewed the configuration, click **OK**.

Tip

If you want to change any configurations, while you are on this page is a good time to do so. For example, to review or change your server-side configuration, click the **Server-Side Configuration** page to see that configuration. To disable client-side monitoring, click the **Enable Client Side Monitoring** page, and clear the check box.

7. On the **Summary** page, review your monitoring configuration for your application group. To create the monitoring template, click **Create**.
8. After the client-side monitoring has been configured, you receive an alert to recycle IIS on the affected servers when the client-side monitoring settings have been applied to the server. You can use the link in the knowledge base article to recycle the IIS application pools on the server.

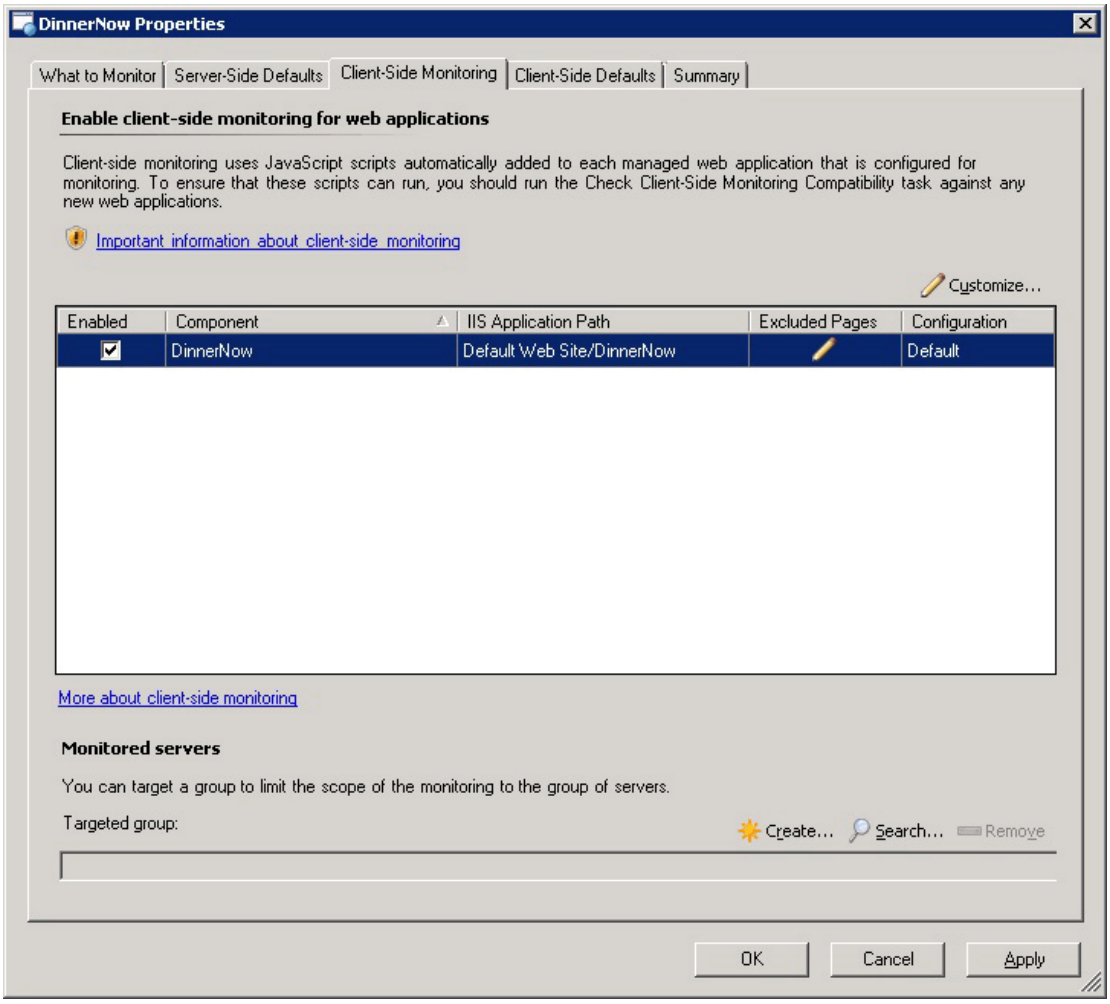
Note

After you restart IIS, an application does not begin to be monitored until it is used.

To add client-side monitoring to an existing .NET Application Performance Monitoring template

1. To enable client-side application monitoring to an existing **.NET Application Performance Monitoring** template, in the Operations Manager console, in the navigation pane, click the **Authoring** button, expand **Management Pack Templates**, click **.NET Application Performance Monitoring**, right-click the application group you configured for server-side monitoring, and then select **Properties**.
2. On the **Properties** page, click the **Enable Client Side Monitoring** tab, and select the **Enable** check box next to the application group.

   Enable client-side monitoring



3. The **Customize** option on this page opens the **Modifying Settings** page as described in the previous procedure.
4. To configure client-side default settings, click the **Client-Side Defaults** tab. These settings and those on the **Advanced Settings** page are described in the above

procedure.

Tip
Only applications hosted on servers that are members of both the server-side and client-side targeted groups are monitored by client-side monitoring.

5. To review all of your monitoring configurations—both server-side configurations and client-side configurations—click the **Summary** tab. After you have reviewed the configuration, click **OK**.
6. On the **Summary** page, review your monitoring configuration for your application group. To create the monitoring template, click **Create**.
7. After the client-side monitoring has been configured, you receive an alert to recycle IIS on the affected servers when the client-side monitoring settings have been applied to the server. You can use the link in the knowledge base article to recycle the IIS application pools on the server.

Note
After you restart IIS, an application does not begin to be monitored until it is used.

See Also

Before You Begin Monitoring .NET Applications

How to Start Monitoring a New Application

Authoring Strategies for .NET Application Monitoring

How to Add, Enable, and Disable Namespaces

Namespaces define where application performance monitoring should go to collect more detailed information, such as parameters and variables for functions in the specified namespaces or classes. They can be added to the default list and be treated as either entry points or as methods. The default monitoring list can be changed by adding, editing, or removing namespaces and classes.

Note
Many large .NET Framework namespaces (such as System.* and Microsoft.*) are disabled by default. To enable them, you need to explicitly add them to the namespaces list as enabled namespaces. Additionally, adding namespaces can affect performance and you should add them only after careful testing.

Note

For System Center 2012 SP1 only: **All namespaces** is present in the list and enabled for monitoring by default. However, **All namespaces**, does not include namespaces that have been explicitly disabled by the user or by the default configuration files.

If a namespace is generating too many events, collection for that namespace is turned off by the agent automatically to prevent overloading the agend and an event is written on the agent in the Operations Manager event log. However, everything else will continue to run as expected.

Add a Namespace

To add a namespace

1. To open the .NET Application Performance Monitoring template, in the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Templates**, and then click **.NET Application Performance Monitoring**.
2. Right-click the application group whose settings you want to modify, and then select **Properties**.
3. On the **Server-Side Defaults** tab, click **Advanced Settings**.
4. On the **Advanced settings** page, click **Set Namespaces** to open the **Namespace list** page. This is where you can add namespaces.
5. To add a namespace, on the **Namespace list** page, select **Namespace or class**, click **Add**, and then type the namespace you want to add.

   Note
   The namespace and class names are case-sensitive. The class name should be specified in the following format: Namespace.ClassName

   The **Enable monitoring** checkbox specifies whether or not you want to collect information from functions contained in the namespace or class. If you want to disable monitoring, perhaps because the functions in the namespace are called very frequently and could be creating performance overhead, clear the **Enable monitoring** checkbox, and the functions will not be monitored. If you want to make this namespace an entry point, select the **Enable as entrypoint** checkbox. Performance event timing begins when the monitor encounters a known entry point and completes when the processing of the entry point finishes. If that time exceeds the alerting threshold, then a performance event is reported. For most ASP.NET, ASP.NET MVC, and WCF applications and services, it is typically not necessary to mark specific namespaces or classes as entry points because the default configuration files already contain the entry points that are used by those technologies. Click **OK**.

   Warning
   Namespaces are set on the process level. If you enable a namespaces for an application that is running in the process and then disable it for a different application running in that process, there will be a namespace conflict and application monitoring will be disabled. To resolve this, you must make the

namespace handling the same for all applications in the same process.

Note
In contrast to namespaces, methods allow you to enable and disable data collection at the specific function level and let you monitor both time measurements as well as collecting deep information, such as variables and parameters used by the methods.

Edit a Namespace

To edit a namespace

1. To open the .NET Application Performance Monitoring template, in the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Templates**, and then click **.NET Application Performance Monitoring**.
2. Right click the application group whose settings you want to modify, and then select **Properties**.
3. On the **Server-Side Defaults** tab, click **Advanced Settings**.
4. On the **Advanced settings** page, click **Set Namespaces** to open the **Namespace list** page. This is where you can edit namespaces.
5. To edit a namespace, on the **Namespace list** page, click **Edit**, make your changes, and then click **OK**.

Note
The namespace and class names are case-sensitive. The class name should be specified in the following format: Namespace.ClassName

Remove a Namespace

To remove a namespace

1. To open the .NET Application Performance Monitoring template, in the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Templates**, and then click **.NET Application Performance Monitoring**.
2. Right click the application group whose settings you want to modify, and then select **Properties**.
3. On the **Server-Side Defaults** tab, click **Advanced Settings**.
4. On the **Advanced settings** page, click **Set Namespaces** to open the **Namespace list** page. This is where you can remove namespaces.
5. To remove a namespace, on the **Namespace list** page, select the namespace or class you want to remove, click **Remove**, and then click **OK**.

When to Enable or Disable Monitoring of All Namespaces and Classes

This setting is used to figure out what you do not know when you are troubleshooting. When you are working with an application, you might not know what you need to enable to get the data you want. This is when you should enable all namespaces. Monitoring all namespaces gives you a view into all the methods that make up the request and ensures that all paths through the application are measured. If, for instance, you only select specific namespaces that you know exist, you might not collect all the information you need to troubleshoot performance problems. You would miss collecting performance information from unlisted namespaces. In this case, the timing in the known functions would include the amount of time spent in the unlisted namespace, giving the false impression that the known functions are slow when they are not.

When to use: Use this when you are trying to troubleshoot a problem and need to isolate the slow function.

Strategy: Before setting specific namespaces, it is good to first set all namespaces to know what's being hit, and then reduce the number of namespaces to those that are relevant. This reduces amount of data collected and reduces impact on monitored application.

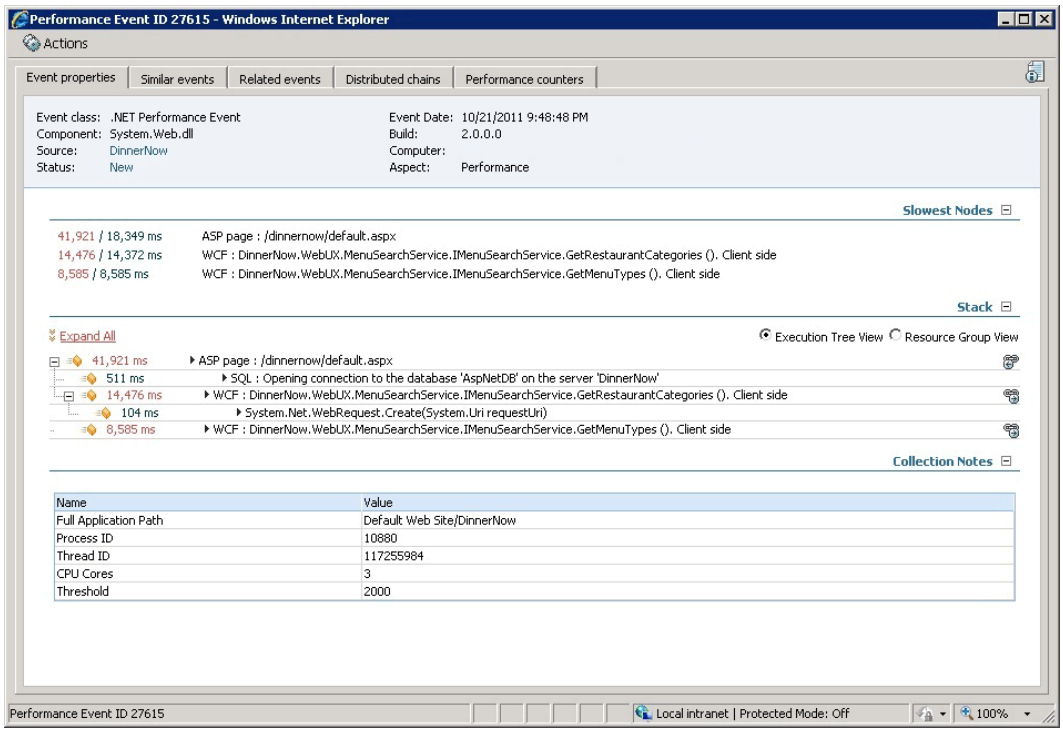
Tip

It is best to enable all namespaces in a test environment before implementing it in a production environment as there is a performance penalty to monitoring all namespaces. When a test environment is not available, begin by measuring a single server's baseline performance, and then enabling all namespaces on that single server. When you can determine that performance is not impacted, then roll out the setting to more servers.

For System Center 2012 SP1 only: **All namespaces** is in the list and enabled for monitoring by default. However, **All namespaces**, does not include namespaces that have been explicitly disabled.

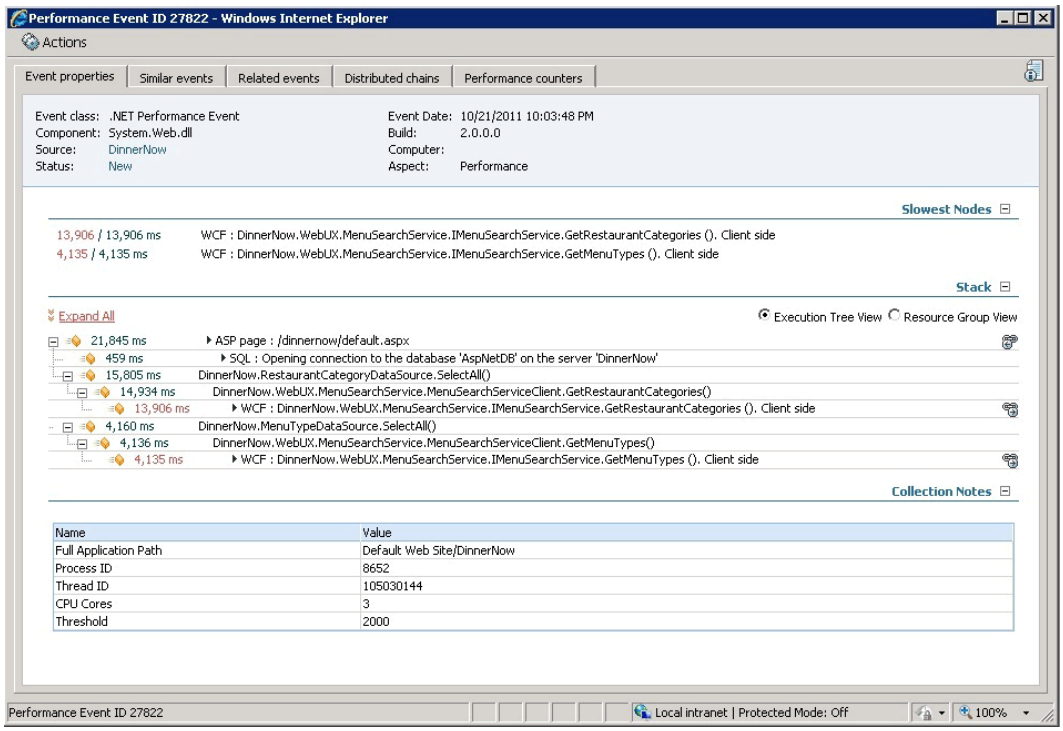
This example shows the difference in monitoring data when you change which namespaces are enabled.

Monitoring with no namespaces



Monitoring with no additional namespaces enabled, the execution tree shows that calls are going to WCF services, but has no details about the actual flow or where those calls are coming from. If a developer tries to investigate this issue and sees that the web service is called from multiple places, the information is incomplete and less useful in helping them find the true root cause.

Monitoring with specific namespaces



By adding the appropriate application specific namespaces, the execution tree shows more details about what is happening in the slow webpage.

To enable or disable monitoring of all namespaces and classes

1. To open the .NET Application Performance Monitoring template, in the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Templates**, and then click **.NET Application Performance Monitoring**.
2. Right click the application group whose settings you want to modify, and then select **Properties**.
3. On the **Server-Side Defaults** tab, click **Advanced Settings**.
4. On the **Advanced settings** page, click **Set Namespaces** to open the **Namespace list** page. This is where you can add namespaces.
5. To add a namespace, on the **Namespace list** page, select **All namespaces**, click **Add**.
6. To enable monitoring for all namespaces, select **Enable monitoring**. If you want to make all namespaces an entry point, select **Enable as entrypoint**. Click **OK**.

Tip

With web applications you typically do not need to enable a namespace or class as an entry point. Entry points are used as the trigger to start measuring performance. .NET provides well-known entry points that should cover the majority of web applications. You need to set the entry point flag only if the monitored application is called through a custom interface.

See Also

Understanding and Using Assemblies and Namespaces in .NET

How to Add, Edit, and Remove Methods

Methods define entry points used to start measuring for performance events and to monitor for exceptions. If the application defines custom entry points that are not directly called from .NET, these entry points might not be monitored because we don't that calls to this function are not part of an existing transaction. Methods also let you make fine-grained changes to how data is collected by .NET Application Performance Monitoring. You can create a method for a specific function and then disable monitoring or disable the collection of parameters. This allows you to ensure that functions working with sensitive data are not going to send that data to the development team who might be working with performance events.

Add a Method

To add a method

1. To open the .NET Application Performance Monitoring template, in the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Templates**, and then click **.NET Application Performance Monitoring**.
2. Right click the application group whose settings you want to modify, and then select **Properties**.
3. On the **Server-Side Defaults** tab, click **Advanced Settings**.
4. On the **Advanced settings** page, click **Set Methods** to open the **Methods list** page. This is where you can add methods.
5. To add a method, on the **Methods list** page, click **Add**, type the method name and in the **Settings** section, select if you want to **Enable monitoring**, set a **Sensitivity threshold** for this method, and **Collect function parameters**. Click **OK** and the application performance monitoring service will add this method to the list of monitored methods.

   Important
   Adding Methods that are defined in the .NET Framework as part of mscorlib will not produce any effect.

   Note
   The method name is case-sensitive and should be specified in the following format: Namespace.ClassName.MethodName

Edit a Method

To edit a method

1. To open the .NET Application Performance Monitoring template, in the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Templates**, and then click **.NET Application Performance Monitoring**.
2. Right click the application group whose settings you want to modify, and then select **Properties**.
3. On the **Server-Side Defaults** tab, click **Advanced Settings**.
4. On the **Advanced settings** page, click **Set Methods** to open the **Methods list** page. This is where you can edit methods.
5. To edit a method, on the **Methods list** page, click **Edit**, make your changes, and then click **OK**.

   Note
   The method name is case-sensitive and should be specified in the following format: Namespace.ClassName.MethodName

Remove a Method

To remove a method

1. To open the .NET Application Performance Monitoring template, in the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Templates**, and then click **.NET Application Performance Monitoring**.
2. Right click the application group whose settings you want to modify, and then select **Properties**.
3. On the **Server-Side Defaults** tab, click **Advanced Settings**.
4. On the **Advanced settings** page, click **Set Methods** to open the **Methods list** page. This is where you can remove methods.
5. To remove a method, on the **Methods list** page, select the method you want to remove, click **Remove**, and then click **OK**.

How to Add, Edit, and Remove Exception Tracking

Adding functions to the Exception tracking list allows you to add namespace or classes where Operations Manager tracks exception parameters or variables and collects additional information about each exception that is raised from a namespace or class.

The default list of .NET functions that are monitored for exceptions includes namespaces and functions, some of which have monitoring disabled by default. For more information, see Using Exception Handlers to Define Critical Exceptions, which includes a list of default exception handlers.

Warning

Exception tracking is set on the process level. If you add a function to the Exception tracking list for an application that is running in the process and then disable it for a different application running in that process, there will be a conflict and application monitoring will be disabled. To resolve this, you must make the Exception tracking list the same for all applications in the same process.

Add a Class or Namespace to the Exception Tracking List

To add a class or namespace to the exception tracking list

1. To open the .NET Application Performance Monitoring template, in the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Templates**, and then click **.NET Application Performance Monitoring**.
2. Right click the application group whose settings you want to modify, and then select **Properties**.
3. On the **Server-Side Defaults** tab, click **Advanced Settings**.
4. On the **Advanced settings** page, click **Exception tracking** to open the **Exception tracking class or namespace** page. This is where you can add classes or namespaces where you intend to collect exceptions.
5. To add a class or namespace, on the **Exception tracking class or namespace** page, click **Add**, select whether you want to collect exceptions for a particular **Namespace or class** or for **All namespaces**, and then type the class or namespace you want to add. The **Enable monitoring** checkbox is selected by default, which means that you want to enable monitoring for this class or namespace. To explicitly disable monitoring of exceptions in a particular class or namespace, clear the checkbox. Click **OK**.

   For System Center 2012 SP1 only: **All namespaces** is present and enabled in this list by default. However, **All namespaces**, does not include namespaces that have been explicitly disabled.

Important
Adding Exception Tracking for namespaces or classes that are defined in the .NET Framework as part of mscorlib will not produce any effect.

Note
The Namespace and Class names are case-sensitive and should be specified in the following format: Namespace.ClassName

Edit a Class or namespace on the Exception Tracking List

To edit a class or namespace on the exception tracking list

1. To open the .NET Application Performance Monitoring template, in the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Templates**, and then click **.NET Application Performance Monitoring**.
2. Right click the application group whose settings you want to modify, and then select **Properties**.
3. On the **Server-Side Defaults** tab, click **Advanced Settings**.
4. On the **Advanced settings** page, click **Exception tracking** to open the **Exception tracking class or namespace** page. This is where you can edit the list of classes or namespaces where to look for exceptions.
5. To edit a class or namespace, on the **Exception tracking class or namespace** page, click **Edit**, modify the settings you want to change, and then click **OK**.

   Note
   The Namespace and Class names are case-sensitive and should be specified in the following format: Namespace.ClassName

Remove a Class or Namespace on the Exception Tracking List

To remove a class or Namespace on the exception tracking list

1. To open the .NET Application Performance Monitoring template, in the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Templates**, and then click **.NET Application Performance Monitoring**.
2. Right click the application group whose settings you want to modify, and then select **Properties**.
3. On the **Server-Side Defaults** tab, click **Advanced Settings**.
4. On the **Advanced settings** page, click **Exception tracking** to open the **Exception**

tracking class or namespace page. This is where you can remove classes or namespaces from the list.

5. To remove a class or namespace, on the **Exception tracking class or namespace** page, click **Edit**, modify the settings you want to change, and then click **OK**.

Note
The Namespace and Class names are case-sensitive and should be specified in the following format: Namespace.ClassName

Using Exception Handlers to Define Critical Exceptions

Exception handlers are application functions that “catch” exceptions that the applications throw to report errors and perform some error handling. By default, .NET Application Performance Monitoring defines critical exceptions as exceptions handled by specific exception handlers provided by the .NET framework. These handlers catch top-level ASP.NET exceptions, and web service exceptions that the monitored application failed to catch and handle internally. By adding exception handlers, you are adding to what application monitoring’s definition of what a critical exception is. In effect, any exceptions handled by these functions will be considered critical exceptions. The advantage to doing this is that you maintain the benefit of streamlined reporting of critical exceptions only, but you have the additional benefit of reporting functions that are of interest to you. It is common to add any customer error handlers defined for web applications to the list of critical exception handlers so that you can be alerted when a user is sent to your error handler page in the web application.

Warning
Exception handlers are set on the process level. If you enable an exception handler for an application that is running in the process and then disable it for a different application running in that process, there will be a configuration conflict and application monitoring will be disabled. To resolve this, you must make the exception handling the same for all applications in the same process.

Default Exception Handlers

The default list of exception handlers includes:

- System.Web.HttpApplication.RecordError
- System.Web.UI.Page.HandleError
- System.Web.Services.Protocols.WebServiceHandler.WriteException
- System.AppDomain.OnUnhandledExceptionEvent
- System.Windows.Forms.Application.ThreadContext.OnThreadException

- System.AppDomain.OnUnhandledExceptionEvent
- System.Runtime.Remoting.Messaging.ReturnMessage..ctor
- System.Windows.Forms.DataGridView.OnDataError

For System Center 2012 SP1 these resources are included:

- Microsoft.Office.Server.Data.SqlSession.LogException
- Microsoft.Office.Excel.Server.CalculationServer.Proxy.ExcelServerProxy.ProcessSoapException
- Microsoft.Office.Excel.Server.CalculationServer.Proxy.ExcelServerProxy.ProcessWebException
- Microsoft.SharePoint.Portal.WebControls.BusinessDataWebPart.ConstructErrorMessage
- Microsoft.SharePoint.Diagnostics.ULS.SendEventTag
- Microsoft.SharePoint.ApplicationRuntime.SPRequestModule.IsWebPartOnExceptionStack
- Microsoft.SharePoint.Utilities.SqlSession.LogException
- Microsoft.Office.Web.Environment.Sharepoint.Diagnostics.ULS.SendExceptionTag
- Microsoft.SharePoint.Diagnostics.ULS.SendExceptionTag
- Microsoft.Office.Server.Diagnostics.ULS.SendExceptionTag
- System.Workflow.Runtime.WorkflowExecutor.IsIrrecoverableException
- System.ServiceModel.DiagnosticUtility.IsFatal
- System.Web.Mvc.ControllerActionInvoker.InvokeExceptionFilters

Add an Exception Handler

To add an exception handler

1. To open the .NET Application Performance Monitoring template, in the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Templates**, and then click **.NET Application Performance Monitoring**.
2. Right click the application group you want to modify, and then select **Properties**.
3. On the **Server-Side Defaults** tab, click **Advanced Settings**.
4. On the **Advanced settings** page, click **Critical Exceptions** to open the **Exception handlers list** page. This is where you can add exception handlers.
5. To add an exception handler, click **Add** and type the method you want to add to the exception handlers list. If you want this exception handler to affect monitoring, make sure the **Enable monitoring** checkbox is selected. Click **OK**.

   Important
   Adding handlers that are defined in the .NET Framework as part of mscorlib as Critical Exceptions will not produce any effect.

Note
The method name is case sensitive and should be specified in the following format: Namespace.ClassName.MethodName

Edit an Exception Handler

To edit an exception handler

1. Open the .NET Application Performance Monitoring template. In the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Templates**, and then click **.NET Application Performance Monitoring**.
2. Right click the application group you want to modify and select **Properties**.
3. On the Server-Side Defaults tab, click **Advanced Settings**.
4. On the **Advanced settings** page, click **Critical Exceptions**. This opens the **Exception handlers list** page where you can edit exception handlers.
5. To edit an exception handler, click **Edit**, select the exception handler you want to change, and then modify it. Click **OK**.

Note
The method name is case sensitive. Additionally, the method name should be specified in the following format: Namespace.ClassName.MethodName

Remove an Exception Handler

To remove an exception handler

1. Open the .NET Application Performance Monitoring template. In the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Templates**, and then click **.NET Application Performance Monitoring**.
2. Right click the application group you want to modify and select **Properties**.
3. On the Server-Side Defaults tab, click **Advanced Settings**.
4. On the **Advanced settings** page, click **Critical Exceptions**. This opens the **Exception handlers list** page where you can remove exception handlers.
5. To remove an exception handler, select the exception handler you want to remove, click **Remove**, and then click **OK**.

Client-Side Monitoring with Targeted Groups and Load Balancers

When load balancers are used during client-side monitoring, the load balancer is designed to get the true client IP addresses. In a simple case, when a client is connected directly to one web server, the web server knows the client IP address. However, when you have several servers and use a load balancer to distribute traffic from the clients among the servers, this can present two problems. First, the IP reported to the collector is the virtual IP that the load balancer uses, not the real end-user IP. When users hit the load balancer, it sends them to an appropriate web server. Due to the load balancer, the web server sees only the internal port IP (inside the network), not the real IP (outside the network). Additionally, if some servers are monitored and some are not, data can be lost because responses from the clients are often sent to servers in a least load or round robin fashion, which means that the response might go to a server that is not hosting a collector.

Here are some strategies for setting up client-side monitoring when you have multiple monitored servers and use load balancers.

Monitoring with a Load Balancer and Targeted Group

When you configure client-side monitoring, you have the option to set the target group, limiting the number of web servers used for monitoring. In this scenario, only monitored servers in the target group will inject the JavaScript used for monitoring and the servers outside the target group that are not monitored will not get instrumented when using load balancers with the web servers. This results in having incorrect data. The load balancer does not know which servers are inside or outside the targeted group and sends client requests to servers that are both inside (monitored) or outside (unmonitored) of the targeted group. The result is that requests that have been instrumented and try to return data to the collectors might send their results to servers that cannot handle the data.

- **Solution 1** If you are authoring a new .NET Application Performance Monitoring template and including client-side monitoring for a targeted group, we recommend that you choose a group of servers that are all served by the same load balancer. Target monitoring to all servers in the load-balanced farm.
- **Solution 2** If you are already running client-side monitoring with a targeted group and a load balancer, you can resolve this issue by creating a rule on the load balancer that directs all of the monitoring traffic to the monitored servers. Monitoring traffic is the monitoring JavaScripts that send data to the collector endpoint. You can identify monitoring traffic because it contains **/CSMCollector** in the URL. Each load balancer has its own model for configuring rules. Refer to your load balancer's documentation for details about how to create the rule.

How to Configure IP Address Exclusion Filters for Client-Side Monitoring

You can use client IP filters to choose the networks that you want to monitor. By applying filters, administrators can limit the scope of the monitored computers. By default, only localhost is monitored. If the IP filter list is empty, all IP addresses are monitored. Any IP addresses that fit the filter definitions are excluded from client-side monitoring.

The following examples show how to use IP filters to monitor IP addresses.

Exclude a Set of IP Addresses from Monitoring

Example: To monitor all IP addresses except 192.168.*.*

1. To monitor all IP addresses, except some (IP addresses 192.168.*.* in this example), on the **Client Side Configuration** tab, in the **Configure client IP filter** section, click **Add**.
2. On the **Client IP address filter** page, set the **Comparison Type** to **IP is in subnet**.

   Note
   Comparison type has two values: **In subnet** excludes user IP addresses that match the IP addresses in the subnet. **Not in subnet** excludes the user IP addresses that do not match the IP addresses in the subnet.
3. In the **IP address** box, enter the IP addresses that you want to exclude from monitoring. In this example, enter **192.168.0.0**.
4. In the **Netmask** box, enter the part of the filter IP address and user IP address that have to be compared for equality. In this example, enter **255.255.0.0**.
5. Click **OK**.

Monitor a Specific Set of IP Addresses

Example: To monitor the specific set IP addresses 192.168.*.*

1. To monitor a specific set of IP addresses (in this example, IP addresses 192.168.*.*), on the **Client Side Configuration** tab, in the **Configure client IP filter** section, click **Add**.
2. On the **Client IP address filter** page, set the **Comparison Type** to **IP is not in subnet**.
3. In the **IP address** box, enter the IP addresses that you want to monitor. In this example, enter **192.168.0.0**.
4. In the **Netmask** box, enter the part of the filter IP address and user IP address that have to be compared for equality. In this example, enter **255.255.0.0**.
5. Click **OK**.

Monitor a Specific Set of IP Addresses and Exclude Some IP Addresses from that Set

Example: To monitor IP addresses 192.168.*.* and exclude IP addresses 192.168.10.*

1. To monitor a specific set of IP addresses and exclude some from that set (in this example, only IP addresses 192.168.*.*, except IP addresses 192.168.10.*), you have to configure two filters. First, create the filter to scope to only IP addresses 192.168.*.*, and then a filter that excludes 192.168.10.*. To create the first filter to monitor only IP addresses 192.168.*.*, on the **Client Side Configuration** tab, in the **Configure client IP filter** section, click **Add**.
2. Set the **Compare Type** to **IP is not in subnet**.
3. In the **IP address** box, enter the IP addresses that you want to monitor. In this example, enter **192.168.0.0**.
4. In the **Netmask** box, enter the part of the filter IP address and user IP address that have to be compared for equality. In this example, enter **255.255.0.0**.
5. Click **OK**.
6. Then, create the second IP filter to exclude IP addresses 192.168.10.*. On the **Client Side Configuration** tab, in the **Configure client IP filter** section, click **Add**.
7. Set the **Compare Type** to **IP is in subnet**.
8. In the **IP address** box, enter the IP addresses that you want to exclude from monitoring. In this example, enter **192.168.10.0**.
9. In the **Netmask** box, enter the part of the filter IP address and user IP address that have to be compared for equality. In this example, enter **255.255.255.0**.
10. Click **OK**.

When to Use the IPv4 and IPv6 Filters

If the IPv4 protocol is the only protocol that is enabled on the web server, leave the **Use IPv6** check box blank.

If the IPv6 protocol is enabled on the web server, select the **Use IPv6** check box to add the IPv6 filter.

How to Start Monitoring a New Application

When you have a new application that you are learning about, you can use the .NET Application Performance Monitoring template in System Center 2012 – Operations Manager to configure monitoring for it. Here are some settings to start with that will help you get to know your new application. In addition, it is ideal that you begin monitoring in a test or development environment.

Monitoring Settings for a New Application

Following this strategy for monitoring a new application will help you get to know how the application behaves within your system and for your customer.

Start Monitoring Server-Side Only with a Simple Monitored System and Short-Term Settings

First, keep the configuration simple: monitor one application on one server. Second, when you first configure .NET Application Performance Monitoring to monitor a new application, plan to keep the settings you implement long enough for you to understand some trends. A day's worth of data should provide you with insight into the performance and usage patterns of the application.

Establish Baseline Performance Using Default Settings and Some Specific Settings

For the most part, you will want to keep default settings. The default settings ensure that you will see any large issues with the application and keep the impact on the monitored application at a minimum.

If you are not getting any performance or exception events raised, you can use the following steps to get a feel for what the baseline performance looks like.

To begin monitoring, here are some settings you might want to adjust as noted here:

- Lower the thresholds for performance. This will help you establish a baseline performance measure by seeing what the current performance characteristics of the application are.
- Enable all namespaces. You want to find out what namespaces are involved and if you set specific namespaces at first, you might miss a namespace where an error is occurring.
- Collect all exceptions, not just critical exceptions. You need to know what kinds of exceptions are being thrown. Using known exception handlers limits the exceptions you will receive.

This can result in a lot of data—more than you would want for long-term monitoring—but at first, this amount of data will be helpful as you will see trends, such as the kinds of paths customers are taking through the system and what normal performance looks like.

With the data collection complete, use the Application Advisor reports, such as Application Performance Analysis, to see how the monitored applications are looking. Using the report you will see what the average duration is for the heaviest (longest running) calls through the system as well as the maximum amount of time spent processing requests. This allows you to set customized smart thresholds based on real application performance. You will also see which functions are running faster than others, and you can create specific web page, web method, and function transactions for the critical methods so that you can ensure they are responding under a tighter SLA than the application as a whole. For more information on viewing reports, see how to scope and run and Application Advisor report in Prioritizing Alerts by Using Application Advisor.

Adjust Settings and Compare to the Baseline

Once you have established a baseline performance measure, begin to adjust the settings to tune the monitoring so it catches the kinds of exceptions that are being raised. By reporting all exceptions, you will see if there are any default exception handlers in the application that are catching exceptions for which you would prefer receiving alerts. The data you get will be more meaningful and lower in volume with each adjustment.

- Remove the custom settings and set thresholds based on the data collected.
- Add specific namespaces based on the call stacks in the performance and exception events you found during the baseline phase.
- Add exception handlers for any application level “catch all” handlers that keep exceptions from going outside the application and to the .NET Framework exception handlers.
- Add specialized transactions to monitor the performance of common methods that should be held to a stronger SLA than the application as a whole.

Compare the new data to your baseline. You will begin to see the real average response time, for instance. Now that you know the various performance exceptions the application is sending, you can add the specific namespaces you want rather than monitoring all namespaces. Your application will be configured to be monitored based on the observed performance levels and will be alerted if things move outside of normal levels.

Gradually Deploy the Application to More Monitored Servers in Your System

After monitoring the application for a time with the new monitoring configuration, when you feel your application is healthy, increase the number of servers you are running the application on and monitoring from one to 10, for example. Once you have it running healthy at that level, increase the deployment and monitoring to more servers, and so on. This gradual rollout approach will help you gain confidence in the monitoring for that application and help ensure the health of your system.

Begin Client-Side Monitoring

When you are confident that your application is running well within your system, it’s a good time to monitor what the customer experiences. This is what client-side application monitoring does. To enable client-side monitoring, see How to Configure Monitoring for .NET Applications

What the Operator can do with This Information

Using this basic information, the operator can have a better idea where the problem is with the application or with the infrastructure and know whether it is something only to the development team can fix or the operator can address directly.

See Also

How to Add, Enable, and Disable Namespaces

Using Exception Handlers to Define Critical Exceptions

Authoring Strategies for .NET Application Monitoring

Application Monitoring Using the Default Settings

Authoring Strategies for .NET Application Monitoring

Here are some scenarios and settings to change during authoring that can help you receive the monitoring experience and data that are most helpful for you.

Monitoring a New Application for which the Administrator has Little Knowledge

Accepting all defaults can be a good way to start monitoring an application for which the administrator has very little or no knowledge. Then, after monitoring with all defaults for some time, the administrator can begin adjusting settings based on the monitoring alerts, Application Diagnostics data, and Application Advisor reports. For more information, see How to Start Monitoring a New Application and Application Monitoring Using the Default Settings

Limit Monitoring to a Specific Set of Servers

Defining a targeted group allows you to limit monitoring to a specific set of servers. In the .NET Application Performance Monitoring wizard, targeted group for server-side monitoring is on the **What to Monitor** page. Targeted group for client-side monitoring is on the **Enable Client-Side Monitoring** page. If you are using a targeted group for client-side monitoring and use a load balancer, see Client-Side Monitoring with Targeted Groups and Load Balancers

For very large application deployments, you typically do not need to monitor all instances of the application. A representative sample is enough to get the data you need. Using only a representative sample will keep the amount of data collected and stored lower.

Reduce the “Noise” by Defining How Much Data You Collect

Increasing the sensitivity threshold allows you to filter out fast-running methods, which reduces overall “noise”, or how deep the call stack is going to go, making it easier for you to determine where the problem is. It also reduces network bandwidth usage.

The sensitivity setting is used to determine if a function call should be included in the call stack. Any function that executes and returns faster than the sensitivity level is dropped, keeping small fast-running functions from hiding the actual problem. Remember that using sensitivity only reduces the number of functions shown in the call stack for specific events, but an event will still be generated if the overall threshold is surpassed.

You can adjust the sensitivity threshold for server-side and client-side monitoring independently.

To change the sensitivity threshold for server-side monitoring

1. To open properties for the application group that you want to reconfigure, in the Operations Manager console, in the navigation pane, click the **Authoring** button, expand **Management Pack Templates**, click **.NET Application Performance Monitoring**, right-click the application group that you want to want to configure, and then select **Properties**.

   Note
   If you are currently authoring a new .NET Application Performance Monitoring template, to change the sensitivity threshold for server-side monitoring, go to the **Server-Side Configuration** page and click **Advanced Settings** Change the **Sensitivity threshold** and click **OK**.
2. To change the sensitivity threshold for server-side monitoring, on the **Properties** page, click the **Server-Side Monitoring** tab, and then click the **Advanced Settings** button.
3. Change the **Sensitivity threshold** and click **OK**.

To change the sensitivity threshold for client-side monitoring

1. To open properties for the application group that you want to reconfigure, in the Operations Manager console, in the navigation pane, click the **Authoring** button, expand **Management Pack Templates**, click **.NET Application Performance Monitoring**, right-click the application group that you want to want to configure, and then select **Properties**.

   Note
   If you are currently authoring a new .NET Application Performance Monitoring template, to change the sensitivity threshold for client-side monitoring, go to the **Client-Side Configuration** page and click **Advanced Settings**. Change the **Sensitivity threshold** and click **OK**.
2. To change the sensitivity threshold for client-side monitoring, on the **Properties** page, click the **Client-Side Monitoring** tab, and then click the **Advanced Settings** button.
3. Change the **Sensitivity threshold** and click **OK**.

It is also possible for high sensitivity to hide problems. In the situation where you have a function that calls another function, if the callee's response time increases even slightly, it might cause issues for the application. For example, if you have a data processing function that calls a lookup function 1,000 times and the lookup's processing time increases by 1 ms, you will increase the response time for your top level function by a full second. This might be masked by the high sensitivity. When you find this kind of situation, you can add the callee as a method and set a

custom sensitivity for it to ensure it is always measured according to the lower sensitivity threshold.

Application failure alerts are application, or code, failures that are detected within the application. You can choose not to receive application failure alerts, which will potentially occur very often if an application has problems because these kinds of alerts usually require code modifications to address. Turning this off reduces the “noise” of many alerts raised that cannot be directly resolved by the operations team.

You can turn off application failure alerts for server-side and client-side monitoring independently.

To turn off alerts for application failures for server-side monitoring

1. To open properties for the application group that you want to reconfigure, in the Operations Manager console, in the navigation pane, click the **Authoring** button, expand **Management Pack Templates**, click **.NET Application Performance Monitoring**, right-click the application group that you want to want to configure, and then select **Properties**.

   Note
   If you are currently authoring a new .NET Application Performance Monitoring template, to turn off alerts for application failures for server-side monitoring, go to the **Server-Side Configuration** page and click **Advanced Settings**. Clear the **Application failure alerts** checkbox and click **OK**.
2. To turn off application failure alerts for server-side monitoring, on the **Properties** page, click the **Server-Side Defaults** tab, and then click the **Advanced Settings** button.
3. On the **Advanced settings** page and clear the **Application failure alerts** checkbox.
4. Click **OK**.

To turn off alerts for application failures for client-side monitoring

1. To open properties for the application group that you want to reconfigure, in the Operations Manager console, in the navigation pane, click the **Authoring** button, expand **Management Pack Templates**, click **.NET Application Performance Monitoring**, right-click the application group that you want to want to configure, and then select **Properties**.

   Note
   If you are currently authoring a new .NET Application Performance Monitoring template, to turn off alerts for application failures for client-side monitoring, go to the **Client-Side Configuration** page and click **Customize**. On the **Modifying Settings** page, in the **Transactions** section, click **Add**. On the **Transaction Properties** page, clear the **Application failure** checkbox and click **OK**.
2. To turn off application failure alerts for client-side monitoring, on the **Properties** page, click the **Client-Side Monitoring** tab, and then click the **Advanced Settings** button.
3. In the **Transactions** section, click **Add**.
4. On the **Transaction Properties** page, clear the **Application failure** checkbox.
5. Click **OK**.

Only Receive Critical Exceptions

By default, .NET Application Performance Monitoring defines critical exceptions as exceptions handled by specific exception handlers provided by the .NET framework. These handlers catch top-level ASP.NET exceptions and web service exceptions that the monitored application failed to catch and handle internally. By adding exception handlers, you are adding to what application monitoring's definition of what a critical exception is. In effect, any exceptions handled by these functions will be considered critical exceptions. The advantage to using exception handlers is that you maintain the benefit of streamlined reporting of critical exceptions only, but you have the additional benefit of reporting functions that are of interest to you. For more information and a list of default exception handlers, see Using Exception Handlers to Define Critical Exceptions.

Improve Client-Side Monitoring Performance and Reduce Load on Your Server

You might also want to adjust the sampling rate to control the performance impact of the monitoring on your application with client-side monitoring. Reducing the sampling rate reduces the application monitoring traffic and helps conserve server resources. If you have even a low-traffic site, instrumenting and collecting data from every user who connects will result in a large amount of non-actionable data to sift through. Taking a random sample will give you the insight you need into the application performance from the client perspective without flooding you with a large amount of data to process and store.

To change the sampling rate for client-side monitoring

1. To open client-side properties for the application group that you want to reconfigure, in the Operations Manager console, in the navigation pane, click the **Authoring** button, expand **Management Pack Templates**, click **.NET Application Performance Monitoring**, right-click the application group that you want to want to reconfigure, and then select **Properties**.

   On the **Properties** page, click the **Client-Side Defaults** tab, and then click the **Advanced Settings** button.

   Note
   Because you can change the sampling rate for both the application group and each application component, changes to the application group settings will not automatically be applied to the component settings when the component settings have been previously customized.
2. In the **Sampling** section, use the drop-down menu to select the percentage of incoming requests that you want to monitor. For example, if you select **50%**, you will monitor 50 percent of the incoming requests. Select **25%** and you will monitor 25 percent of the incoming requests, and so on. To get helpful information, you do not have to monitor all of the incoming requests.
3. When you have set the sampling rate, click **OK**.

See Also

How to Start Monitoring a New Application

Application Monitoring Using the Default Settings

Accepting all defaults can be a good way to start monitoring an application for which the administrator has very little or no knowledge. Then, after monitoring with all defaults for some time, the administrator can begin adjusting settings based on the monitoring alerts, Application Diagnostics data, and Application Advisor reports.

Using Default Settings for Server-Side Monitoring

You still need to select the application you want to monitor and the target management pack, but then you can start monitoring with “all defaults”. With all default settings Application Performance Monitoring will monitor only server-side, and all thresholds for all pages will be the same. To see the default values, you can go through the wizard without changing anything.

Using Default Settings for Client-Side Monitoring

The defaults are enough to get this started and to allow you to test it out from localhost connections. It is simply scoped to monitor localhost by default.

You can certainly accept the default settings for client-side monitoring, but it is very important to run the compatibility check task to validate if the application can be monitored and if any of the pages should be excluded from monitoring. Therefore, simply applying of client-side monitoring defaults might be risky. For more information about running the compatibility check task, see Before You Begin Monitoring .NET Applications

In general, client-side threshold settings should be higher than server-side threshold settings. This is because the client-side monitoring contains the server time, too. For instance, when a client-side event is divided into various parts, some of the time is spent on the server, but the client also monitors the time spent on the network and the time spent in the browser.

IP Address Filters and Load balancers Also, IP filters by default will enable client-side monitoring for localhost only. Additionally, load balancer settings need to be set correctly for client-side monitoring. If the IP header is not set, all client-side monitoring traffic will appear to be coming from a single IP address. All IP- and subnet- based reports in Application Advisor will be invalid if the default settings are used with a load balancer.

There is no default for the load balancers. The load balancer setting is one you can opt to change, whereas you must change the client IP filters because if you do not update those settings you will not get any data at all.

IP Address Filters You can use client IP filters to choose the networks that you want to monitor. By applying filters, administrators can limit the scope of the monitored computers. By default, only localhost IP addresses are monitored. If the IP filter list is empty, all IP addresses are monitored. Any IP addresses that fit the filter definitions are excluded from client-side monitoring. For more information, see How to Configure IP Address Exclusion Filters for Client-Side Monitoring

See Also

Authoring Strategies for .NET Application Monitoring

How to Start Monitoring a New Application

Monitoring SharePoint 2010 Applications in System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

SharePoint application technologies provide various extensibility and customization mechanisms. Custom application code running in SharePoint environment can extend or replace standard pages, can implement custom business rules, often integrates with third-party components, and custom solutions written to operate using SharePoint framework. The customizations and code errors in custom components can affect server performance, significantly impacting overall application experience.

Operations Manager lets you monitor SharePoint 2010 web front-end components. You can monitor standard and custom SharePoint webpages for performance degradation and server-side exceptions.

Warning
Client-side .NET Application Performance Monitoring (APM) is not supported for SharePoint. Enabling client-side .NET Application Performance Monitoring for SharePoint can result in unpredictable application behavior and failures.

Monitoring for SharePoint Applications

SharePoint web front-end components are natively discovered by the IIS management pack as endpoints. You can enable monitoring for SharePoint applications in much the same way you enable monitoring for other .NET web applications. Use the .NET Application Performance Monitoring template to configure SharePoint application monitoring. For more information, see .NET Application Performance Monitoring Template.

When monitoring SharePoint applications for performance violations, events in Application Diagnostics contain additional information, such as **SharePoint server API calls** and **Web Part calls**. For each API call, the APM agent will collect relevant SharePoint methods parameters. The APM agent also tracks the execution time for the slowest calls. When detecting performance

issues from standard SharePoint webpages using web parts, the slowest resource calls are shown and poorly performing web part names are collected next to the location of the web part on the SharePoint page. When detecting performance issues from custom SharePoint webpages, only the SharePoint API calls are shown.

When monitoring SharePoint applications for exceptions, the exception call stack contains the relevant SharePoint specific parameters available for troubleshooting.

Appendix for .NET Application Monitoring

Information in this appendix is the default entry points and default methods, which includes resource calls and functions that are included with .NET Application Performance Monitoring in System Center 2012 – Operations Manager.

See Also

Default Entry Points for .NET Application Monitoring

Default Methods for .NET Application Monitoring

Default Entry Points for .NET Application Monitoring

Application Performance Monitoring in Operations Manager is preconfigured with many well-known entry points (see below), but also lets you extend the default list by defining your own entry points. In addition to adding functions as entry points, you may also define entire Namespaces to act as entry points, so that the system begins timing execution the first time that it encounters the namespace during execution. Additionally, the application monitoring agent collects the values of variables for each entry point at the time the event occurs.

Entry points Monitored by Default

For ASP.NET pages

- System.Web.UI.Page.ProcessRequest
- (System.Web.IHttpHandler).ProcessRequest

For ASP.NET 2.0 asynchronous pages

- For System Center 2012 SP1 only: System.Web.UI.Page.AsyncPageBeginProcessRequest
- System.Web.Services.Protocols.LogicalMethodInfo.Invoke

-

For COM+ server-side

- System.EnterpriseServices.ServicedComponent.RemoteDispatchHelper

For .NET Remoting server-side

- System.Runtime.Remoting.Messaging.ServerObjectTerminatorSink.AsyncProcessMessage
- System.Runtime.Remoting.Messaging.ServerObjectTerminatorSink.SyncProcessMessage

For WCF Server Side

- System.ServiceModel.Dispatcher.SyncMethodInvoker.Invoke

For WWF

- System.Workflow.Runtime.WorkflowExecutor.RunScheduler

For AJAX.NET

- System.Web.Script.Services.RestHandler.ExecuteWebServiceCall

For Windows Services

For System Center 2012 SP1 these entry points are included:

- System.ServiceProcess.ServiceBase.ServiceCommandCallback
- System.ServiceProcess.ServiceBase.ServiceQueuedMainCallback
- System.ServiceProcess.ServiceBase.Stop
- System.ServiceProcess.ServiceBase.DeferredPowerEvent
- System.ServiceProcess.ServiceBase.DeferredSessionChange

For MVC

For System Center 2012 SP1 these entry points are included:

- System.Web.Mvc.ControllerBase.Execute
- (System.Web.Mvc.IController).Execute
- System.Web.Mvc.AsyncController.BeginExecute
- (System.Web.Mvc.IAsyncController).BeginExecute
- System.Web.Mvc.ViewResultBase.ExecuteResult

Default Methods for .NET Application Monitoring

Application Performance Monitoring in Operations Manager includes many functions and resources calls that are monitored by default.

Functions Monitored by Default

Application Performance Monitoring includes many well-known Microsoft .NET Framework functions that are monitored for slow performance or exception data collection.

For SharePoint

For System Center 2012 SP1 these resources are included:

- Microsoft.Office.Excel.WebUI.ExcelWebRenderer.OnPreRender
- Microsoft.Office.Excel.WebUI.InternalEwr.OnPreRender
- Microsoft.SharePoint.Portal.WebControls.ContactFieldControl.OnPreRender
- Microsoft.SharePoint.Portal.WebControls.IndicatorWebpart.OnPreRender
- Microsoft.SharePoint.Portal.WebControls.KPIListWebPart.OnPreRender
- Microsoft.SharePoint.WebPartPages.ContentEditorWebPart.RenderWebPart
- Microsoft.SharePoint.WebPartPages.ContentEditorWebPart.OnPreRender
- Microsoft.SharePoint.WebPartPages.ListFormWebPart.OnPreRender
- Microsoft.SharePoint.WebPartPages.ListFormWebPart.RenderWebPart
- Microsoft.SharePoint.WebPartPages.ListViewWebPart.CreateChildControls
- Microsoft.SharePoint.WebPartPages.ListViewWebPart.RenderWebPart
- Microsoft.SharePoint.WebPartPages.ListViewWebPart.OnInit
- Microsoft.SharePoint.WebPartPages.ListViewWebPart.OnPreRender
- Microsoft.SharePoint.Portal.WebControls.BusinessDataActionsWebPart.RenderWebPart
- Microsoft.SharePoint.Portal.WebControls.GroupDetailWebPart.RenderWebPart
- Microsoft.SharePoint.Portal.WebControls.RelatedGroupsWebPart.RenderWebPart
- Microsoft.SharePoint.Portal.WebControls.WebPartLoc.OnPreRender
- Microsoft.SharePoint.Portal.WebControls.WebPartLoc.RenderWebPart
- Microsoft.SharePoint.Search.Internal.WebControls.SearchPagingWebPart.OnPreRender
- Microsoft.SharePoint.Search.Internal.WebControls.SearchPagingWebPart.RenderWebPart
- Microsoft.SharePoint.Search.Internal.WebControls.SearchStatsWebPart.OnPreRender
- Microsoft.SharePoint.Search.Internal.WebControls.SearchStatsWebPart.RenderWebPart
- Microsoft.SharePoint.Search.Internal.WebControls.SearchSummaryWebPart.RenderWebPart

- Microsoft.SharePoint.Search.Internal.WebControls.SearchSummaryWebPart.OnPreRender
- Microsoft.SharePoint.WebPartPages.ImageWebPart.RenderWebPart
- Microsoft.SharePoint.WebPartPages.PageViewerWebPart.RenderWebPart
- Microsoft.SharePoint.WebPartPages.XmlWebPart.RenderWebPart
- Microsoft.SharePoint.WebPartPages.XmlWebPart.OnPreRender
- Microsoft.SharePoint.WebPartPages.AggregationWebPart.RenderWebPart
- Microsoft.SharePoint.WebPartPages.ChartViewWebPart.RenderWebPart
- Microsoft.SharePoint.WebPartPages.DataViewWebPart.OnPreRender
- Microsoft.SharePoint.WebPartPages.DataViewWebPart.RenderWebPart
- Microsoft.SharePoint.WebPartPages.ListFormWebPart.OnLoad
- Microsoft.SharePoint.WebPartPages.ListFormWebPart.OnInit
- Microsoft.SharePoint.Portal.WebControls.BusinessDataWebPart.GetCallbackResult
- Microsoft.SharePoint.Portal.WebControls.BusinessDataDetailsWebPart.CreateChildControls
- Microsoft.SharePoint.Portal.WebControls.BusinessDataListWebPart.CreateChildControls
- Microsoft.Office.Server.ApplicationRegistry.MetadataModel.Entity.ExecuteInternal
- Microsoft.Office.Server.ApplicationRegistry.SystemSpecific.WebService.WebServiceSystemUtility.ExecuteStatic
- Microsoft.Office.Server.ApplicationRegistry.SystemSpecific.Db.DbSystemUtility.ExecuteStatic
- Microsoft.SharePoint.WebPartPages.DataFormWebPart.OnPreRender

For SharePoint: Base Classes Monitoring

For System Center 2012 SP1 these resources are included:

- System.Web.UI.WebControls.WebParts.WebPart.OnDataBinding
- System.Web.UI.WebControls.WebParts.WebPart.OnPreRender
- System.Web.UI.WebControls.WebParts.WebPart.OnInit
- System.Web.UI.WebControls.WebParts.WebPart.OnLoad
- System.Web.UI.WebControls.WebParts.WebPart.Render
- System.Web.UI.WebControls.WebParts.WebPart.RenderWebPart
- System.Web.UI.WebControls.WebParts.WebPart.OnUnload
- [System.Web.UI.WebControls.WebParts.WebPart].OnDataBinding
- [System.Web.UI.WebControls.WebParts.WebPart].OnPreRender
- [System.Web.UI.WebControls.WebParts.WebPart].OnInit
- [System.Web.UI.WebControls.WebParts.WebPart].OnLoad
- [System.Web.UI.WebControls.WebParts.WebPart].Render
- [System.Web.UI.WebControls.WebParts.WebPart].RenderWebPart
- [System.Web.UI.WebControls.WebParts.WebPart].OnUnload

- [Microsoft.SharePoint.WebPartPages.WebPart].OnDataBinding
- [Microsoft.SharePoint.WebPartPages.WebPart].OnPreRender
- [Microsoft.SharePoint.WebPartPages.WebPart].OnInit
- [Microsoft.SharePoint.WebPartPages.WebPart].OnLoad
- [Microsoft.SharePoint.WebPartPages.WebPart].Render
- [Microsoft.SharePoint.WebPartPages.WebPart].RenderWebPart
- [Microsoft.SharePoint.WebPartPages.WebPart].OnUnload

For SharePoint: SPrequest Methods, Basic SharePoint 2007 APIs

For System Center 2012 SP1 these resources are included:

- Microsoft.SharePoint.Library.SPRequest.AccessContentTypes
- Microsoft.SharePoint.Library.SPRequest.AddField
- Microsoft.SharePoint.Library.SPRequest.AddGroup
- Microsoft.SharePoint.Library.SPRequest.AddMeeting
- Microsoft.SharePoint.Library.SPRequest.AddMeetingFromEvent
- Microsoft.SharePoint.Library.SPRequest.AddMeetingFromICal
- Microsoft.SharePoint.Library.SPRequest.AddNavigationNode
- Microsoft.SharePoint.Library.SPRequest.AddOnProvision
- Microsoft.SharePoint.Library.SPRequest.AddOrDeleteUrl
- Microsoft.SharePoint.Library.SPRequest.AddOrUpdateItem
- Microsoft.SharePoint.Library.SPRequest.AddRoleDef
- Microsoft.SharePoint.Library.SPRequest.AddSubscription
- Microsoft.SharePoint.Library.SPRequest.AddWebPart
- Microsoft.SharePoint.Library.SPRequest.AddWebPartPageToLibrary
- Microsoft.SharePoint.Library.SPRequest.AddWebPartRightsCheck
- Microsoft.SharePoint.Library.SPRequest.AddWorkflowAssociation
- Microsoft.SharePoint.Library.SPRequest.AddWorkflowToListItem
- Microsoft.SharePoint.Library.SPRequest.AddWorkItem
- Microsoft.SharePoint.Library.SPRequest.ApplyAutoHyperLinking
- Microsoft.SharePoint.Library.SPRequest.ApplyTheme
- Microsoft.SharePoint.Library.SPRequest.ApplyViewToListWebPart
- Microsoft.SharePoint.Library.SPRequest.ApplyWebTemplate
- Microsoft.SharePoint.Library.SPRequest.BackupSite
- Microsoft.SharePoint.Library.SPRequest.BreakRoleDefsInheritance
- Microsoft.SharePoint.Library.SPRequest.BuildCabinetFile
- Microsoft.SharePoint.Library.SPRequest.BypassUseRemoteApis
- Microsoft.SharePoint.Library.SPRequest.CalculatePermissionsForCurrentThread

- Microsoft.SharePoint.Library.SPRequest.CallCalcEngine
- Microsoft.SharePoint.Library.SPRequest.CancelMeeting
- Microsoft.SharePoint.Library.SPRequest.CancelWorkflow
- Microsoft.SharePoint.Library.SPRequest.ChangeAccountPassword
- Microsoft.SharePoint.Library.SPRequest.CheckInFile
- Microsoft.SharePoint.Library.SPRequest.CheckOutFile
- Microsoft.SharePoint.Library.SPRequest.CheckZoneProps
- Microsoft.SharePoint.Library.SPRequest.ClearAllVars
- Microsoft.SharePoint.Library.SPRequest.ClearListCache
- Microsoft.SharePoint.Library.SPRequest.ClearTimerStoreServer
- Microsoft.SharePoint.Library.SPRequest.CloseStream
- Microsoft.SharePoint.Library.SPRequest.CompleteInProgressWorkItems
- Microsoft.SharePoint.Library.SPRequest.ConfirmUsage
- Microsoft.SharePoint.Library.SPRequest.CreateAuditEntry
- Microsoft.SharePoint.Library.SPRequest.CreateAuditEntryForUrl
- Microsoft.SharePoint.Library.SPRequest.CreateCustomList
- Microsoft.SharePoint.Library.SPRequest.CreateFolderOnImport
- Microsoft.SharePoint.Library.SPRequest.CreateList
- Microsoft.SharePoint.Library.SPRequest.CreateListFromFormPost
- Microsoft.SharePoint.Library.SPRequest.CreateListOnImport
- Microsoft.SharePoint.Library.SPRequest.CreateListViewPart
- Microsoft.SharePoint.Library.SPRequest.CreateOrUpdateFileAndItem
- Microsoft.SharePoint.Library.SPRequest.CreateSite
- Microsoft.SharePoint.Library.SPRequest.CreateView
- Microsoft.SharePoint.Library.SPRequest.CreateViewOnImport
- Microsoft.SharePoint.Library.SPRequest.CreateWeb
- Microsoft.SharePoint.Library.SPRequest.CrossListQuery
- Microsoft.SharePoint.Library.SPRequest.CustomizeCssFile
- Microsoft.SharePoint.Library.SPRequest.DeleteAllFileVersions
- Microsoft.SharePoint.Library.SPRequest.DeleteAllListItemVersions
- Microsoft.SharePoint.Library.SPRequest.DeleteCommentsOfDocs
- Microsoft.SharePoint.Library.SPRequest.DeleteFileVersion
- Microsoft.SharePoint.Library.SPRequest.DeleteInProgressWorkItems
- Microsoft.SharePoint.Library.SPRequest.DeleteItem
- Microsoft.SharePoint.Library.SPRequest.DeleteList
- Microsoft.SharePoint.Library.SPRequest.DeleteListItemVersion
- Microsoft.SharePoint.Library.SPRequest.DeleteNavigationNode
- Microsoft.SharePoint.Library.SPRequest.DeleteSite

- Microsoft.SharePoint.Library.SPRequest.DeleteSubscription
- Microsoft.SharePoint.Library.SPRequest.DeleteView
- Microsoft.SharePoint.Library.SPRequest.DeleteWeb
- Microsoft.SharePoint.Library.SPRequest.DeleteWebPart
- Microsoft.SharePoint.Library.SPRequest.DeleteWebPartPagePersonalization
- Microsoft.SharePoint.Library.SPRequest.DeleteWebPartPagePersonalizationForAUser
- Microsoft.SharePoint.Library.SPRequest.DeleteWebPartPersonalization
- Microsoft.SharePoint.Library.SPRequest.DeleteWorkflowAssociation
- Microsoft.SharePoint.Library.SPRequest.DeleteWorkItem
- Microsoft.SharePoint.Library.SPRequest.DetectOrphans
- Microsoft.SharePoint.Library.SPRequest.DispatchTimerJob
- Microsoft.SharePoint.Library.SPRequest.EnableModule
- Microsoft.SharePoint.Library.SPRequest.EnableModuleFromXml
- Microsoft.SharePoint.Library.SPRequest.EnsureSystemAccount
- Microsoft.SharePoint.Library.SPRequest.EnsureUserExists
- Microsoft.SharePoint.Library.SPRequest.ExecSiteSearch
- Microsoft.SharePoint.Library.SPRequest.ExecuteBatchReorder
- Microsoft.SharePoint.Library.SPRequest.ExpandListSchemaForExport
- Microsoft.SharePoint.Library.SPRequest.ExportNavigationXml
- Microsoft.SharePoint.Library.SPRequest.ExtractFilesFromCabinet
- Microsoft.SharePoint.Library.SPRequest.FetchActiveFeaturesFromSessionCache
- Microsoft.SharePoint.Library.SPRequest.FIrmProtectorFor
- Microsoft.SharePoint.Library.SPRequest.ForceDeleteList
- Microsoft.SharePoint.Library.SPRequest.FormatDateAsString
- Microsoft.SharePoint.Library.SPRequest.GenerateChangeNumber
- Microsoft.SharePoint.Library.SPRequest.GetAcceptHeaderExtensionsAsStringList
- Microsoft.SharePoint.Library.SPRequest.GetAclForCurrentWeb
- Microsoft.SharePoint.Library.SPRequest.GetAclForScope
- Microsoft.SharePoint.Library.SPRequest.GetAdminRecycleBinItems
- Microsoft.SharePoint.Library.SPRequest.GetAdminRecycleBinItemsForUI
- Microsoft.SharePoint.Library.SPRequest.GetAdminRecycleBinStatistics
- Microsoft.SharePoint.Library.SPRequest.GetAllAclsForCurrentSite
- Microsoft.SharePoint.Library.SPRequest.GetAllAuthenticatedUsersString
- Microsoft.SharePoint.Library.SPRequest.GetAllRolesForCurrentUser
- Microsoft.SharePoint.Library.SPRequest.GetAllWebsOfSite
- Microsoft.SharePoint.Library.SPRequest.GetAttachmentsInfo
- Microsoft.SharePoint.Library.SPRequest.GetCachedNavigationData
- Microsoft.SharePoint.Library.SPRequest.GetColumnDistinctAsSafeArray

- Microsoft.SharePoint.Library.SPRequest.GetContainingList
- Microsoft.SharePoint.Library.SPRequest.GetContentTypeSchema
- Microsoft.SharePoint.Library.SPRequest.GetContentTypeWorkflowAssociationsAsSafeArray
- Microsoft.SharePoint.Library.SPRequest.GetContextEventReceivers
- Microsoft.SharePoint.Library.SPRequest.GetCurrentUserPermissionOnGroup
- Microsoft.SharePoint.Library.SPRequest.GetCustomizedDocumentsInWeb
- Microsoft.SharePoint.Library.SPRequest.GetDbNow
- Microsoft.SharePoint.Library.SPRequest.GetDeadWebInfo
- Microsoft.SharePoint.Library.SPRequest.GetDocEventReceivers
- Microsoft.SharePoint.Library.SPRequest.GetDocsHavingComments
- Microsoft.SharePoint.Library.SPRequest.GetEffectiveRightsForCurrentUser
- Microsoft.SharePoint.Library.SPRequest.GetEventReceivers
- Microsoft.SharePoint.Library.SPRequest.GetExecuteUrl
- Microsoft.SharePoint.Library.SPRequest.GetExpandedFolderNSPath
- Microsoft.SharePoint.Library.SPRequest.GetExternalSecurityProviderConfiguration
- Microsoft.SharePoint.Library.SPRequest.GetExternalSecurityProviderId
- Microsoft.SharePoint.Library.SPRequest.GetFieldsSchemaXml
- Microsoft.SharePoint.Library.SPRequest.GetFieldTypeInfo
- Microsoft.SharePoint.Library.SPRequest.GetFile
- Microsoft.SharePoint.Library.SPRequest.GetFileAndFolderProperties
- Microsoft.SharePoint.Library.SPRequest.GetFileAndFpMetaInfo
- Microsoft.SharePoint.Library.SPRequest.GetFileAndMetaInfo
- Microsoft.SharePoint.Library.SPRequest.GetFileAsByteArray
- Microsoft.SharePoint.Library.SPRequest.GetFileAsStream
- Microsoft.SharePoint.Library.SPRequest.GetFileUrlFromViewTitle
- Microsoft.SharePoint.Library.SPRequest.GetFileVersionAsByteArray
- Microsoft.SharePoint.Library.SPRequest.GetFileVersions
- Microsoft.SharePoint.Library.SPRequest.GetFirstUniqueAncestorWebUrl
- Microsoft.SharePoint.Library.SPRequest.GetFolderContentTypeId
- Microsoft.SharePoint.Library.SPRequest.GetFolderContentTypeOrder
- Microsoft.SharePoint.Library.SPRequest.GetGhostedFile
- Microsoft.SharePoint.Library.SPRequest.GetGlobalContentTypeXml
- Microsoft.SharePoint.Library.SPRequest.GetGroupsDataAsSafeArray
- Microsoft.SharePoint.Library.SPRequest.GetHash
- Microsoft.SharePoint.Library.SPRequest.GetHtmlTrCacheItemIfValid
- Microsoft.SharePoint.Library.SPRequest.GetHtmlTrUrlFromExt
- Microsoft.SharePoint.Library.SPRequest.GetIcon
- Microsoft.SharePoint.Library.SPRequest.GetIgnoreCanary

- Microsoft.SharePoint.Library.SPRequest.GetInfoFromCabinet
- Microsoft.SharePoint.Library.SPRequest.GetLanguageAttributes
- Microsoft.SharePoint.Library.SPRequest.GetLinkInfo
- Microsoft.SharePoint.Library.SPRequest.GetListAndChildrenNSInfo
- Microsoft.SharePoint.Library.SPRequest.GetListContentTypes
- Microsoft.SharePoint.Library.SPRequest.GetListCurrentFolderInfo
- Microsoft.SharePoint.Library.SPRequest.GetListItemDataAndRenderedViewWithCallback
- Microsoft.SharePoint.Library.SPRequest.GetListItemDataWithCallback
- Microsoft.SharePoint.Library.SPRequest.GetListItemPerm
- Microsoft.SharePoint.Library.SPRequest.GetListItemWorkflowAsSafeArrayAndLock
- Microsoft.SharePoint.Library.SPRequest.GetListItemWorkflowsAsSafeArray
- Microsoft.SharePoint.Library.SPRequest.GetListScopeDataAsSafeArray
- Microsoft.SharePoint.Library.SPRequest.GetListsWithCallback
- Microsoft.SharePoint.Library.SPRequest.GetListTemplates
- Microsoft.SharePoint.Library.SPRequest.GetListWorkflowAssociationsAsSafeArray
- Microsoft.SharePoint.Library.SPRequest.GetMetadataForUrl
- Microsoft.SharePoint.Library.SPRequest.GetMinFieldTypeInfo
- Microsoft.SharePoint.Library.SPRequest.GetModules
- Microsoft.SharePoint.Library.SPRequest.GetMtgInstanceID
- Microsoft.SharePoint.Library.SPRequest.GetMtgResponseCookie
- Microsoft.SharePoint.Library.SPRequest.GetNavigationNode
- Microsoft.SharePoint.Library.SPRequest.GetNavigationNodeChild
- Microsoft.SharePoint.Library.SPRequest.GetNavigationNodeProperties
- Microsoft.SharePoint.Library.SPRequest.GetNTFullNameandEmailfromLogin
- Microsoft.SharePoint.Library.SPRequest.GetNTFullNamefromLogin
- Microsoft.SharePoint.Library.SPRequest.GetNTFullNamefromLoginEx
- Microsoft.SharePoint.Library.SPRequest.GetPageListId
- Microsoft.SharePoint.Library.SPRequest.GetParentWebUrl
- Microsoft.SharePoint.Library.SPRequest.GetPermissionsDataAsSafeArray
- Microsoft.SharePoint.Library.SPRequest.GetPortalServerSettings
- Microsoft.SharePoint.Library.SPRequest.GetPortalSubscriptionUrl
- Microsoft.SharePoint.Library.SPRequest.GetPropertiesXmlForUncustomizedViews
- Microsoft.SharePoint.Library.SPRequest.GetRarelyUsedWebProps
- Microsoft.SharePoint.Library.SPRequest.GetRecycleBinItems
- Microsoft.SharePoint.Library.SPRequest.GetRecycleBinItemsForUI
- Microsoft.SharePoint.Library.SPRequest.GetRoleDefsDataAsSafeArray
- Microsoft.SharePoint.Library.SPRequest.GetRunnableWorkItemsAsSafeArray
- Microsoft.SharePoint.Library.SPRequest.GetSchemaXML

- Microsoft.SharePoint.Library.SPRequest.GetSecurityInfo
- Microsoft.SharePoint.Library.SPRequest.GetServerFileRedirect
- Microsoft.SharePoint.Library.SPRequest.GetSingleViewSchemaXml
- Microsoft.SharePoint.Library.SPRequest.GetSiteFlags
- Microsoft.SharePoint.Library.SPRequest.GetSiteItemSizes
- Microsoft.SharePoint.Library.SPRequest.GetSiteQuota
- Microsoft.SharePoint.Library.SPRequest.GetSiteUsageSummary
- Microsoft.SharePoint.Library.SPRequest.GetSizeOfWebPartsOnPage
- Microsoft.SharePoint.Library.SPRequest.GetStackTraceOnCreate
- Microsoft.SharePoint.Library.SPRequest.GetSTSVersion
- Microsoft.SharePoint.Library.SPRequest.GetSubscriptions
- Microsoft.SharePoint.Library.SPRequest.GetSubwebs
- Microsoft.SharePoint.Library.SPRequest.GetSubwebsFiltered
- Microsoft.SharePoint.Library.SPRequest.GetTimerRunningJobs
- Microsoft.SharePoint.Library.SPRequest.GetTimeZoneInfo
- Microsoft.SharePoint.Library.SPRequest.GetTimeZoneMoveParameters
- Microsoft.SharePoint.Library.SPRequest.GetTokenOfCurrentUser
- Microsoft.SharePoint.Library.SPRequest.GetUncustomizedDefaultView
- Microsoft.SharePoint.Library.SPRequest.GetUncustomizedViewByBaseViewId
- Microsoft.SharePoint.Library.SPRequest.GetUserAccountDirectoryPath
- Microsoft.SharePoint.Library.SPRequest.GetUserRegionalSettings
- Microsoft.SharePoint.Library.SPRequest.GetUsersDataAsSafeArray
- Microsoft.SharePoint.Library.SPRequest.GetUserStorageInfo
- Microsoft.SharePoint.Library.SPRequest.GetUserToken
- Microsoft.SharePoint.Library.SPRequest.GetVersionIndependentProp
- Microsoft.SharePoint.Library.SPRequest.GetVersionIndependentProps
- Microsoft.SharePoint.Library.SPRequest.GetViewsSchemaXml
- Microsoft.SharePoint.Library.SPRequest.GetViewStylesXML
- Microsoft.SharePoint.Library.SPRequest.GetWebAncestry
- Microsoft.SharePoint.Library.SPRequest.GetWebAndChildrenNSInfo
- Microsoft.SharePoint.Library.SPRequest.GetWebListPermMask
- Microsoft.SharePoint.Library.SPRequest.GetWebMetainfo
- Microsoft.SharePoint.Library.SPRequest.GetWebPartPagePersonalizations
- Microsoft.SharePoint.Library.SPRequest.GetWebSubscriptionsUniqueUsers
- Microsoft.SharePoint.Library.SPRequest.GetWebsWithTimestamps
- Microsoft.SharePoint.Library.SPRequest.GetWebTemplates
- Microsoft.SharePoint.Library.SPRequest.GetWebThemeComposite
- Microsoft.SharePoint.Library.SPRequest.GetWebUrl

- Microsoft.SharePoint.Library.SPRequest.GetWebUsageData
- Microsoft.SharePoint.Library.SPRequest.GetWorkflowAssociationAsSafeArray
- Microsoft.SharePoint.Library.SPRequest.GetWorkflowDataForItemAsSafeArrays
- Microsoft.SharePoint.Library.SPRequest.GetWorkItemAsSafeArray
- Microsoft.SharePoint.Library.SPRequest.GetWorkItemsAsSafeArray
- Microsoft.SharePoint.Library.SPRequest.GregorianISOToIntlISODate
- Microsoft.SharePoint.Library.SPRequest.HandleCookieOrAcceptTypes
- Microsoft.SharePoint.Library.SPRequest.ImportNavigationXml
- Microsoft.SharePoint.Library.SPRequest.InitHeap
- Microsoft.SharePoint.Library.SPRequest.InsertAlertEvent
- Microsoft.SharePoint.Library.SPRequest.InvalidateWebIdCache
- Microsoft.SharePoint.Library.SPRequest.InvokeTimerJob
- Microsoft.SharePoint.Library.SPRequest.IrmClientPresent
- Microsoft.SharePoint.Library.SPRequest.IrmClientReady
- Microsoft.SharePoint.Library.SPRequest.IsAttachment
- Microsoft.SharePoint.Library.SPRequest.IsCurrentUserMachineAdmin
- Microsoft.SharePoint.Library.SPRequest.IsCurrentUserMemberOfGroup
- Microsoft.SharePoint.Library.SPRequest.IsCurrentUserSiteAdmin
- Microsoft.SharePoint.Library.SPRequest.IsUrlSafeForRedirect
- Microsoft.SharePoint.Library.SPRequest.IsValidLoginName
- Microsoft.SharePoint.Library.SPRequest.IsVotingAllowed
- Microsoft.SharePoint.Library.SPRequest.ListRegionalOptions
- Microsoft.SharePoint.Library.SPRequest.LocalizeText
- Microsoft.SharePoint.Library.SPRequest.LocalizeXml
- Microsoft.SharePoint.Library.SPRequest.LogBinary
- Microsoft.SharePoint.Library.SPRequest.LogHelper
- Microsoft.SharePoint.Library.SPRequest.ManageAdminRecycleBin
- Microsoft.SharePoint.Library.SPRequest.ManageRecycleBin
- Microsoft.SharePoint.Library.SPRequest.MapUrlToListAndView
- Microsoft.SharePoint.Library.SPRequest.MigrateUserAccount
- Microsoft.SharePoint.Library.SPRequest.MiniSproc
- Microsoft.SharePoint.Library.SPRequest.ModifySubscription
- Microsoft.SharePoint.Library.SPRequest.MoveNavigationNode
- Microsoft.SharePoint.Library.SPRequest.MoveUrl
- Microsoft.SharePoint.Library.SPRequest.NavStructContainsPage
- Microsoft.SharePoint.Library.SPRequest.OpenSite
- Microsoft.SharePoint.Library.SPRequest.OpenWeb
- Microsoft.SharePoint.Library.SPRequest.OpenWebInternal

- Microsoft.SharePoint.Library.SPRequest.ParseMetaInfo
- Microsoft.SharePoint.Library.SPRequest.PatchUrl
- Microsoft.SharePoint.Library.SPRequest.PreInitServer
- Microsoft.SharePoint.Library.SPRequest.ProcessBatchData
- Microsoft.SharePoint.Library.SPRequest.PublishFile
- Microsoft.SharePoint.Library.SPRequest.PutFile
- Microsoft.SharePoint.Library.SPRequest.QueryGroups
- Microsoft.SharePoint.Library.SPRequest.QueryGroupsByIds
- Microsoft.SharePoint.Library.SPRequest.QueryUserInfo
- Microsoft.SharePoint.Library.SPRequest.ReadAuditFlags
- Microsoft.SharePoint.Library.SPRequest.ReadPagesRightsCheck
- Microsoft.SharePoint.Library.SPRequest.RecalculateSiteDiskUsed
- Microsoft.SharePoint.Library.SPRequest.ReCalculateWebFGP
- Microsoft.SharePoint.Library.SPRequest.RegisterContextEventReceiver
- Microsoft.SharePoint.Library.SPRequest.RegisterDocEventReceiver
- Microsoft.SharePoint.Library.SPRequest.RegisterEventReceiver
- Microsoft.SharePoint.Library.SPRequest.ReleaseResources
- Microsoft.SharePoint.Library.SPRequest.RelinkMeeting
- Microsoft.SharePoint.Library.SPRequest.RemoveExternalSecurityProvider
- Microsoft.SharePoint.Library.SPRequest.RemoveField
- Microsoft.SharePoint.Library.SPRequest.RemoveGroup
- Microsoft.SharePoint.Library.SPRequest.RemoveRoleDef
- Microsoft.SharePoint.Library.SPRequest.RemoveWorkflowFromListItem
- Microsoft.SharePoint.Library.SPRequest.RenameWeb
- Microsoft.SharePoint.Library.SPRequest.RenderColumn
- Microsoft.SharePoint.Library.SPRequest.RenderErrorPage
- Microsoft.SharePoint.Library.SPRequest.RenderFormAsHtml
- Microsoft.SharePoint.Library.SPRequest.RenderFormDigest
- Microsoft.SharePoint.Library.SPRequest.RenderListProperty
- Microsoft.SharePoint.Library.SPRequest.RenderListRelatedTasks
- Microsoft.SharePoint.Library.SPRequest.RenderNavigationBar
- Microsoft.SharePoint.Library.SPRequest.RenderSearchForm
- Microsoft.SharePoint.Library.SPRequest.RenderViewAsHtml
- Microsoft.SharePoint.Library.SPRequest.RepairOrphans
- Microsoft.SharePoint.Library.SPRequest.ReserveItemIdsForWorkflow
- Microsoft.SharePoint.Library.SPRequest.ResetSecurityScope
- Microsoft.SharePoint.Library.SPRequest.RestoreAdminRecycleBinItem
- Microsoft.SharePoint.Library.SPRequest.RestoreFileVersion

- Microsoft.SharePoint.Library.SPRequest.RestoreRecycleBinItem
- Microsoft.SharePoint.Library.SPRequest.RestoreSite
- Microsoft.SharePoint.Library.SPRequest.RevertContentStreams
- Microsoft.SharePoint.Library.SPRequest.RevertInProgressWorkItem
- Microsoft.SharePoint.Library.SPRequest.RevertInProgressWorkItems
- Microsoft.SharePoint.Library.SPRequest.SaveListAsTemplate
- Microsoft.SharePoint.Library.SPRequest.SaveWebAsTemplate
- Microsoft.SharePoint.Library.SPRequest.SealField
- Microsoft.SharePoint.Library.SPRequest.SeedEtag
- Microsoft.SharePoint.Library.SPRequest.SelectSitesAndUserInfoForMigration
- Microsoft.SharePoint.Library.SPRequest.SendMail
- Microsoft.SharePoint.Library.SPRequest.SetAnonymousAccessMask
- Microsoft.SharePoint.Library.SPRequest.SetAttendeeResponse
- Microsoft.SharePoint.Library.SPRequest.SetAuditFlags
- Microsoft.SharePoint.Library.SPRequest.SetDisableAsyncEvents
- Microsoft.SharePoint.Library.SPRequest.SetExactWebUrlFlag
- Microsoft.SharePoint.Library.SPRequest.SetGhostedFile
- Microsoft.SharePoint.Library.SPRequest.SetHtmlTrCacheItem
- Microsoft.SharePoint.Library.SPRequest.SetHttpParameters
- Microsoft.SharePoint.Library.SPRequest.SetIgnoreCanary
- Microsoft.SharePoint.Library.SPRequest.SetIgnoreCheckoutLock
- Microsoft.SharePoint.Library.SPRequest.SetIPAddr
- Microsoft.SharePoint.Library.SPRequest.SetListContentTypes
- Microsoft.SharePoint.Library.SPRequest.SetListProps
- Microsoft.SharePoint.Library.SPRequest.SetMondoProcHint
- Microsoft.SharePoint.Library.SPRequest.SetMtgInstanceID
- Microsoft.SharePoint.Library.SPRequest.SetPortalServerSettings
- Microsoft.SharePoint.Library.SPRequest.SetRequestAccessInfo
- Microsoft.SharePoint.Library.SPRequest.SetSiteFlags
- Microsoft.SharePoint.Library.SPRequest.SetSiteProps
- Microsoft.SharePoint.Library.SPRequest.SetSiteQuota
- Microsoft.SharePoint.Library.SPRequest.SetUserAccountDirectoryPath
- Microsoft.SharePoint.Library.SPRequest.SetVar
- Microsoft.SharePoint.Library.SPRequest.SetVersionIndependentProps
- Microsoft.SharePoint.Library.SPRequest.SetVersionIndependentPropsAdditive
- Microsoft.SharePoint.Library.SPRequest.SetWebAssociatedGroups
- Microsoft.SharePoint.Library.SPRequest.SetWebMetainfo
- Microsoft.SharePoint.Library.SPRequest.SetWebProps

- Microsoft.SharePoint.Library.SPRequest.SscCreateSite
- Microsoft.SharePoint.Library.SPRequest.TakePublishFileOffline
- Microsoft.SharePoint.Library.SPRequest.ThrowError
- Microsoft.SharePoint.Library.SPRequest.TZConvertDate
- Microsoft.SharePoint.Library.SPRequest.UncheckOutFile
- Microsoft.SharePoint.Library.SPRequest.UpdateField
- Microsoft.SharePoint.Library.SPRequest.UpdateFileOrFolderProperties
- Microsoft.SharePoint.Library.SPRequest.UpdateGroup
- Microsoft.SharePoint.Library.SPRequest.UpdateListItemWorkflow
- Microsoft.SharePoint.Library.SPRequest.UpdateListItemWorkflowLock
- Microsoft.SharePoint.Library.SPRequest.UpdateListSecurityTrim
- Microsoft.SharePoint.Library.SPRequest.UpdateMeeting
- Microsoft.SharePoint.Library.SPRequest.UpdateMeetingFromICal
- Microsoft.SharePoint.Library.SPRequest.UpdateMembers
- Microsoft.SharePoint.Library.SPRequest.UpdateNavigationNode
- Microsoft.SharePoint.Library.SPRequest.UpdateRoleAssignment
- Microsoft.SharePoint.Library.SPRequest.UpdateRoleDef
- Microsoft.SharePoint.Library.SPRequest.UpdateSiteHashKey
- Microsoft.SharePoint.Library.SPRequest.UpdateTimerRunningJobProgress
- Microsoft.SharePoint.Library.SPRequest.UpdateUser
- Microsoft.SharePoint.Library.SPRequest.UpdateView
- Microsoft.SharePoint.Library.SPRequest.UpdateWebPar
- Microsoft.SharePoint.Library.SPRequest.UpdateWebPartCache
- Microsoft.SharePoint.Library.SPRequest.UpdateWebPartIsIncluded
- Microsoft.SharePoint.Library.SPRequest.UpdateWebPartTypeId
- Microsoft.SharePoint.Library.SPRequest.UpdateWorkflowAssociation
- Microsoft.SharePoint.Library.SPRequest.UpdateWorkItem
- Microsoft.SharePoint.Library.SPRequest.UseDefaultAssociatedGroups
- Microsoft.SharePoint.Library.SPRequest.ValidateFormDigest
- Microsoft.SharePoint.Library.SPRequest.ValidateSubscriptionFilter
- Microsoft.SharePoint.Library.SPRequest.VssHelperIsEnabled
- Microsoft.SharePoint.Library.SPRequest.VssHelperOnIdentify
- Microsoft.SharePoint.Library.SPRequest.VssHelperOnPostRestore
- Microsoft.SharePoint.Library.SPRequest.VssHelperOnPreBackup
- Microsoft.SharePoint.Library.SPRequest.WebTemplateName

For SharePoint, Help Function for Site Name Retrieving

For System Center 2012 SP1 these resources are included:

- Microsoft.SharePoint.WebPartPages.SPWebPartManager.LoadWebParts

For SharePoint, KPI Helper

For System Center 2012 SP1 these resources are included:

- Microsoft.SharePoint.Portal.WebControls.KpiRenderer.getKpiData

For MVC

For System Center 2012 SP1 these resources are included:

- System.Web.Mvc.ReflectedActionDescriptor.Execute
- System.Web.Mvc.Async.ReflectedAsyncActionDescriptor.BeginExecute

For Windows Azure Storage Queue

For System Center 2012 SP1 these resources are included:

- Microsoft.WindowsAzure.StorageClient.CloudQueue.AddMessage
- Microsoft.WindowsAzure.StorageClient.CloudQueue.Clear
- Microsoft.WindowsAzure.StorageClient.CloudQueue.Create
- Microsoft.WindowsAzure.StorageClient.CloudQueue.CreateIfNotExist
- Microsoft.WindowsAzure.StorageClient.CloudQueue.Delete
- Microsoft.WindowsAzure.StorageClient.CloudQueue.UpdateMessage
- Microsoft.WindowsAzure.StorageClient.CloudQueue.DeleteMessage
- Microsoft.WindowsAzure.StorageClient.CloudQueue.Exists
- Microsoft.WindowsAzure.StorageClient.CloudQueue.GetMessagesInternal
- Microsoft.WindowsAzure.StorageClient.CloudQueue.PeekMessage
- Microsoft.WindowsAzure.StorageClient.CloudQueue.PeekMessages
- Microsoft.WindowsAzure.StorageClient.CloudQueue.FetchAttributes
- Microsoft.WindowsAzure.StorageClient.CloudQueue.SetMetadata

For Windows Azure Storage Table

For System Center 2012 SP1 these resources are included:

- Microsoft.WindowsAzure.StorageClient.CloudTableClient.CreateTablesFromModel
- Microsoft.WindowsAzure.StorageClient.CloudTableClient.CreateTable
- Microsoft.WindowsAzure.StorageClient.CloudTableClient.CreateTableIfNotExist
- Microsoft.WindowsAzure.StorageClient.CloudTableClient.DeleteTable
- Microsoft.WindowsAzure.StorageClient.CloudTableClient.DeleteTableIfExist
- Microsoft.WindowsAzure.StorageClient.CloudTableClient.DoesTableExist
- Microsoft.WindowsAzure.StorageClient.CloudTableClient.ListTablesSegmented

For Windows Azure Storage Blob Container

For System Center 2012 SP1 these resources are included:

- Microsoft.WindowsAzure.StorageClient.CloudBlobContainer.Create
- Microsoft.WindowsAzure.StorageClient.CloudBlobContainer.CreateIfNotExist
- Microsoft.WindowsAzure.StorageClient.CloudBlobContainer.Delete
- Microsoft.WindowsAzure.StorageClient.CloudBlobContainer.SetPermissions
- Microsoft.WindowsAzure.StorageClient.CloudBlobContainer.GetPermissions
- Microsoft.WindowsAzure.StorageClient.CloudBlobContainer.FetchAttributes
- Microsoft.WindowsAzure.StorageClient.CloudBlobContainer.SetMetadata
- Microsoft.WindowsAzure.StorageClient.CloudBlobContainer.ListBlobsSegmented
- Microsoft.WindowsAzure.StorageClient.CloudBlobDirectory.ListBlobsSegmented

For Windows Azure Storage Blobs

For System Center 2012 SP1 these resources are included:

- Microsoft.WindowsAzure.StorageClient.CloudBlob.CopyFromBlob
- Microsoft.WindowsAzure.StorageClient.CloudBlob.CreateSnapshot
- Microsoft.WindowsAzure.StorageClient.CloudBlob.Delete
- Microsoft.WindowsAzure.StorageClient.CloudBlob.DeleteIfExists
- Microsoft.WindowsAzure.StorageClient.CloudBlob.UploadText
- Microsoft.WindowsAzure.StorageClient.CloudBlob.DownloadText
- Microsoft.WindowsAzure.StorageClient.CloudBlob.UploadFile
- Microsoft.WindowsAzure.StorageClient.CloudBlob.DownloadToFile
- Microsoft.WindowsAzure.StorageClient.CloudBlob.UploadFromStream
- Microsoft.WindowsAzure.StorageClient.CloudBlob.DownloadToStream
- Microsoft.WindowsAzure.StorageClient.CloudBlob.SetProperties
- Microsoft.WindowsAzure.StorageClient.CloudBlob.GetSharedAccessSignature
- Microsoft.WindowsAzure.StorageClient.CloudBlockBlob.PutBlock
- Microsoft.WindowsAzure.StorageClient.CloudBlockBlob.PutBlockList
- Microsoft.WindowsAzure.StorageClient.CloudBlockBlob.DownloadBlockList
- Microsoft.WindowsAzure.StorageClient.CloudPageBlob.WritePages
- Microsoft.WindowsAzure.StorageClient.CloudPageBlob.Create
- Microsoft.WindowsAzure.StorageClient.CloudPageBlob.ClearPages
- Microsoft.WindowsAzure.StorageClient.CloudPageBlob.GetPageRanges

For Windows Azure Storage Blob Stream

For System Center 2012 SP1 these resources are included:

- Microsoft.WindowsAzure.StorageClient.BlobReadStream.Read

- Microsoft.WindowsAzure.StorageClient.BlobWriteStream.Write
- Microsoft.WindowsAzure.StorageClient.BlobWriteStream.Commit
- Microsoft.WindowsAzure.StorageClient.CloudBlobClient.ListBlobsWithPrefixSegmented
- Microsoft.WindowsAzure.StorageClient.CloudBlobClient.ListContainersSegmented
- Microsoft.WindowsAzure.StorageClient.Tasks.Task`1.ExecuteAndWait
- System.Data.Services.Client.DataServiceContext.SaveChanges
- System.Data.Services.Client.DataServiceContext.Execute
- System.Data.Services.Client.DataServiceContext.ExecuteBatch
- Microsoft.WindowsAzure.StorageClient.TableServiceContext.SaveChangesWithRetries

For COM+ Services (Client Side)

- System.EnterpriseServices.RemoteServicedComponentProxy.Invoke

For COM+ Services (Server Side)

- For System Center 2012 SP1 only: System.EnterpriseServices.ServicedComponentProxy.LocalInvoke

For SQL server

- For System Center 2012 SP1 only: System.Data.SqlClient.SqlConnection.Open
- For System Center 2012 SP1 only: System.Data.SqlClient.SqlConnection.Close
- System.Data.SqlClient.SqlCommand.ExecuteReader
- System.Data.SqlClient.SqlCommand.ExecuteNonQuery
- System.Data.SqlClient.SqlCommand.ExecuteScalar
- System.Data.SqlClient.SqlDataAdapter.Fill

For OLEDB

- For System Center 2012 SP1 only: System.Data.OleDb.OleDbConnection.Open
- For System Center 2012 SP1 only: System.Data.OleDb.OleDbConnection.Close
- System.Data.OleDb.OleDbCommand.ExecuteReader
- System.Data.OleDb.OleDbCommand.System.Data.OleDb.OleDbCommand.System.Data.IDbCommand.ExecuteReader
- System.Data.OleDb.OleDbCommand.ExecuteNonQuery
- System.Data.OleDb.OleDbCommand.ExecuteScalar
- System.Data.OleDb.OleDbDataAdapter.Fill

For ODBC

- For System Center 2012 SP1 only: System.Data.Odbc.OdbcConnection.Open

- For System Center 2012 SP1 only: System.Data.Odbc.OdbcConnection.Close
- System.Data.Odbc.OdbcCommand.ExecuteReader
- System.Data.Odbc.OdbcCommand.ExecuteNonQuery
- System.Data.Odbc.OdbcCommand.ExecuteScalar
- System.Data.Odbc.OdbcDataAdapter.Fill

For .NET Framework Data Provider for Oracle

- System.Data.OracleClient.OracleCommand.ExecuteNonQuery
- System.Data.OracleClient.OracleCommand.ExecuteReader
- System.Data.OracleClient.OracleCommand.ExecuteScalar
- System.Data.SqlClient.SqlConnection.Open
- System.Data.Odbc.OdbcConnection.Open
- System.Data.OleDb.OleDbConnection.Open

For Oracle

- For System Center 2012 SP1 only: System.Data.OracleClient.OracleConnection.Open
- For System Center 2012 SP1 only: System.Data.OracleClient.OracleConnection.Close
- Oracle.DataAccess.Client.OracleCommand.ExecuteReader
- Oracle.DataAccess.Client.OracleCommand.ExecuteNonQuery
- Oracle.DataAccess.Client.OracleCommand.ExecuteScalar
- System.Data.Common.DbAdapter.Fill

For System.Web.Mail

- System.Web.Mail.SmtpMail@CdoSysHelper.Send

For Instrumentation

- System.Web.UI.Page.ProcessRequest
- System.Web.UI.Page.ProcessRequest
- System.Web.Services.Protocols.SoapHttpClientProtocol.Invoke
- System.Web.Services.Protocols.SoapHttpClientProtocol.BeginInvoke
- System.Web.Services.Protocols.LogicalMethodInfo.Invoke

For Instrumentation (Framework 1.0)

- System.Web.Services.Protocols.SoapHttpClientProtocol.ReadResponse

For Instrumentation (Framework 1.1)

- System.Web.Services.Protocols.SoapHttpClientProtocol.ReadResponse

- System.Web.HttpServerUtility.ExecuteInternal
- System.Web.UI.LosFormatter.Deserialize

For Instrumentation (Framework 2.0)

- System.Web.HttpServerUtility.Execute

For File System Operations

- System.IO.Directory.GetFileSystemEntries
- System.IO.Directory.GetFiles
- System.IO.File.Open
- System.IO.FileStream..ctor
- System.IO.FileStream.ReadCore
- System.IO.FileStream.WriteCore
- System.IO.FileStream.BeginReadCore
- System.IO.BeginWriteCore
- System.IO.Directory.InternalCreateDirectory
- System.IO.Directory.Delete
- System.IO.Directory.InternalGetFileDirectoryNames
- System.IO.DirectoryInfo.MoveTo
- System.IO.Directory.Move
- System.IO.File.Delete
- System.IO.FileInfo.Delete
- System.IO.File.Move
- System.IO.FileInfo.MoveTo

For Remoting Client-Side

- System.Runtime.Remoting.Proxies.RemotingProxy.InternalInvoke
- System.Runtime.Remoting.Proxies.RealProxy.HandleReturnMessage
- System.Runtime.Remoting.Proxies.RealProxy.PrivateInvoke

For Remoting Server-Side

- System.Runtime.Remoting.Messaging.ServerObjectTerminatorSink.AsyncProcessMessage
- System.Runtime.Remoting.Messaging.ServerObjectTerminatorSink.SyncProcessMessage

For MS Message Queuing

- System.Messaging.MessageQueue.Send
- ystem.Messaging.MessageQueue.Receive

For Sockets

- System.NET.Sockets.Socket.Connect
- System.NET.Sockets.Socket.Receive
- System.NET.Sockets.Socket.Send
- System.NET.Sockets.Socket.Listen

For System.Web

- System.NET.FileWebRequest.GetResponse
- System.NET.FileWebRequest.GetRequestStream
- System.NET.HttpWebRequest.GetResponse
- System.NET.HttpWebRequest.GetRequestStream
- System.NET.FtpWebRequest.GetResponse
- System.NET.FtpWebRequest.GetRequestStream
- System.NET.WebClient.OpenRead

For Reflection

- System.Reflection.RuntimeConstructorInfo.Invoke
- System.RuntimeType.InvokeMember

For Registry

- Microsoft.Win32.RegistryKey.OpenSubKey

For Parsing

- System.Byte.Parse
- System.SByte.Parse
- System.Int16.Parse
- System.Int32.Parse
- System.Int64.Parse
- System.UInt16.Parse
- System.UInt32.Parse
- System.UInt64.Parse
- System.Single.Parse
- System.Double.Parse
- System.Boolean.Parse
- System.Char.Parse
- System.Decimal.Parse
- System.DateTime.Parse

- System.DateTime.ParseExact
- System.TimeSpan.Parse
- System.SqlBoolean.Parse
- System.SqlByte.Parse
- System.SqlDateTime.Parse
- System.SqlInt16.Parse
- System.SqlInt32.Parse
- System.SqlInt64.Parse
- System.SqlSingle.Parse
- System.SqlDouble.Parse
- System.SqlMoney.Parse

For IBM DB2

- IBM.Data.DB2.DB2Command.ExecuteReader
- IBM.Data.DB2.DB2Command.ExecuteReader
- IBM.Data.DB2.DB2Command.ExecuteNonQuery
- IBM.Data.DB2.DB2Command.ExecuteScalar

For Sybase

- Sybase.Data.AseClient.AseCommand.ExecuteScalarSybase.Data.AseClient.AseCommand.System.Data.IDbCommand.ExecuteReader
- Sybase.Data.AseClient.AseCommand.ExecuteNonQuery

Resource Calls Monitored by Default

Application Performance Monitoring includes well-known Microsoft .NET Framework resource calls that are monitored for slow performance.

For Custom Functions FW 1.0

- System.Data.Common.DbDataAdapter.FillFromReader

For Custom Functions FW 2.0

- System.Data.Common.DataAdapter.FillFromReader

For HTTP Handlers Calls .NET 1.1

- System.Web.Handlers.BatchHandler.System.Web.IHttpHandler.ProcessRequest
- System.Web.Handlers.TraceHandler.System.Web.IHttpHandler.ProcessRequest

- System.Web.HttpDebugHandler.ProcessRequest
- System.Web.HttpForbiddenHandler.ProcessRequest
- System.Web.HttpMethodNotAllowedHandler.ProcessRequest
- System.Web.HttpNotFoundHandler.ProcessRequest
- System.Web.HttpNotImplementedHandler.ProcessRequest
- System.Web.DefaultHttpHandler.ProcessRequest
- System.Web.SessionState.StateApplication.ProcessRequest
- System.Web.StaticFileHandler.ProcessRequest
- System.Web.UI.TrivialPage.ProcessRequest

For HTTP Handlers Calls .NET 2.0

- System.Web.Handlers.AssemblyResourceLoader.System.Web.IHttpHandler.ProcessRequest

For HTTP Modules Calls .NET 1.1

- System.Web.Caching.OutputCacheModule.OnEnter
- System.Web.Caching.OutputCacheModule.OnLeave
- System.Web.Security.DefaultAuthenticationModule.OnEnter
- System.Web.Security.FileAuthorizationModule.OnEnter
- System.Web.Security.FormsAuthenticationModule.OnAuthenticate
- System.Web.Security.PassportAuthenticationModule.OnAuthenticate
- System.Web.Security.UrlAuthorizationModule.OnEnter
- System.Web.Security.WindowsAuthenticationModule.OnAuthenticate
- System.Web.SessionState.SessionStateModule.BeginAcquireState

For HTTP Modules Calls .NET 2.0

- System.Web.Profile.ProfileModule.OnEnter
- System.Web.Profile.ProfileModule.OnLeave
- System.Web.Security.AnonymousIdentificationModule.OnEnter
- System.Web.Security.RoleManagerModule.OnEnter
- System.Web.UrlMappingsModule.OnEnter

For COM+ Server-Side

- System.EnterpriseServices.ServicedComponentProxy.LocalInvoke

For COM+ Client-Side

- System.EnterpriseServices.RemoteServicedComponentProxy.Invoke

For Remoting Client-Side

- System.Runtime.Remoting.Proxies.RemotingProxy.InternalInvoke

For Abstract Data Access Function

- System.Data.Common.DbDataAdapter.Update

For SQL Server Resources

- System.Data.SqlClient.SqlCommand.ExecuteReader
- System.Data.SqlClient.SqlCommand.ExecuteReader
- System.Data.SqlClient.SqlCommand.ExecuteXmlReader
- System.Data.SqlClient.SqlCommand.ExecuteNonQuery
- System.Data.SqlClient.SqlCommand.ExecuteScalar
- System.Data.SqlClient.SqlConnection.Open
- System.Data.SqlClient.SqlConnection.Close

For SQL Server Resources FW 2.0 Specific (Async Methods)

- System.Data.SqlClient.SqlCommand.BeginExecuteReader
- System.Data.SqlClient.SqlCommand.BeginExecuteNonQuery

For OLEDB Resources

- System.Data.OleDb.OleDbCommand.ExecuteReader
- System.Data.OleDb.OleDbCommand.ExecuteNonQuery
- System.Data.OleDb.OleDbCommand.ExecuteScalar
- System.Data.OleDb.OleDbConnection.Open
- System.Data.OleDb.OleDbConnection.Close

For ODBC Resources

- System.Data.Odbc.OdbcCommand.ExecuteReader
- System.Data.Odbc.OdbcCommand.ExecuteNonQuery
- System.Data.Odbc.OdbcCommand.ExecuteScalar
- System.Data.Odbc.OdbcConnection.Open
- System.Data.Odbc.OdbcConnection.Close

For Oracle Resources

- System.Data.OracleClient.OracleCommand.ExecuteReader
- System.Data.OracleClient.OracleCommand.ExecuteNonQuery
- System.Data.OracleClient.OracleCommand.ExecuteScalar

- System.Data.OracleClient.OracleConnection.Open
- System.Data.OracleClient.OracleConnection.Close
- Oracle.DataAccess.Client.OracleCommand.ExecuteReader
- Oracle.DataAccess.Client.OracleCommand.ExecuteNonQuery
- Oracle.DataAccess.Client.OracleCommand.ExecuteScalar
- Oracle.DataAccess.Client.OracleConnection.Open
- Oracle.DataAccess.Client.OracleConnection.Close

For IBM DB2 iSeries

- IBM.Data.DB2.iSeries.iDB2Command.ExecuteReader
- IBM.Data.DB2.iSeries.iDB2Command.ExecuteReader
- IBM.Data.DB2.iSeries.iDB2Command.ExecuteNonQuery
- IBM.Data.DB2.iSeries.iDB2Command.ExecuteScalar
- IBM.Data.DB2.iSeries.iDB2Connection.Open
- IBM.Data.DB2.iSeries.iDB2Connection.Close

For Web Services Resources

- System.Web.Services.Protocols.SoapHttpClientProtocol.Invoke
- System.Web.Services.Protocols.SoapHttpClientProtocol.BeginInvoke

For System.Messaging

- System.Messaging.MessageQueue.Send
- System.Messaging.MessageQueue.Receive

For System.IO

- System.IO.File.Open
- System.IO.Directory.GetFileSystemEntries
- System.IO.Directory.GetFiles

For System.Web.Mail

- System.Web.Mail.SmtpMail.Send

For IBM DB2

- IBM.Data.DB2.DB2Command.ExecuteReader
- IBM.Data.DB2.DB2Command.ExecuteReader
- IBM.Data.DB2.DB2Command.ExecuteNonQuery
- IBM.Data.DB2.DB2Command.ExecuteScalar

- IBM.Data.DB2.DB2Connection.Open
- IBM.Data.DB2.DB2Connection.Close

For WCF Client-Side

- System.ServiceModel.Channels.ServiceChannelProxy.InvokeService
- System.ServiceModel.Channels.ServiceChannelProxy.InvokeBeginService
- System.ServiceModel.Channels.ServiceChannelProxy.InvokeEndService

For Mail

- System.Web.Mail.SmtpMail@CdoSysHelper.Send

For RK Sybase Resources

- Sybase.Data.AseClient.AseCommand.ExecuteScalar
- Sybase.Data.AseClient.AseCommand.ExecuteNonQuery
- Sybase.Data.AseClient.AseCommand.System.Data.IDbCommand.ExecuteReader

For LINQ

- System.Data.Linq.SqlClient.SqlProvider.System.Data.Linq.Provider.IProvider.Execute
- System.Data.Linq.SqlClient.SqlProvider.BuildQuery
- System.Data.Linq.SqlClient.SqlProvider.BuildQuery

For WWF

- System.Workflow.ComponentModel.ActivityExecutorDelegateInfo`1@ActivityExecutorDelegateOperation.Run
- System.Workflow.ComponentModel.ActivityExecutor`1.Execute
- System.Workflow.ComponentModel.Activity.SetStatus
- System.Workflow.ComponentModel.ActivityExecutionContext.ExecuteActivity
- System.Workflow.ComponentModel.Activity.Invoke

For ADOMD

- Microsoft.AnalysisServices.AdomdClient.AdomdCommand.ExecuteCellSet
- Microsoft.AnalysisServices.AdomdClient.AdomdCommand.ExecuteReader
- Microsoft.AnalysisServices.AdomdClient.AdomdCommand.ExecuteNonQuery
- Microsoft.AnalysisServices.AdomdClient.AdomdCommand.Execute

For AJAX.NET

- System.Web.Script.Services.RestHandler.InvokeMethod

For WebClient

- System.Net.WebClient.UploadBits
- System.Net.WebClient.DownloadBits
- System.Web.HttpPostedFile.SaveAs

For WebClient FW 1.1

- System.Net.WebClient.UploadValues System.Net.WebClient.UploadBits
- System.Net.WebClient.UploadFile
- System.Net.WebClient.DownloadFile

OLE DB Data Source Template

OLE DB (Object Linking and Embedding Database) is a Microsoft technology for accessing a variety of data sources by using a common method to connect to different databases such as Microsoft SQL Server.

The **OLE DB Data Source** template lets you monitor the availability and performance of any database that can be accessed with OLE DB. One or more watcher nodes connect to the database to verify its availability and test its performance. The watcher nodes can test the connection to the database or measure the time taken to perform a particular query.

The database can reside on any computer whether it has an agent for Operations Manager installed or not, but it must be accessible from the watcher nodes. Each watcher node must have an Operations Manager agent installed.

Scenarios

Use the **OLE DB Data Source** template in scenarios where applications rely on a database. You can either define a single watcher node to ensure that the database is accessible and responds to requests, or you can define each application server as a watcher node. The monitors that the template creates attempt to connect to the database from each location at the defined interval, and verify that each watcher node can connect successfully. In addition to validating the health of the database itself, any network connections and other required features between the watcher node and the database are also validated. You can use any number of watcher nodes, but it is typically most useful to select a sample that represents different environment or network segments.

Monitoring Performed by OLE DB Data Source Template

Depending on your selections in the OLE DB Data Source Template wizard, the monitoring performed by the created monitors and rules can include any of the following settings.

Type	Description	Enabled?
Monitors	Success of the database connection or query	Enabled by default.
	Time to connect to database	Enabled if specified in wizard.
	Time to complete query	Enabled if specified in the wizard and the query is provided.
	Time to fetch results of query	Enabled if specified in the wizard and the query is provided.
Collection Rules	Collection of time to connect to the database	Enabled by default.
	Collection of time to complete the query	Always enabled if the query is provided.
	Collection of time to fetch results of query	Always enabled if the query is provided.

Viewing Monitoring Data

All data collected by the **OLE DB Data Source** template is available in the **OLE DB Data Source State** view located in the **Synthetic Transaction** folder. In this view, an object represents each of the watcher nodes. The state of each object represents the worst state of the set of database monitors that are running on that node. If one or more of the nodes is shown with an error while at least one other node is healthy, it could indicate a problem with that particular node accessing the database, a network issue. If all of the nodes are unhealthy, it could indicate a problem with the database itself.

You can view the state of the individual database monitors by opening the Operations Manager Health Explorer for each object. You can view performance data by opening the Performance view for each of these objects.

Wizard Options

When you run the **OLE DB Data Source** template, you have to provide values for options in the following tables. Each table represents a single page in the wizard.

General Properties

The following options are available on the **General Options** page of the wizard.

Option	Description
Name	The name used for the monitoring wizard. This name is displayed in the Operations console in the **OLE DB Data Source State** view.
Description	Optional description of the monitor.
Management Pack	Management pack to store the classes, monitors, and rules that the template created. For more information about management packs, see Selecting a Management Pack File.

Connection String

The following options are available on the **Connection String** page of the wizard.

Option	Description
Connection string	The connection string to connect to the database. A connection string contains the properties required to locate and connect to the database. It contains such information as the server that is hosting the database, the database name, and the type of authentication to perform. You can type a connection string or build a connection string in a dialog box by clicking **Build**. For more detailed information about connection strings, see Connection String Syntax.
Query to execute	Optional query after the connection to the database has been made. If no query is provided, the monitor only attempts to connect to the database.

Option	Description
Query time-out	If a query is provided, this option specifies the maximum number of seconds that the query can take before it times out. You must set the **Query Time-out** value.

Query Performance

The following options are available on the **Query Performance** page of the wizard.

Option	Description
Connection time in milliseconds	If selected, the values **Error Threshold** and **Warning Threshold** provide the number of milliseconds for the connection when the monitor enters that state and an alert is generated. If not selected, the connection time is not monitored.
Query time in milliseconds	If selected, the values **Error Threshold** and **Warning Threshold** define the number of milliseconds the query can run before the monitor enters that state and generates an alert. If not selected, the time to run the query is not monitored. If a query is not provided, this option is not available.
Fetch time in milliseconds	If selected, the values **Error Threshold** and **Warning Threshold** define the number of milliseconds to retrieve the results of the query before the monitor enters that state and generates an alert. If not selected, the time to retrieve the results of the query is not monitored. If a query is not provided, this option is not available.

Watcher Nodes

The following options are available on the **Watcher Nodes** page of the wizard.

Option	Description
Select one or more agent-managed computers	Specify one or more agent-managed

Option	Description
	computers to run the monitor. For more information, see Watcher Nodes.
Run this query every	The frequency to attempt the connection to the database and run the query, if specified.

Security Considerations

The **OLE DB Data Source** template creates two Run As profiles. The name for each of these profiles starts with the name that you provided in the template and is followed by “Simple Authentication Profile” and “Synthetic Transaction Profile”. If no Run As account is added to either of these profiles, the Default Action Account for each watcher node is used to connect the database and run the query. If the Default Action Account does not have access to the database that is being monitored, the connection fails. You can specify either integrated security or simple authentication by creating a Run As account and adding it to the appropriate Run As profile that the **OLE DB Data Source** template created.

When you run the **OLE DB Data Source** template, it creates two Run As profiles. The name for each starts with the **Name** that you provided when you ran the template. The **OLE DB Synthetic Transaction Profile** is used when you want to use integrated security for the database connection. The **OLE DB Simple Authentication Profile** is used when you want to use simple authentication for the database connection.

Integrated Security

Integrated security lets you connect to the database by using credentials stored in Active Directory Domain Services. To connect the watcher nodes to the database by using integrated security, create a Run As account with **Windows** as the **Account type** and the credentials for the appropriate user account. Then add this Run As profile to the **OLE DB Synthetic Transaction Profile**.

Simple Authentication

Simple authentication lets you connect to the database by using a simple name and password. For a SQL Server database, this simple authentication could be used for SQL Server authentication. To have the watcher nodes connect to the database by using simple authentication, create a Run As account with **Simple Authentication** as the **Account type** and the credentials for the appropriate user account. Then add this Run As profile to the **OLE DB Simple Authentication Profile**. When you specify the connection string for the template, select the **Use Simple Authentication RunAs Profile created for this OLE DB data source transaction** check box. This adds variables to the connection string for the user name and password that you specified in the Run As account.

Creating and Modifying OLE DB Data Source Templates

To run the OLE DB Data Source wizard

1. Start the Operations console with an account that has Author credentials in the management group.
2. Open the **Authoring** workspace.
3. In the **Authoring** navigation pane, right-click **Management Pack Templates**, and then select **Add Monitoring Wizard**.
4. On the **Select Monitoring Type** page, select **OLE DB Data Source**, and then click **Next**.
5. On the **General Properties** page, in the **Name** and **Description** boxes, type a name and an optional description.
6. Select a management pack in which to save the monitor, or click **New** to create a new management pack. For more information, see Selecting a Management Pack File.
7. Click **Next**.
8. In the **Connection string** box, type a connection string for the database, or click the **Build** button to be prompted for the required information.
9. If you want the monitor to run a query, select **Query to execute**, and then type a query.
10. If you want to set a time-out for the query, type the number of seconds in the **Query time-out** box.
11. Click **Test** to perform a test connection by using the connection string and query that you just provided.

    Note

    The test is performed on the workstation that you are using to run the template. If this workstation cannot access the database, this test fails. When the template is completed, the query is run from the watcher nodes that you specify.
12. Click **Next** when you have validated your connection string and query.
13. Select the measurements that you want to monitor and set an error and warning threshold for each. Click **Next**.
14. Select one or more Watcher Nodes to run the monitor.
15. Specify the frequency to run the monitor in the **Run this query** box. Click **Next**.
16. Review the summary of the monitor, and then click **Create**.
17. If a Run As account with credentials that have access to the database does not exist, create an appropriate Run As account in the **Administration** workspace. For more information, see How to Create a Run As Account.

    Note

    To create and modify a Run As account, you must have administrative

credentials for the management group.

18. If the database uses integrated security, add the Run As account to the **Synthetic Transaction Action Profile** for the template. If the database uses simple authentication, add the Run As account to the **Simple Authentication Profile** for the template.

    Note
    To create and modify a Run As profile, you must have administrative credentials for the management group.

To modify an existing OLE DB Data Source template

1. Open the Operations console with a user account that has Author credentials.
2. Open the **Authoring** workspace.
3. In the **Authoring** navigation pane, expand **Management Pack Templates**, and then select **OLE DB Data Source**.
4. In the **OLE DB Data Source** pane, locate the monitor to change.
5. Right-click the monitor, and then select **Properties**.
6. Enter the changes that you want, and then click **OK**.

Viewing OLE DB Data Source Monitors and Collected Data

To view all OLE DB Data Source monitors

1. Open the Operations console.
2. Open the **Monitoring** workspace.
3. In the **Monitoring** navigation pane, select **Synthetic Transaction**, and then click **OLE DB Data Source State**.

To view the state of each monitor

1. In the **OLE DB Data Source State** pane, right-click an object. Select **Open**, and then click **Health Explorer**.
2. Expand the **Availability** and **Performance** nodes to view the individual monitors.

To view the performance collected for a monitor

1. In the **OLE DB Data Source State** pane, right-click an object. Select **Open**, and then click **Performance**.
2. In the **Legend** pane, select the counters that you want to view.
3. Use options in the **Actions** pane to modify the Performance view.

See Also

Creating Management Pack Templates

Watcher Nodes

Process Monitoring Template

The *Process Monitoring* template lets you monitor whether a particular process is running on a computer. By using this template, you can implement two different basic scenarios: You might require the process to be running for a particular application and want to be warned if it is not running, or you might have to be alerted if you discover that an unwanted process is running. In addition to monitoring whether the application is running, you can collect performance data for the processor and memory usage of the process.

Scenarios

Use the **Process Monitoring** template in different scenarios where you have to monitor a running process on an agent-managed Windows-based computer. Your application can monitor the following processes.

Critical Process

A process that must be running at all times. Use the **Process Monitoring** template to ensure that this process is running on the computers where it is installed, and use the **Process Monitoring** template to measure its performance.

Unwanted Process

A process that should not be running. This process might be a known rogue process that can cause damage, or it might be a process that is automatically started when an error in the application occurs. The **Process Monitoring** template can monitor for this process and send an alert if it is found to be running.

Long Running Process

A process that runs for short periods at a time. If the process is running for an excessive length of time, it might indicate a problem. The **Process Monitoring** template can monitor for the length of time that this process runs and send an alert if the running time exceeds a particular duration.

Monitoring Performed by Process Monitoring Template

Depending on your selections in the Process Monitoring wizard, the monitoring performed by the created monitors and rules can include any of the following settings.

Type	Description	When Enabled
Monitors	Count of wanted processes running	Enabled if you select **Processes you want** on the **Process to Monitor** page and **Number of processes** on the **Running Processes** page.
	Time that a wanted process has been running	Enabled if you select **Processes you want** on the **Process to Monitor** page and **Duration** on the **Running Processes** page.
	Unwanted process running	Enabled if **Monitoring Scenario** is for unwanted processes.
	Processor utilization of process	Enabled if you select **Processes you want** on the **Process to Monitor** page, and you enable **CPU alert** on the **Performance Data** page.
	Memory usage of process	Enabled if you select **Processes you want** on the **Process to Monitor** page, and you enable **memory alert** on the **Performance Data** page.
Collection Rules	Collection of processor utilization of process	Enabled if you select **Processes you want** on the **Process to Monitor** page, and you enable **CPU alert** on the **Performance Data** page.
	Collection of memory usage of process.	Enabled if you select **Processes you want** on the **Process to Monitor** page, and you enable **memory alert** on

Type	Description	When Enabled
		the **Performance Data** page.

Viewing Monitoring Data

All data collected by the **Process Monitoring** template is available in the **Process State** view located in the **Windows Service and Process Monitoring** folder. In this view, an object is listed for each agent in the group that you selected. Even if an agent does not monitor a process, it is listed, and the monitor reflects the state for the process that is not running.

You can view the state of the individual process monitors by opening the Operations Manager Health Explorer for the process object. You can view performance data by opening the Performance view for the process object.

The same process objects that are listed in the **Process State** view are included in the Health Explorer for the computer that hosts the process. The health state of the process monitors rolls up to the health of the computer.

Wizard Options

When you run the **Process Monitoring** template, you have to provide values for the options in the following tables. Each table represents a single page in the wizard.

General Properties

The following options are available on the **General Options** page of the wizard.

Option	Description
Name	The name used for the process. This name is displayed in the Operations console for the wizard. It does not have to be the same name as the process.
Description	Optional description of the process.
Management Pack	Management pack to store the class and monitors that the template creates. If you create any additional monitors or rules that are using the service as a target class, they have to be stored in the same management pack. For more information about management packs, see Selecting a Management Pack File.

Process to Monitor

The following options are available on the **Process to Monitor** page of the wizard.

Option	Description
Monitoring Scenario	The kind of monitoring that is to be performed. Select **Monitor whether and how a process is running** to monitor for a wanted process and set the monitor to a critical state when the process is not running. Select **Monitor only whether a process is running** to monitor for an unwanted process and set the monitor to a critical state when the process is running.
Process name	The full name of the process. This is the name of the process as it appears in Task Manager. It should not include the path to the actual executable file. You can either type the name or click the ellipse (**…**) button to locate the file name.
Targeted group	The process is monitored on all computers that are included in the specified group.

Running Processes

The following options are available on the **Running Processes** page of the wizard.

Option	Description
Generate an alert of the number of processes is below the minimum value or above the maximum value for longer than the specified duration	If selected, the monitor is set to a critical state, and an alert is created if the number of instances of the specified process is less than the specified minimum or greater than the specified maximum for a longer period than the specified duration. To ensure that at least one instance of the process is running, set both the minimum and maximum to 1.
Minimum number of processes	The minimum number of processes that should be running.
Maximum number of processes	The maximum number of processes that should

Option	Description
	be running.
Duration	Specifies how long the number of running processes must exceed the specified range before the monitor is set to a critical state. Do not set this value to less than 1 minute.
Generate an alert if the process runs longer than the specified duration	If selected, the monitor is set to a critical state, and an alert is created if one instance of the process runs for longer than the specified duration.

Performance Data

The following options are available on the **Performance Data** page of the wizard.

Option	Description
Generate an alert if CPU usage exceeds the specified threshold	Specifies if CPU usage of the process should be monitored. A monitor will be created to set an error state on the object and generate an alert when the specified threshold is exceeded. A rule is created to collect CPU usage for analysis and reporting.
CPU Usage (percentage)	If CPU utilization is monitored, this option sets the threshold. If the percentage of total CPU usage exceeds the threshold, the object is set to an error state, and an alert is generated.
Generate an alert if memory usage exceeds the specified threshold	Specifies if memory usage of the process should be monitored. A monitor will be created to set an error state on the object, and generate an alert when the specified threshold is exceeded. A rule is created to collect CPU usage for analysis and reporting.
Memory Usage (MB)	If memory usage is monitored, this option sets the threshold. If the disk space in megabytes (MB) of total CPU usage exceeds the threshold, the object is set to an error state, and an alert is generated.
Number of samples	If CPU usage or memory is monitored, this

Option	Description
	option specifies the number of consecutive performance samples that must be exceeded before the object is set to an error state, and an alert is generated. Specifying a number greater than 1 for this option limits the noise from monitoring by ensuring that an alert is not generated when the service only briefly exceeds the threshold. The larger the value that you set, the longer the period of time before you are alerted to a problem. A typical value is 2 or 3.
Sampling interval	If CPU usage or memory is monitored, specify the length of time between performance samples. A smaller value for this option reduces the time for detecting a problem but increases overhead on the agent and the amount of data collected for reporting. A typical value is between 5 and 15 minutes.

Additional Monitoring

In addition to performing the specified monitoring, the **Process Monitoring** template creates a targetd class that you can use for additional monitors and workflows. Any monitor or rule using this class as a target will run on any agent-managed computer in the group specified in the template. If it creates Windows events that indicate an error, for example, you could create a monitor or rule that detects the particular event and uses the process' class as a target.

Creating and Modifying Process Monitor Templates

To run the Process Monitoring wizard

1. Determine the target group for the monitor by using the following logic:
   - If you want to discover the process on all Windows-based computers in the management group, you do not have to create a group. You can use the existing group **All Windows Computers**.
   - If you only want the process to be discovered on a certain group of computers, either

ensure that an appropriate group exists or create a new group by using the procedure in **How to Create Groups in Operations Manager 2012**.

- If the process that you are monitoring is in a cluster, create a group with objects of the class **Virtual Server** representing the nodes of the cluster that contain the service.

2. Start the Add Monitoring wizard.
3. On the **Select Monitoring Type** page, select **Process Monitoring**, and then click **Next**.
4. On the **General Properties** page, in the **Name** and **Description** boxes, type a name and an optional description. The name is used to describe the process in the Operations console. It is not the actual name of the process.
5. Select a management pack in which to save the monitor, or click **New** to create a new management pack. For more information, see Selecting a Management Pack File.
6. Click **Next**.
7. On the **Process to Monitor** page, do the following:
   a. Select whether you want to monitor a **wanted** or an **unwanted** process.
   b. In the **Process name** box, type the complete name of the process to monitor. For example, **notepad.exe**. You can also click the ellipse **(…)** button and locate the executable file.
   c. Click the ellipse **(…)** button to the right of the **Targeted Group** box, and then select the group from the first step of this procedure.
   d. Click **Next**.
8. If you selected the option for a **wanted** process, on the **Running Processes** page, do the following:
   a. If you want to monitor whether the process is running, do the following:
      i. Select the option to **Generate an alert of the number of processes is below the minimum value or above the maximum value for longer than the specified duration**.
      ii. In the **Minimum number of processes** box, enter the minimum number of processes that should be running. For a single instance of the process, this is typically 1.
      iii. In the **Maximum number of processes** box, enter the maximum number of instances of the process that should be running.
      iv. In the **Duration** box, enter the length of time that running processes must exceed the specified range before the monitor is set to a critical state. This value should not be set to less than 1 minute. Note that the process could stop and restart within this time window with no error detected.
   b. If you want to monitor for the length that a process runs, do the following:
      i. Select the option to **Generate an alert if the process runs longer than the specified duration**.
      ii. In the **Duration** box, enter the maximum length of time that you want the process to run before the monitor is set to a critical state. This value should not be set to less than 1 minute.

9. If you selected the option for a wanted process, on the **Performance Data** page, select the performance counters and thresholds that you want to monitor. For more detailed information, see the Wizard Options section.

   Note
   This page is disabled if you selected the option for an **unwanted** process.
10. If you have selected performance counters, specify the monitoring interval.
11. Click **Next**.
12. Review the summary of the monitor, and then click **Create**.

To modify an existing Process Monitoring template

1. Open the Operations console with a user account that has Author credentials.
2. Open the **Authoring** workspace.
3. In the **Authoring** navigation pane, expand **Management Pack Templates**, and then click **Process Monitoring**.
4. In the **Process Monitoring** pane, locate the monitor to change.
5. Right-click the monitor, and then select **Properties**.
6. Enter the changes that you want, and then click **OK**.

Viewing Process Monitoring Monitors and Collected Data

To view all Process Monitoring monitors

1. Open the Operations console.
2. Open the **Monitoring** workspace.
3. In the **Monitoring** navigation pane, select **Windows Service and Process Monitoring**, and then click **Process State**.

To view the state of each monitor

1. In the **Process State** pane, right-click an object. Select **Open**, and then click **Health Explorer**.
2. Expand the **Availability** and **Performance** nodes to view the individual monitors.

To view the performance collected for a process

1. In the **Process State** pane, right-click an object. Select **Open**, and then click **Performance**.
2. In the **Legend** pane, select the counters that you want to view.
3. Use options in the **Actions** pane to modify the Performance view.

See Also

Creating Management Pack Templates

Watcher Nodes

TCP Port Template

The **TCP Port** template lets you monitor the availability of an application that is accessible over TCP.

The application that is being tested can reside on any computer whether an agent for Operations Manager installed or not. Each watcher node must have an Operations Manager agent installed.

Scenarios

Use the **TCP Port** template in scenarios where applications rely on a service accessible over TCP. You can define each client as a watcher node. The monitors created by the template attempt to connect to the application from each client at the defined interval. The monitors verify that each client can connect successfully. In addition to validating the availability of the application itself, any network connections and other required features between the watcher node and the application are also validated.

Monitoring Performed by the TCP Port Template

The monitoring performed by the monitors and rules created by the TCP Port template can include any of the following settings.

Type	Description	Enabled?
Monitors	Target host reachable	Enabled
	Connection accepted	Enabled
	Connection timeout	Enabled
	DNS resolution	Enabled
Collection Rules	Connection time	Enabled

Viewing Monitoring Data

All data collected by the **TCP Port** template is available in the **TCP Port Checks State** view located in the **Synthetic Transaction** folder. In this view, an object represents each of the watcher nodes. The state of each object represents the worst state of the set of TCP Port

monitors running on that node. If one or more of the nodes is shown with an error while at least one other node is healthy, it could indicate a problem with that particular node accessing the specified computer, for example, a network issue. If all of the nodes are unhealthy, it could indicate a problem with the application itself, either the computer being offline or the application not responding on the specified port.

You can view the state of the individual TCP Port monitors by opening the Operations Manager Health Explorer for each object. You can view performance data by opening the Performance view for each of these objects.

Wizard Options

When you run the **TCP Port** template, you have to provide values for options in the following tables. Each table represents a single page in the wizard.

General Options

The following options are available on the **General Options** page of the wizard.

Option	Description
Name	The name used for the template. This name is displayed in the Operations console.
Description	Optional description of the service.
Management Pack	Management pack to store the class and monitors that the template created. If you create any additional monitors or rules by using the service as a target class, you must store them in the same management pack. For more information about management packs, see Selecting a Management Pack File.

Target and Port

The following options are available on the **Target and Port** page of the wizard.

Option	Description
Computer or device name	The name of the computer or device to connect to. This can be a name or an IP address. It must be resolved by and accessible to each watcher node that you specify.

Option	Description
Port	The number of the port on which the application is listening.

Watcher Nodes

The following options are available on the **Watcher Nodes** page of the wizard.

Option	Description
Select one or more agent managed computers	Specify one or more computers to run the monitors and rules. For more information, see Watcher Nodes.
Run this query every	The frequency to attempt the connection to the specified computer and port.

Creating and Modifying TCP Port Templates

To run the TCP Port data source wizard

1. Start the Operations console with an account that has Author credentials in the management group.
2. Open the **Authoring** workspace.
3. In the **Authoring** navigation pane, right-click **Management Pack Templates**, and then select **Add Monitoring Wizard**.
4. On the **Select Monitoring Type** page, select **TCP Port**, and then click **Next**.
5. On the **General Properties** page, in the **Name** and **Description** boxes, type a name and an optional description.
6. Select a management pack in which to save the monitor, or click **New** to create a new management pack. For more information, see Selecting a Management Pack File.
7. Click **Next**.
8. In the **Computer or device name** box, type the name or IP address of the computer or device to connect to.
9. In the **Port** box, type the port number on which the application is listening.
10. Click **Test** to perform a test connection by using the connection string and query that you just provided.

    Note
    The test is performed on the workstation that you are using to run the template. If

this workstation cannot access the computer or device, this test fails. When the template is completed, the test is run from the watcher nodes that you specify.

11. Click **Next** when you have validated your connection.
12. Select one or more Watcher Nodes to run the monitor.
13. Specify the frequency to run the monitor in the **Run this query** box. Click **Next**.
14. Review the summary of the monitor, and then click **Create**.

To modify an existing TPC Port template

1. Open the Operations console with a user account that has Author credentials.
2. Open the **Authoring** workspace.
3. In the **Authoring** navigation pane, expand **Management Pack Templates**, and then select **TCP Port**.
4. In the **TCP Port** pane, locate the template to change.
5. Right-click the monitor, and then select **Properties**.
6. Enter the changes that you want, and then click **OK**.

Viewing TCP Port Monitors and Collected Data

To view all TCP Port monitors

1. Open the Operations console.
2. Open the **Monitoring** workspace.
3. In the **Monitoring** navigation pane, select **Synthetic Transaction**, and then click **TCP Port Checks State**.

To view the state of each monitor

1. In the **TCP Port Checks State** pane, right-click an object. Select **Open**, and then click **Health Explorer**.
2. Expand the **Availability** and **Performance** nodes to view the individual monitors.

To view the performance collected for a monitor

1. In the **TCP Port Checks State** pane, right-click an object. Select **Open**, and then click **Performance**.
2. In the **Legend** pane, select the counters you want to view.
3. Use options in the **Actions** pane to modify the Performance view.

See Also

Creating Management Pack Templates

UNIX or Linux Log File

The **UNIX/Linux Log File Monitoring** template lets you create an alert when a particular text is detected in a log file.

Scenarios

Use the **UNIX/Linux Log File Monitoring** template for any application that writes to a log file when a particular error occurs. You provide the path to the log file and the text that indicates an error, and an alert is created for you anytime that text is detected.

Monitoring Performed by the UNIX/Linux Log File Monitoring Template

The following table shows the monitoring activity that the **UNIX/Linux Log FileMonitoring** template performs.

Type	Description	When Enabled
Rule	Creates an alert when a specified text is detected.	Enabled

Wizard Options

When you run the **UNIX/Linux Log File Monitoring** template, you have to provide values for the options in the following tables. Each table represents a single page in the wizard.

General Options

The following options are available on the **General Options** page of the wizard.

Option	Description
Name	The name used for the template. This name is displayed in the Operations console.
Description	Optional description of the template.
Management Pack	Management pack file to store the rule that the template creates.

Option	Description
	For more information about management packs, see Selecting a Management Pack File.

Log File Details

The following options are available on the **Log File Details** page of the wizard.

Option	Description
Computer	If you want to monitor a single computer, enter the name of the agent-managed UNIX or Linux computer with the log file to monitor. Click the **Select a Computer** button to select one of the agent-managed UNIX or Linux computers that are installed in your management group.
Computer group name	If you are going to monitor a group of computers, enter the name of the group of agent-managed UNIX or Linux computers with the log file to monitor. Click the **Computer Group** button to select from the group in your management group.
Log file path	Complete path and name of the log file.
Expression	Regular expression of the text to detect. If you want to detect a simple string of characters, type the string of characters.

Creating and Modifying UNIX/Linux Log File Templates

To create a UNIX/Linux Log File template

1. If you want to monitor the log file on a group of computers, determine the target group for the monitor by using the following logic:
   - If you want to monitor the log file on all UNIX and Linux computers in the management group, you do not have to create a group. You can use the existing group **UNIX/Linux Computer Group**.

- If you only want the log file to be monitored on a certain group of computers, either ensure that an appropriate group exists or create a new computer group by using the procedure in **How to Create Groups in Operations Manager** .

2. Start the **Add Monitoring** wizard.
3. On the **Select Monitoring Type** page, select **UNIX/Linux Log File Monitoring**, and then click **Next**.
4. On the **General Properties** page, in the **Name** and **Description** boxes, type a name and description for this new template.
5. Select a management pack in which to save the template or click **New** to create a new management pack. For more information, see Selecting a Management Pack File.
6. If you want to monitor the log file on a single computer, do the following:
   a. Click the **Select a Computer** button next to the **Computer name** box.
   b. Select the computer to monitor, and then click **OK**.
7. If you want to monitor the log file on a group of computers, do the following:
   a. Click the **Select a Group** button next to the **Computer group name** box.
   b. Select the computer to monitor, and then click **OK**.
8. In the **Log file path** box, type the path and name of the log file to monitor.
9. In the **Expression** box, type the text to watch for, such as **error**. You can type a regular expression for more complex logic.
10. Optionally, click **Test** to open a new dialog to test Regular expression matching against sample text that you input.
11. Select a **Run As Profile** to use. The account associated with the target computer in this profile will be used to read the log file.
12. Select an **Alert Severity**.
13. Click **Next**.
14. Verify the summary information for the template, and then click **Create**.

To modify an existing UNIX/Linux Log File template

1. Open the Operations console with a user account that has Author credentials.
2. Open the **Authoring** workspace.
3. In the **Authoring** navigation pane, expand **Management Pack Templates**, and then select **UNIX/Linux Log File**.
4. In the **UNIX/Linux Log File Monitoring** pane, locate the template to change.
5. Right-click the template, and then select **Properties**.
6. Enter the changes that you want, and then click **OK**.

Viewing UNIX/Linux Log File Data

There is no monitor or collected data for the **UNIX/Linux Log File Monitoring** template. If a match is found in the specified log file, an alert is generated. You can view this alert in the **Active Alerts** view with the other alerts.

See Also

Creating Management Pack Templates

Watcher Nodes

UNIX or Linux Process

The *UNIX/Linux Process Monitoring* template lets you monitor that a particular process installed on an UNIX or Linux computer runs.

Scenarios

The **UNIX/Linux Process Monitoring** template is useful for monitoring any application as monitoring processes is typically critical to the health of the application.

Monitoring Performed by the UNIX/Linux Process Monitoring Template

The following table shows the monitoring activity that the **UNIX/Linux Process Monitoring** template performs.

Type	Description	When Enabled
Monitors	Process Count is Outside of Range	Always enabled.

Wizard Options

When you run the **UNIX/Linux Process Monitoring** template, you have to provide values for options in the following tables. Each table represents a single page in the wizard.

General Options

The following options are available on the **General Options** page of the wizard.

Option	Description
Name	The name used for the template. This is the name that is displayed in the Operations console.
Description	Optional description of the template.

Option	Description
Management Pack	Management pack to store the class and monitors that the template creates. If you create any additional monitors or rules that are using the process as a targeted process, you must store them in the same management pack. For more information about management packs, see Selecting a Management Pack File.

Process Monitoring Details

The following options are available on the **Process Monitoring Details** page of the wizard.

Option	Description
Process name	The name of the process. You can use the **Select a Process** button to connect to a monitored UNIX/Linux computer and list current running processes in order to select a process by name. If you wish to target the monitor to only a single computer, you must use the **Select a Process** button to select a computer and process.
Computer Group	The name of the group of UNIX or Linux computers for the process to monitor. Click the **Select a group** button to select a group that is installed in your management group. If you have used the **Select a Process** button to select a running process from a computer, the monitor will be targeted to that computer. After using the **Select a Process** button to select a process, you can use the **Select a Group** button to target a group with the monitor for the selected process.
Alert Severity	The severity for the alert: Error, Warning, or Information.
Regular Expression to filter process arguments	An optional Regular expression to use in filtering processes by arguments. If this option is used, processes that match the provided

Option	Description
	process name will be additionally filtered by their arguments. Only processes with arguments that match the Regular expression will be evaluated by the monitor. This is useful to identify a process for a specific application when other applications on the system may use a process with the same name. The Regular expression is evaluated against a concatenated list of process arguments.
Expression Matching Results	If you use the **Select a Process** button to connect to a monitored computer and select a process by name, the list of all processes with the selected process name for that computer are shown in this field. When you provide a **Regular expression to filter process arguments** the processes listed in this field are filtered so that you can preview the filtering by argument.

Process Template Settings

The following options are available on the **Process Template Settings** page of the wizard.

Option	Description
Minimum number of instances	The minimum number of running instances of the monitored process. To alert if no instances of the process are running, check the box **Generate an alert when the number of process instances is less than the specified value**, and input a value of 1. The number of process instances is calculated after filtering by process name and the optional Regular expression to filter process arguments. If the number of running instances is less than the provided value, an alert will be generated.
Maximum number of instances	The maximum number of running instances of the monitored process. To alert if more than a specific number of instances of the process are running, check the box **Generate an alert**

Option	Description
	when the number of process instances is greater than the specified value, and input the maximum threshold value. The number of process instances is calculated after filtering by process name and the optional Regular expression to filter process arguments. If the number of running instances is greater than the provided value, an alert will be generated.

Additional Monitoring

In addition to performing the specified monitoring, the **UNIX/Linux Process Monitoring** template creates a target class that you can use for additional monitors and rules. Any monitor or rule that uses this class as a target runs on any agent where the process is installed.

Creating and Modifying UNIX/Linux Process Monitoring Templates

To create a UNIX/Linux Process Monitoring template

1. If you want to monitor a process on a group of computers, determine the targeted group for the monitor by using the following logic:
   - If you want to discover the process on all UNIX and Linux computers in the management group, you do not have to create a group. You can use the existing group **UNIX/Linux Computer Group**.
   - If you only want the process to be discovered on a certain group of computers, then either ensure that an appropriate group exists or create a one by using the procedure in **How to Create Groups in Operations Manager 2012**.
2. Start the **Add Monitoring** wizard.
3. On the **Select Monitoring Type** page, select **UNIX/Linux Process Monitoring**, and then click **Next**.
4. On the **General Properties** page, in the **Name** and **Description** boxes, type a name and optional description for this new template.
5. Select a management pack in which to save the monitor or click **New** to create a new management pack. For more information, see Selecting a Management Pack File.
6. Click **Next**.

7. Click the **Select a Process** button.
8. Click the **Browse** button and select a computer that has the process installed, and then click **OK**.
9. In the **Processes** box, select the process to monitor.
10. Select an **Alert Severity**.
11. Optionally, provide a Regular expression to filter the matched process list by process arguments, in the field **Regular expression to filter process arguments**.
12. If you want to monitor the process on a group of computers, do the following:
    a. Click the **Select a Group** button.
    b. Select a group that contains the computers with the process, and then click **OK**.
13. Click **Next**.
14. Check the appropriate boxes for **Generate an alert when the number of process instances is less than the specified value** and **Generate an alert when the number of process instances is greater than the specified value**.
15. Provide values for **Minimum number of instances** and **Maximum number of instances**, if appropriate.
16. Click **Next**.
17. Click **Create**.

To modify an existing UNIX/Linux Process Monitoring template

1. Open the Operations console with a user account that has Author credentials.
2. Open the **Authoring** workspace.
3. In the **Authoring** navigation pane, expand **Management Pack Templates**, and then select **UNIX/Linux Process Monitoring**.
4. In the **UNIX/Linux Process Monitoring** pane, locate the template to change.
5. Right-click the template, and then select **Properties**.
6. Enter the changes that you want, and then click **OK**.

Viewing UNIX/Linux Process Monitors and Collected Data

To view the state of each monitor

1. Select the **UNIX/Linux Computers** view.
2. In the **UNIX/Linux Computers** pane, right-click an object, select **Open**, and then click **Health Explorer**.
3. Expand the **Availability** node, and then click the **Application/Service Availability Rollup** node to view the individual process monitor.

See Also

Creating Management Pack Templates

Web Application Availability Monitoring Template

The **Web Application Availability Monitoring** template lets you create availability monitoring tests for one or more web application URLs and run these monitoring tests from internal locations. In addition to state and alert views, you can display the status of these tests in a provided map dashboard and a details dashboard.

Scenarios

Use the **Web Application Availability Monitoring** template in scenarios where you have to monitor web-based applications from different locations to see if they are working according to certain requirements, which you can specify.

Internal Locations

You might have web applications that must be available at all times at internal locations. Use the **Web Application Availability Monitoring** template to see which web applications are available from which internal locations.

Monitoring Performed by the Web Application Availability Monitoring Template

By default, the **Web Application Availability Monitoring** template configures the following monitoring by default. You can modify the monitor in the **Change Configuration** page of the **Web Application Availability Monitoring** template.

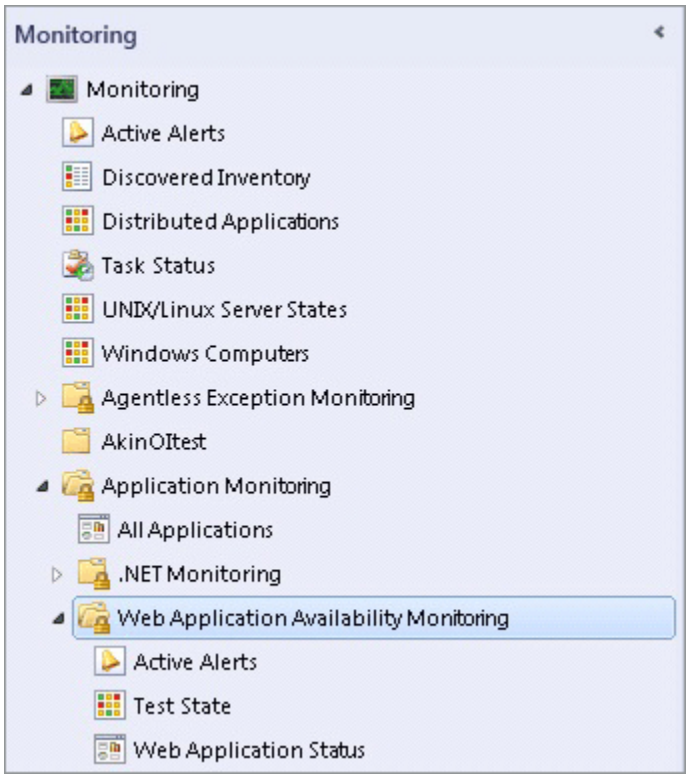
Monitor description	Default values
Web Application Monitor	• The monitor is enabled by default. • Test Frequency: 10 minutes • Performance data collection interval: 1 every 10 minutes • Test time-out: 45 seconds • HTTP status code: 400 (An alert will be generated if the HTTP status code is 400 or greater.)

Monitor description	Default values
	• Number of consecutive times a criteria should fail before an alert is generated: 1 • Generate alerts from each test: enabled • Allow redirects: enabled • HTTP version: HTTP/1.1 • HTTP method: GET • HTTP headers: accept “/” • HTTP headers: accept language of your product • HTTP headers: accept encoding GZIP
Performance Data Collection	• Transaction response time: enabled • Response time: enabled • TCP connect time: enabled • Time to first byte: enabled • Time to last byte: enabled • DNS resolution time: enabled • Content size: enabled • Content time: enabled • Download time: enabled

Viewing Monitoring Data

All data collected by the **Web Application Availability Monitoring** template appears in the **Web Application Availability Monitoring** folder in the **Application Monitoring** folder in the **Monitoring** navigation pane. The **Application Availability Monitoring** folder contains the default views and subfolders that provide Test State, Web Application Status, and alerts related to the tests being monitored. By using the Test State view, you can see the test state of the individual tests. The state of each object matches the state of the targeted object that has the worst health state so that you see the worst state of the monitors that are running. If one or more of the tests are shown with an error while at least one other test is healthy, it could indicate a problem for that particular test location. If all of the components are unhealthy, it could indicate a problem with the web application itself.

Web Application Availability Monitoring folder

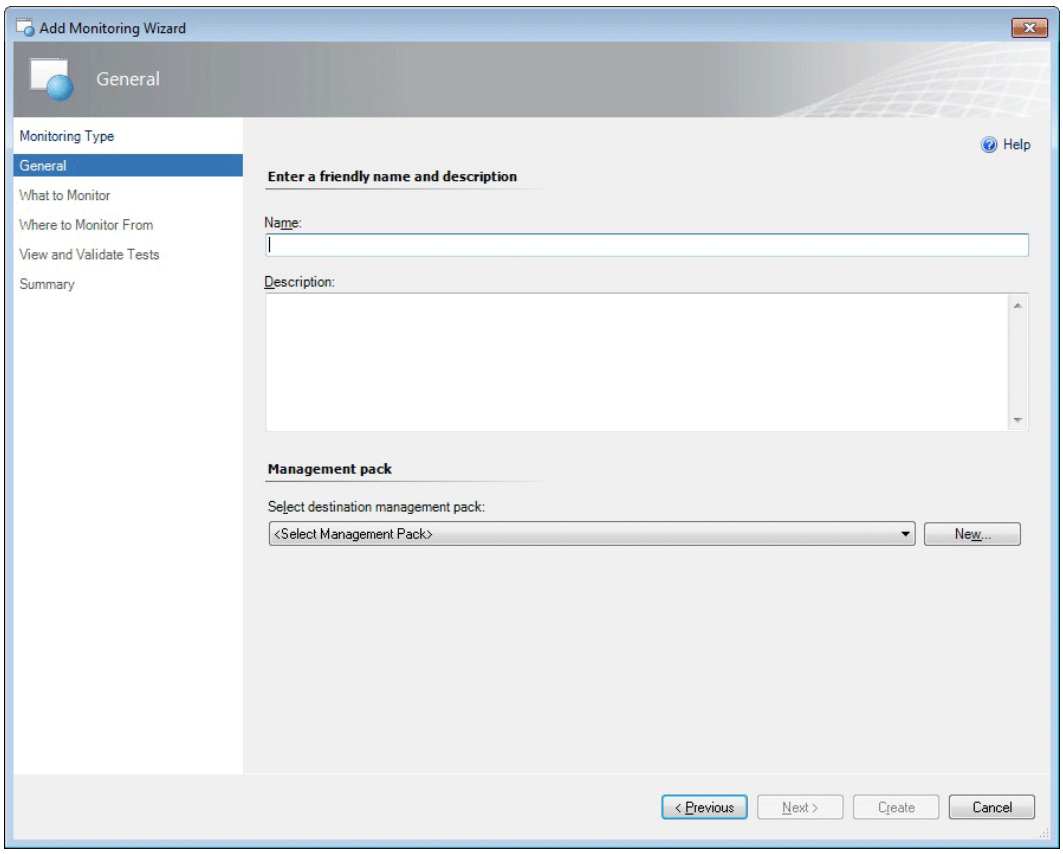


To view the state of the individual monitors, open the Health Explorer for each test.

Wizard Options

When you run the **Web Application Availability Monitoring** template, you have to provide values for options as listed in the following tables. Each table represents a single page in the wizard.

General

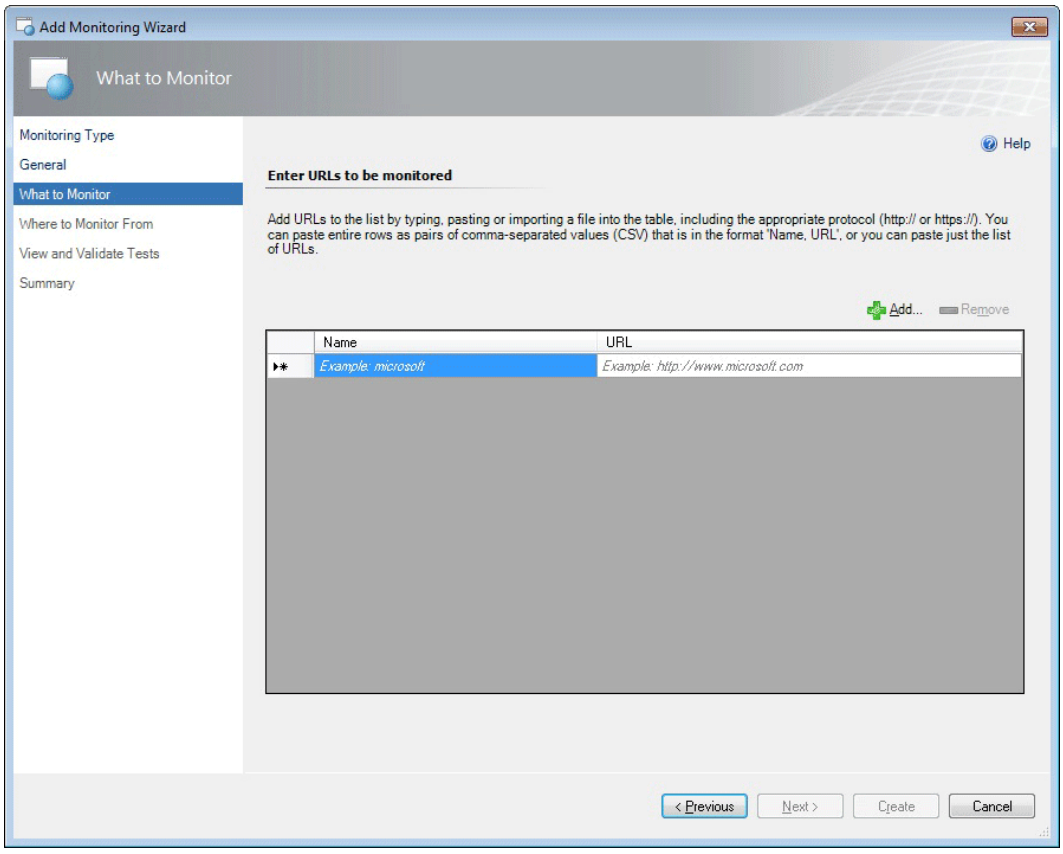


The following options are available on the **General** page of the wizard.

Option	Description
Name	Enter the friendly name used for the template and test group that you are creating. This name is displayed in the Operations Console in the Web Application status view and is used for the folder under the **Web Application Availability Monitoring** folder. **Note** After you have given the template a name and saved the template, this name cannot be edited without deleting and re-creating the template.
Description	Describe the template. (Optional)
Select destination management pack	Select the management pack to store the views

Option	Description
	and configuration created by the template. Use the same name for your new management pack as the test group so you can easily pair the two names. You can use an existing management pack or create a new management pack. For more information about management packs, see Selecting a Management Pack File.

What to Monitor

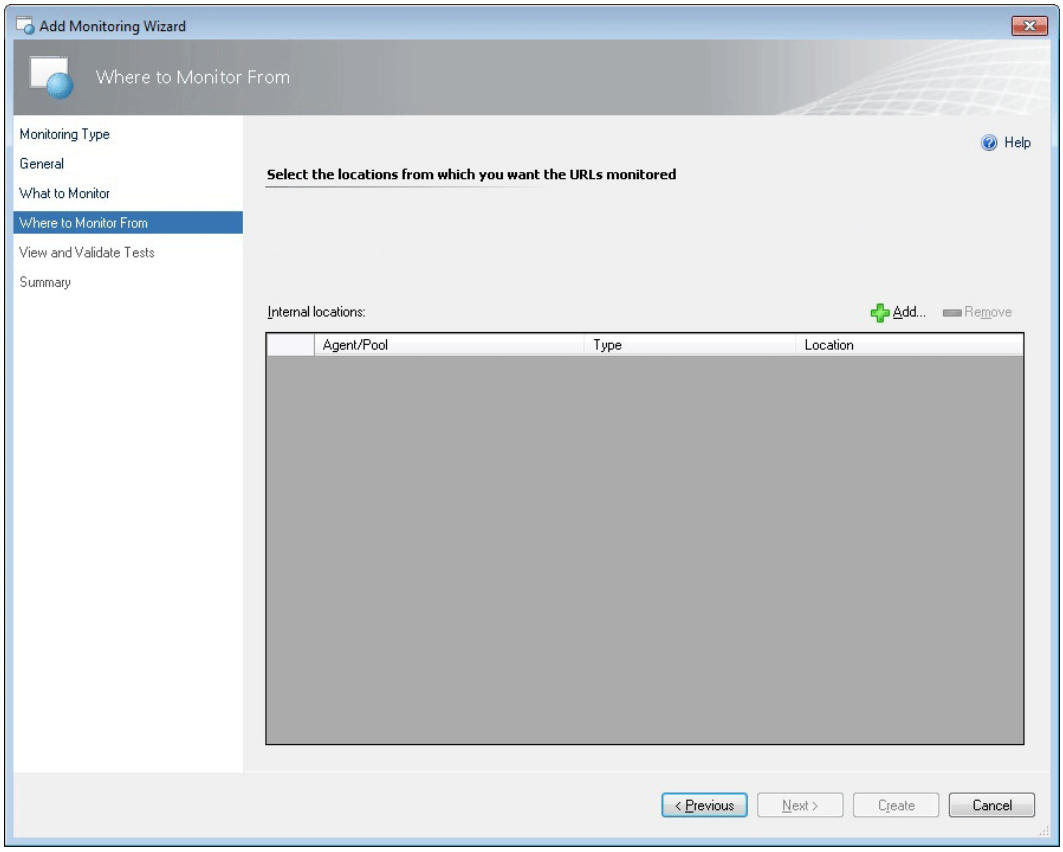


Add URLs to the list by typing, pasting, or importing a file into the table, including the appropriate protocol (http:// or https://). You can paste entire rows as pairs of comma-separated values (CSV) that are in the format 'Name, URL', or you can paste just the list of URLs.

The following options are available on the **What to Monitor** page of the wizard.

Option	Description
Name	Name of the website you want to monitor.
URL	URL of the website you want to monitor in the format: http://www.website.com
Add	Add URLs to monitor from an external file. You can paste a list of URLs or rows of a spreadsheet as pairs of comma-separated values that are in the format: Name, URL

Where to Monitor From



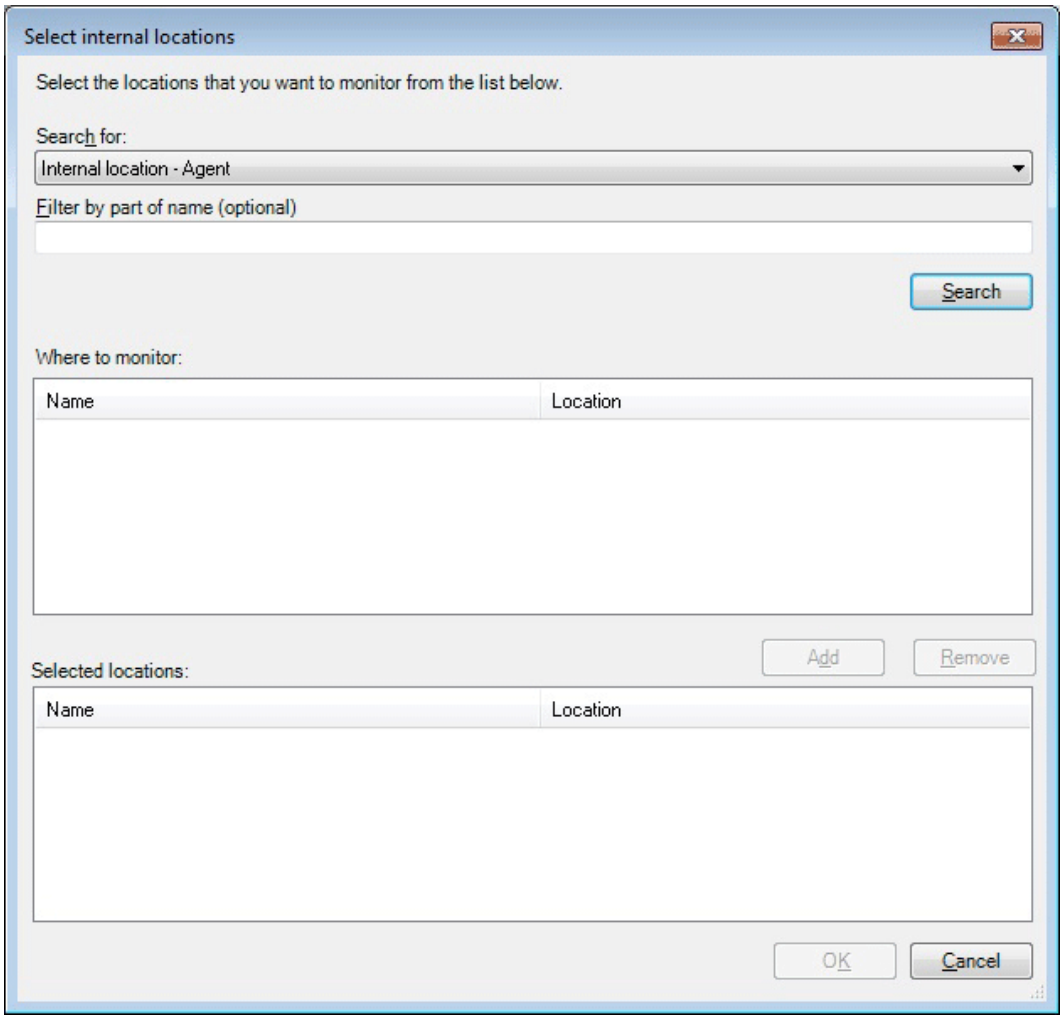
Select the internal locations from which you want the URLs to be monitored.

The following options are available on the **Where to Monitor From** page of the wizard.

Option	Description
Internal locations	The internal locations you are configuring to

Option	Description
	monitor from.
Add/Remove	Add or remove internal locations you want to monitor from.

Select Internal Locations

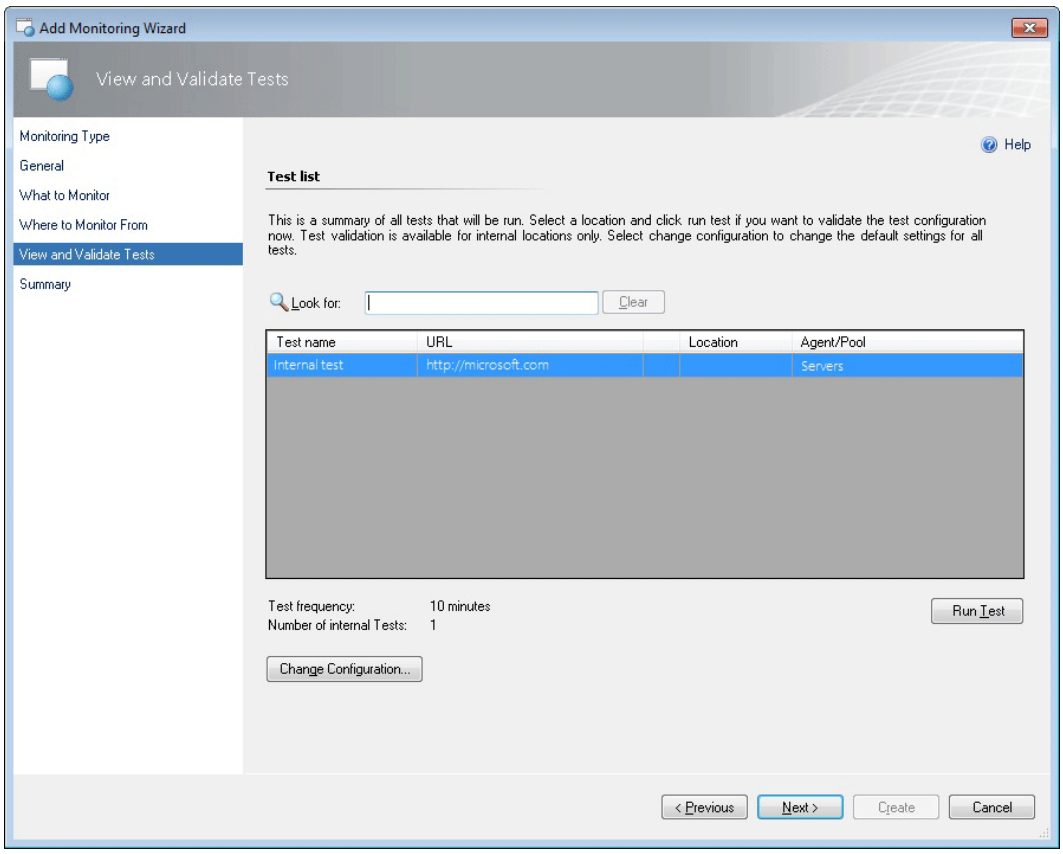


Select the internal locations from which you want to monitor the URLs you specified on the **What to Monitor** page. Click Add to add internal locations and then search for and select the internal locations that you want to monitor from.

The following options are available on the **Select internal locations** page of the wizard.

Option	Description
Search for	Option showing the kind of locations you search will look for. You can choose agents or pools.
Filter by part of name	Filter your search of internal locations.
Search	Search for locations that are available to monitor from. Available locations are displayed in the in the Location area.
Where to monitor: Name	List of the internal locations from which you can select to monitor from.
Where to monitor: Location	
Add	Add the internal locations you have selected to the Selected locations area. These are the locations you are configuring the wizard to monitor from.
Selected locations: Name	These are the internal locations you have chosen to monitor from.
Selected locations: Location	List of the locations you have chosen to monitor from.

View and Validate Tests



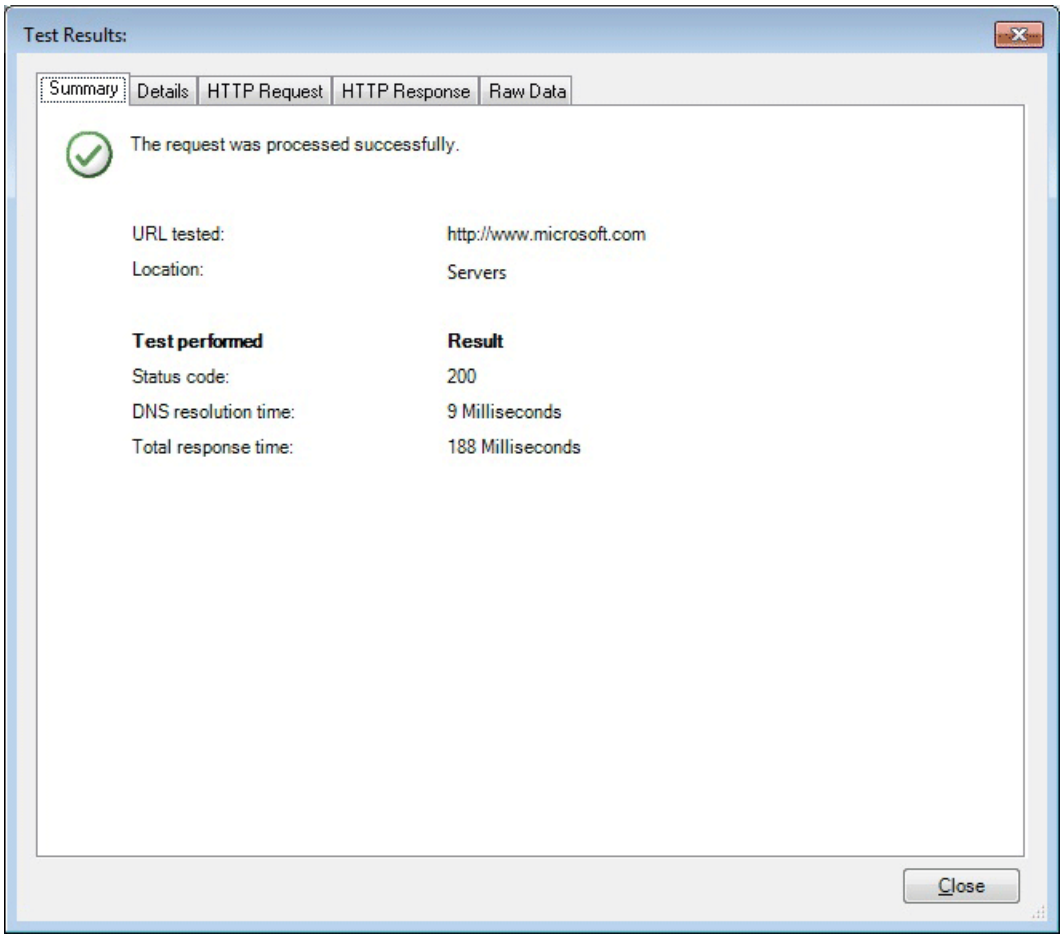
This is a summary of all tests that will be run. Select an internal location and click **Run Test** to validate the test configuration. Select Change configuration to change the default settings for all tests in this template.

The following options are available on the **View and Validate Tests** page of the wizard.

Option	Description
Look for	Search for and returns results for items in the list of test names, URLs, Locations, and Agent/Pools. Use this to find specific tests or sets of tests that you want to validate.
Test Name	Name of a test.
URL	URL for a specific test.
Agent/Pool	The Agent or Pool location for your internal URL tests.
Run Test	Run a validation test for internal tests that are

Option	Description
	selected.
Change Configuration	Open the **Change Configuration** page where you can change the settings for all tests in the template you are authoring.

Test Results: Summary Tab

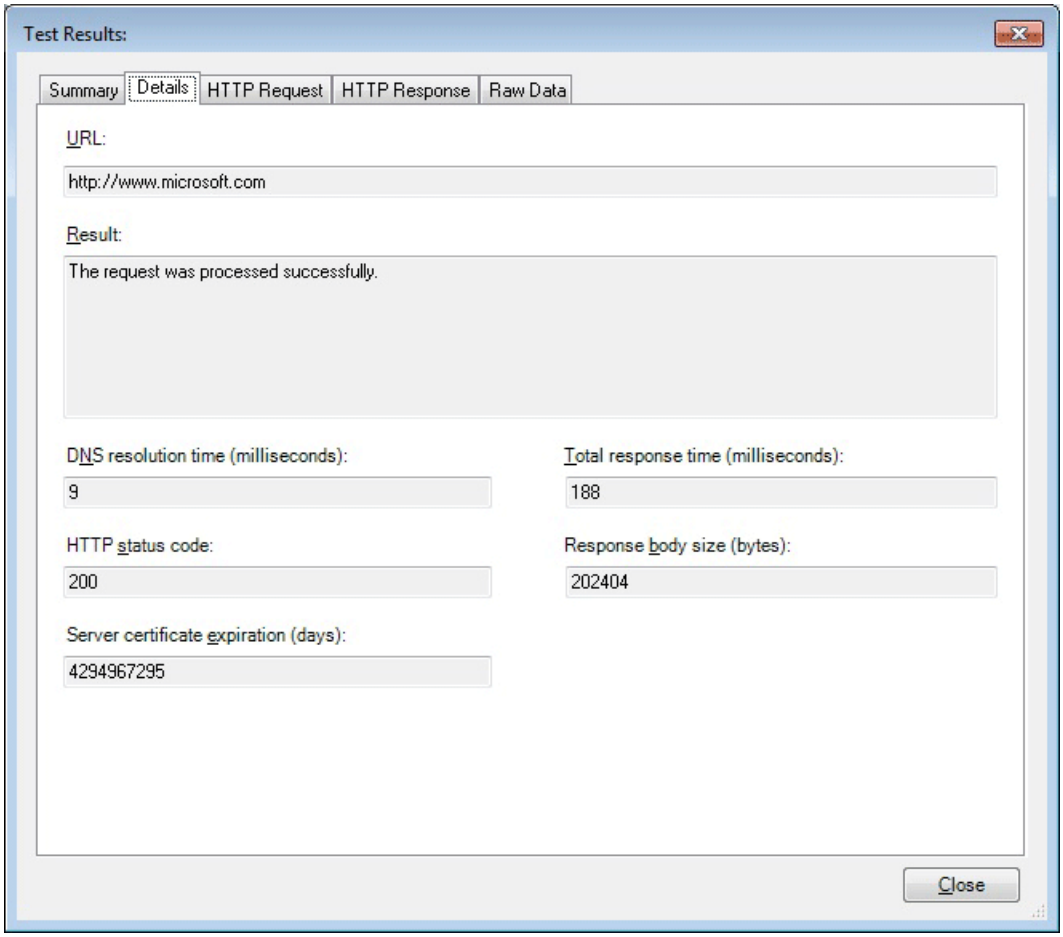


The following options are available on the **Test Results Summary** tab of the wizard.

Option	Description
Summary tab	Confirms if the test request was correctly processed and shows the URL and Location used in the test. Additionally. The specific tests and results are shown: Status code, DNS

Option	Description
	resolution time, and Total response time.

Test Results: Details Tab

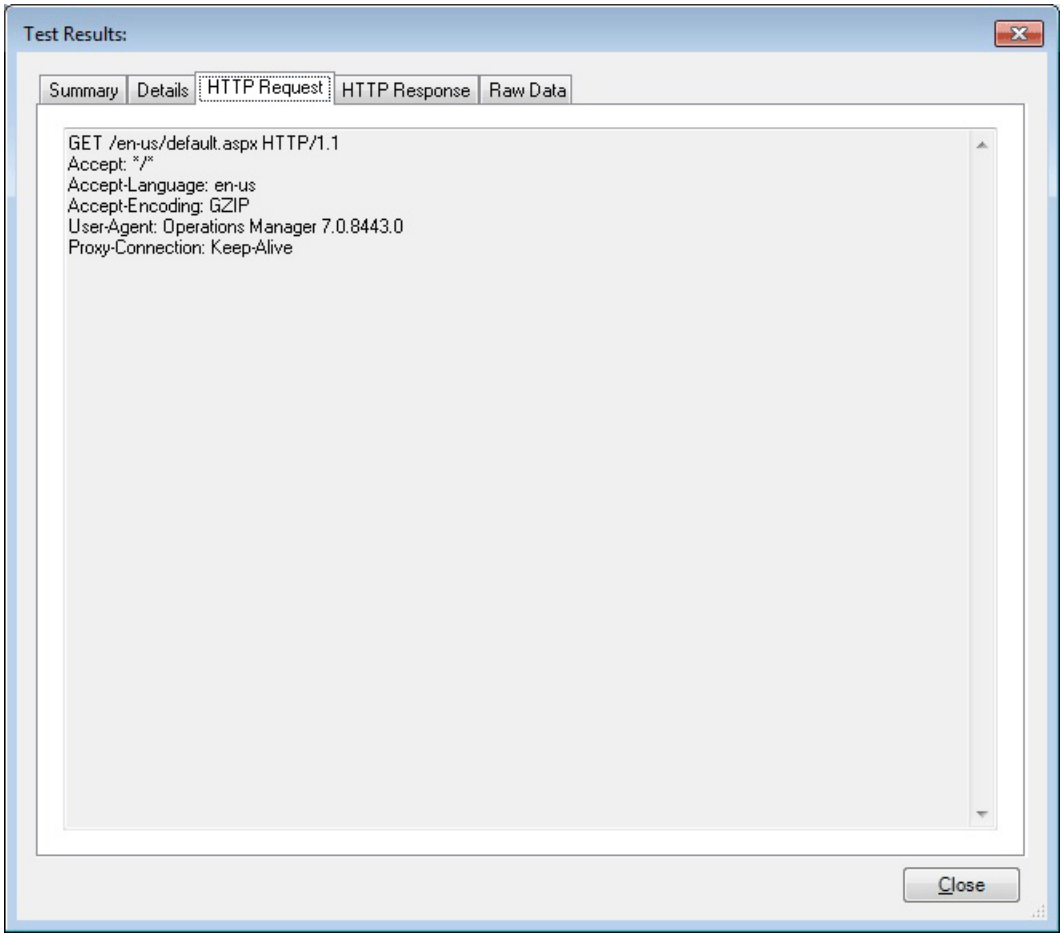


The following options are available on the **Test Results Details** tab of the wizard.

Option	Description
Details tab: URL	See detailed information about the test. Displays which URL was tested.
Details tab: Result	Displays whether the test request was processed successfully or not.
Details tab: DNS resolution time (milliseconds)	Displays the DNS resolution time which checks that website performs as you expected it to. What's the IP address of the URL you are.

Option	Description
	Time it takes for DNS to get the IP address for the website.
Details tab: Total response time (milliseconds)	Displays the Total response time from same as transaction time performance counter.
Details tab: HTTP status code	Displays the HTTP status code when you ping a website, you get a status code.
Details tab: Response body size (bytes)	Displays the Response body size of the HTTP response information.
Details tab: Server certificate expiration (days)	Displays the certificate expiration of the date when the site expired. Website can have expired certificates.

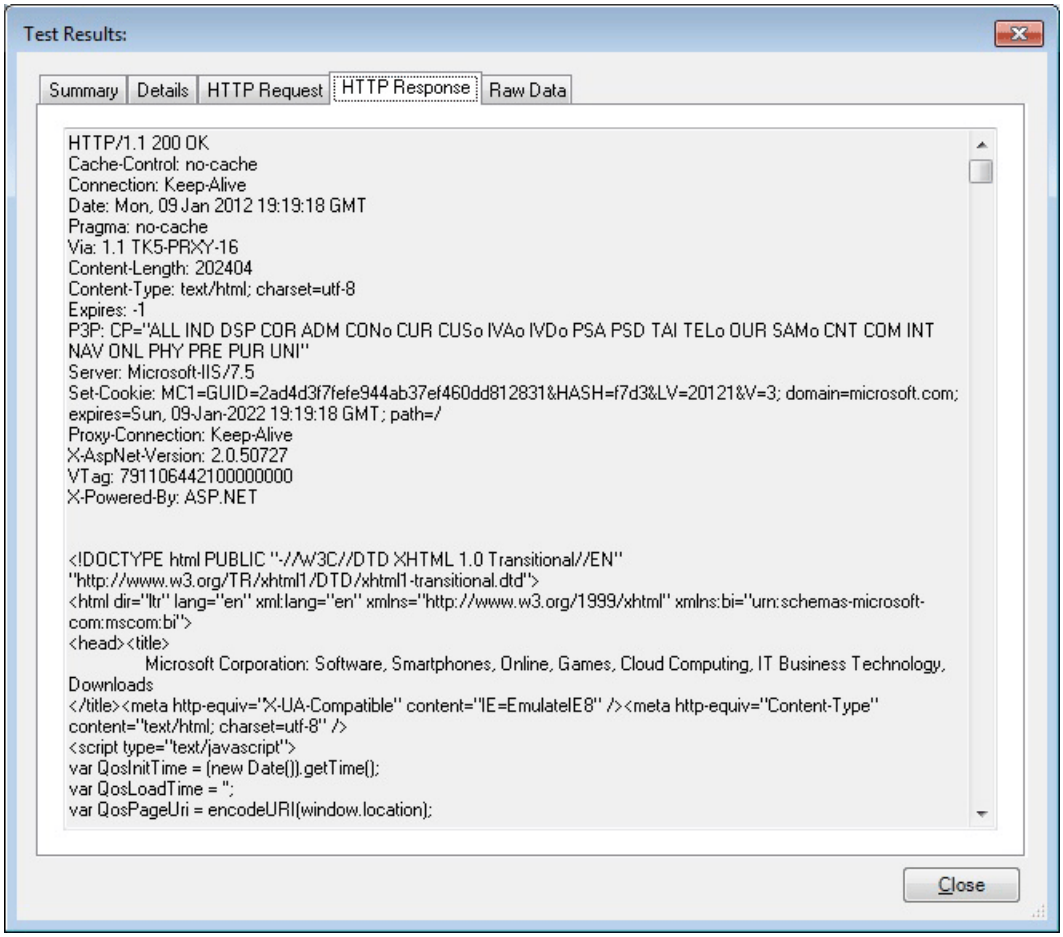
Test Results: HTTP Request Tab



The following options are available on the **Test Results HTTP Request** tab of the wizard.

Option	Description
HTTP Request tab	Displays details about the HTTP request of the test what is sent to the website.

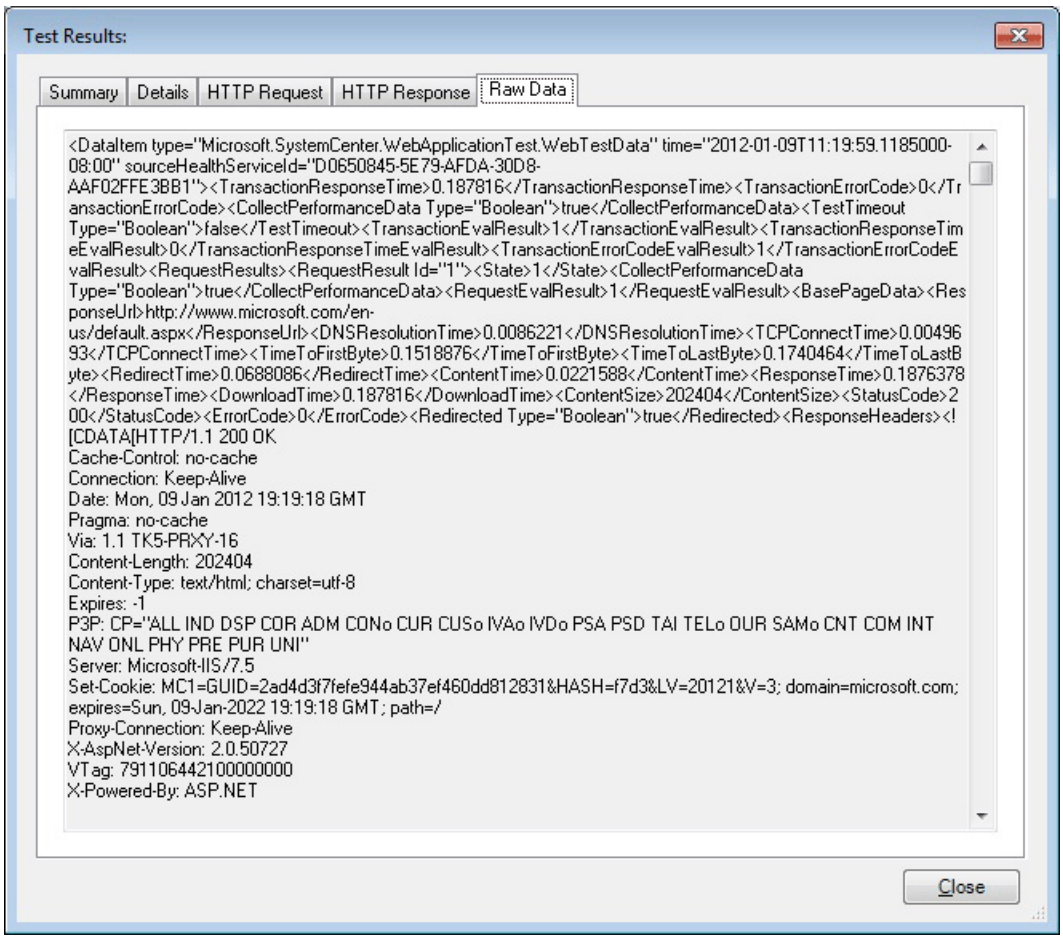
Test Results: HTTP Response Tab



The following options are available on the **Test Results HTTP Response** tab of the wizard.

Option	Description
What is shown on this tab	Displays details about the HTTP Response for the test comes back from website.

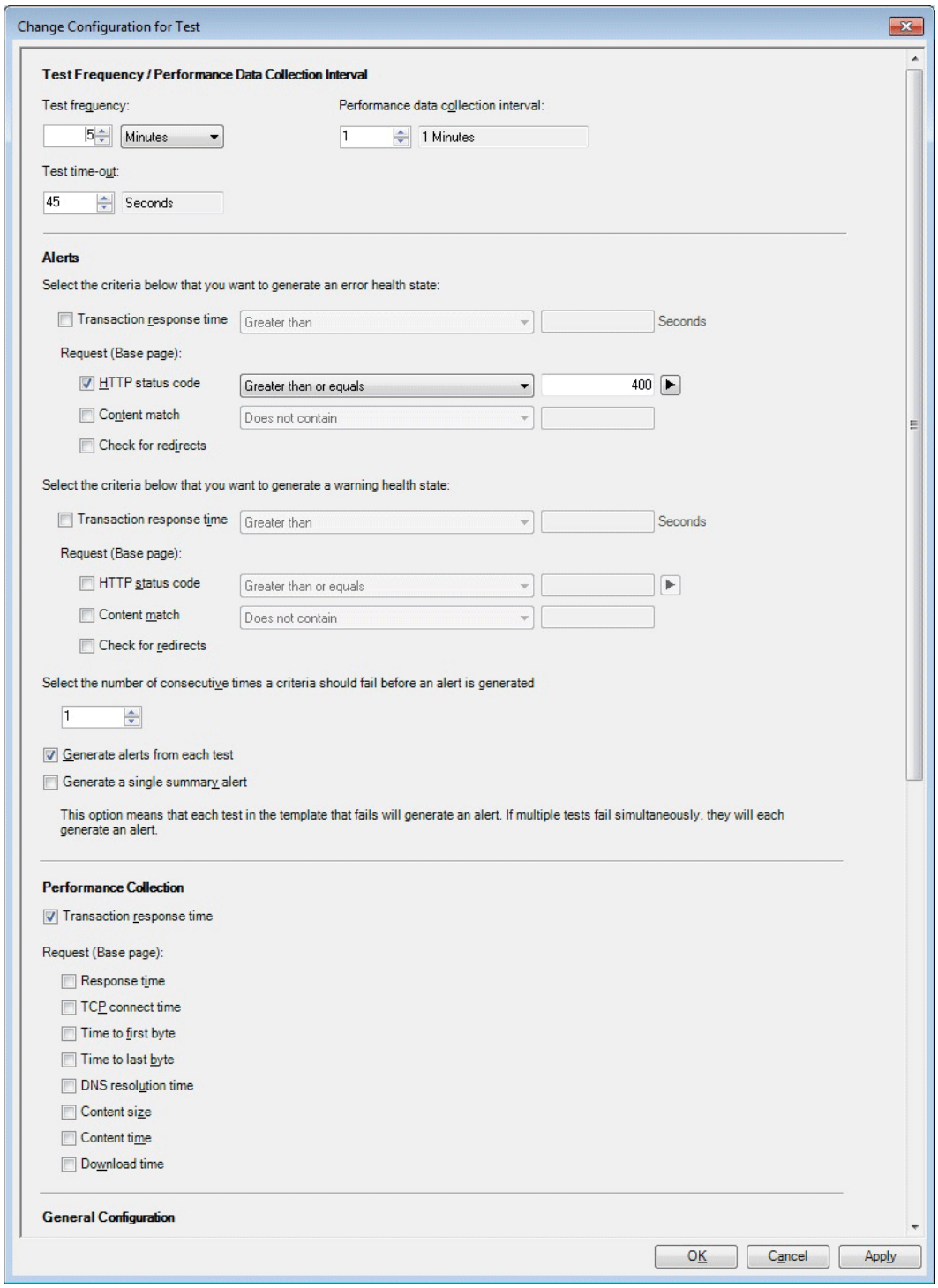
Test Results: Raw Data Tab

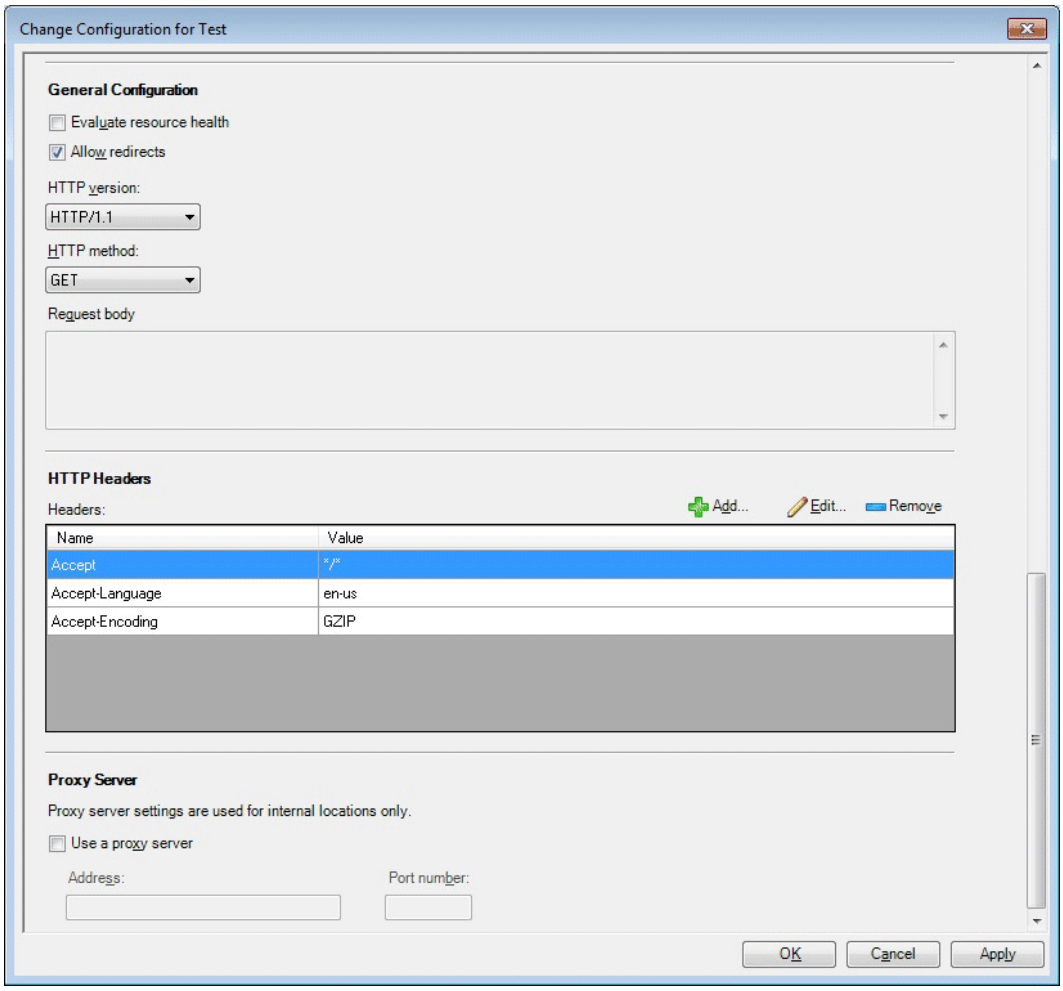


The following options are available on the **Test Results Raw Data** tab of the wizard.

Option	Description
What is shown on this tab	Displays all of the data unformatted that we get back from the site. If there's a problem with the website, this information might help you figure out what might be wrong with the website.

Change Configuration for Test Set





The following options are available on the **Change Configuration for Test Set** page of the wizard.

Important

Settings on this page apply to all tests in the template.

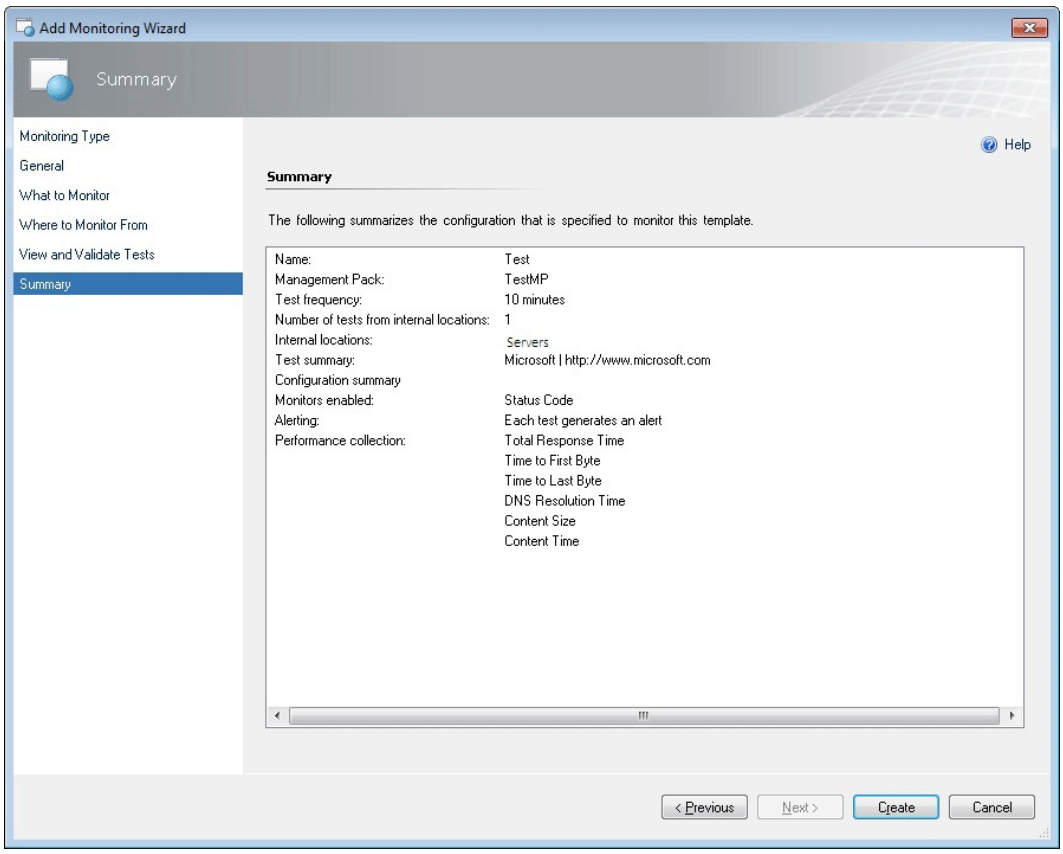
Option	Description
Test Frequency/Performance Data Collection Interval: Test frequency	Enter the how often you want to run each test.
Test Frequency/Performance Data Collection Interval: Performance data collection interval	Enter the frequency with which you want to collect performance data. This specifies whether you want to collect performance data every interval or not. For example, if the interval is 10 minutes and the collection interval is set to 2, this means that performance data will be

Option	Description
	collected every other interval, or once every 20 minutes.
Test Frequency/Performance Data Collection Interval: Test time-out	Enter how long you want the test to keep a request active until the test times out and cancels.
Alerts: Criteria for error health state: Transaction response time	Specify if transaction response time is a factor that should or should not generate an error health state. If it is specified to generate an error health state, set the threshold in seconds that a transaction must exceed before it generates an error health state.
Alerts: Criteria for error health state: Request (Base page): HTTP status code	Specify if the HTTP status code is a factor that should or should not generate an error health state. If it is specified to generate an error health state, set the HTTP status code to the number for which you want it to generate an error health state.
Alerts: Criteria for error health state: Request (Base page): Content match	Specify if any content matches should or should not generate an error health state. If it is specified to generate an error health state, specify the content you wish to match.
Alerts: Criteria for error health state: Request (Base page): Check for redirects	Specify if the presence of redirects should or should not generate an error health state.
Alerts: Criteria for warning health state: Transaction response time	Specify if the transaction response time is a factor that should or should not generate a warning health state. If it is specified to generate warning health state, set the threshold in seconds that a transaction must exceed before it generates a warning health state.
Alerts: Criteria for warning health state: Request (Base page): HTTP status code	Specify if the HTTP status code should or should not generate a warning health state. If it is specified to generate warning health state, set the HTTP status code to the number for which you want it to generate a warning health state.
Alerts: Criteria for warning health state: Request (Base page): Content match	Specify if any content matches should or should not generate a warning health state. If it is specified to generate a warning health state,

Option	Description
	specify the content you wish to match.
Alerts: Criteria for warning health state: Request (Base page): check for redirects	Specify if the presence of redirects should or should not generate a warning health state.
Alerts: Number of consecutive time a criteria should fail before an alert is generated	Specify the number of consecutive times selected criteria in the Alerts section list should fail before an alert is generated.
Alerts: Generate alerts from each test	Select to receive an alert for each URL test for an application.
Alerts: Generate a single summary alert	Select to receive a summary alert for an application, rather than choosing to receive an alert for each URL test for an application. This is helpful if you are monitoring a vertical website or an application because this will reduce the number of alerts you receive and keep the focus of your alerts the overall state of the application. You can further reduce alerts by raising the threshold for how many failures you want to have before receiving an alert. Together, these two approaches will focus your alerts on what is most important to you: How well the application is running, given the performance you require.
Performance Collection: Transaction response time	Cumulative response time: DNS_RESOLUTION_TIME + TCP_CONNECT_TIME + TIME_TO_LAST_BYTE
Performance Collection: Request (Base page): Response time	Processing time for the request, such as opening a browser and waiting for all resources to load.
Performance Collection: Request (Base page): TCP connect time	Time taken to establish a TCP connection to the target server and receive the initial greeting from the service.
Performance Collection: Request (Base page): Time to first byte	Time take since the TCP connection is established till the first byte of response is received.
Performance Collection: Request (Base page): Time to last byte	Time from when TCP connection is established until the last byte of response is completely

Option	Description
	received.
Performance Collection: Request (Base page): DNS resolution time	Time taken to resolve the URL domain name to the IP address.
Performance Collection: Request (Base page): Content size	Size of the response body received.
Performance Collection: Request (Base page): Content time	Base page download time (base page only).
Performance Collection: Request (Base page): Download time	Processing time for the request, such as opening a browser and waiting for all resources to load.
General Configuration: Evaluate resource health	Specify whether to evaluate the health of the entire resource.
General Configuration: Allow redirects	Specify if redirects can be allowed and not cause an error or warning state.
General Configuration: HTTP version	Specify the HTTP version being tested.
General Configuration: HTTP method	Specify the HTTP method.
General Configuration: Request body	
HTTP Headers: Headers column	Specify which headers can be accepted.
HTTP Headers: Value column	Specify the value in the header that can be accepted.
HTTP Headers: Add	Add header names and values that can be accepted.
HTTP Headers: Edit	Opens the HTTP Header Properties page where you can change the Name or Value of the selected HTTP headers.
HTTP Headers: Remove	Removes selected header from the accepted list.
Proxy Server: Use a proxy server	Specify whether to use a proxy server.
Proxy Server: Address	Specify the address of the proxy server.
Proxy Server: Port number	Specify the port number.

Summary



The **Summary** page of the wizard lists the settings you have configured for the **Web Application Availability Monitoring** template. If you want to change any of these settings, click **Previous** or the template page until you reach the page with the settings that you want to change.

Creating and Modifying Web Application Availability Monitoring Templates

For the procedure to run the .NET Application Performance Monitoring wizard, see How to Configure Web Application Availability Monitoring

To modify an existing Web Application Availability Monitoring template

1. Open the Operations console with a user account that has Author credentials in the management group.
2. Click the **Authoring** workspace.
3. In the **Authoring** navigation pane, expand **Management Pack Templates**, and then select **Web Application Availability Monitoring**.
4. In the **Web Application Availability Monitoring** pane, locate the template you want to change.

5. Right-click the test group that you want to modify, and then select **Properties**.
6. Using the tabs to navigate the pages of settings, make the desired changes, such as reconfiguring criteria for tests in this group, and then click **OK**.

Viewing Web Application Availability Monitoring Monitors and Collected Data

After you configure monitoring for an application, these three views will help you get started with the monitoring experience.

To view all Web Application Availability Monitoring monitored applications

1. Open the Operations console.
2. Click the **Monitoring** workspace.
3. In the **Monitoring** navigation pane, expand **Application Monitoring**, expand **Web Application Availability Monitoring**, and then click **Web Application Status**.

To view the state of each monitor

1. Open the Operations console.
2. Click the **Monitoring** workspace.
3. In the **Monitoring** navigation pane, expand **Application Monitoring**, expand **Web Application Availability Monitoring**, and then click **Test State**.
4. In the **Test State** view, right-click an object. Select **Open**, and then click **Health Explorer**.

To view the performance collected for an application component

1. Open the Operations console.
2. Click the **Monitoring** workspace.
3. In the **Monitoring** navigation pane, expand **Application Monitoring**, expand **Web Application Availability Monitoring**, and then click **Web Application Status**.
4. In the **Test State** pane, right-click an object. Select **Open**, and then click **Performance View**.
5. In the **Legend** pane, select the counters that you want to view.
6. Use options in the **Actions** pane to modify the Performance view.

See Also

How to Configure Web Application Availability Monitoring

Monitoring Web Application Availability Tests and Alerts

Dashboard Views for Web Application Availability Monitoring

Reporting for Web Application Availability Monitoring

How to Configure Web Application Availability Monitoring

The **Web Application Availability Monitoring** template in System Center 2012 – Operations Manager lets you monitor web applications from internal locations.

Key Concepts and Strategies

Here are some key concepts and strategies to keep in mind as you use the template to configure tests:

- Web Application Availability Monitoring can monitor applications as well as individual URLs. Your tests can be authored to optimize for application monitoring or vertical application feature monitoring. For example, a website shopping experience is a vertical application feature. Alternatively, you can monitor horizontal application features, such as all home pages on a site.
- Give your tests friendly names you can easily recognize when you monitor.
- Group URLs by Web Application and you will see one entry in the monitoring view for each application. This lets you see the state of each application template run at a glance and helps isolate problems related to servers or networks.
- Web Applications State is a defined as the worst of rollup of individual tests. You can use overrides to change what it displays.
- Validate each test configuration before exiting the Add Monitoring Wizard so you can check that the response you get is the one you expect for internal watcher nodes.
- If you are monitoring a vertical website or an application, you can focus alerts on application state by setting up a summary alert for an application, rather than choosing to receive an alert for each URL test for an application. This will reduce the number of alerts you receive and keep the focus of your alerts the overall state of the application. You can further reduce alerts by set the threshold for how many failures you want to have before receiving an alert. Together, these two approaches will focus your alerts on what is most important to you: how well the application is running.

How to Configure Monitoring

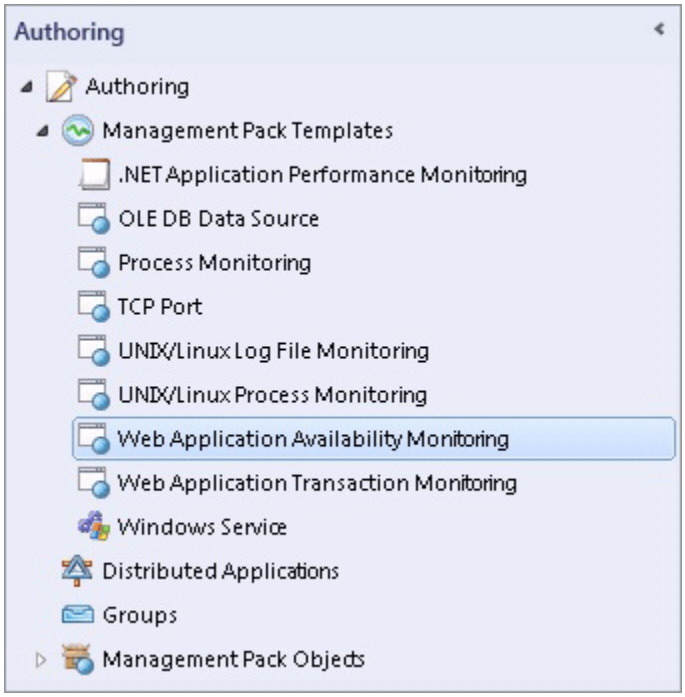
To configure Web Application Availability Monitoring

1. To configure internal URL tests, use the Web Application Availability Monitoring template. This template allows you to create availability monitoring tests for one or more Web Application URLs and run them from internal locations and will walk you through selecting the URLs you want to monitor and where you want to monitor them from.

   To open the Web Application Availability Monitoring template, in the Operations Manager console, in the navigation pane, click the **Authoring** button, click **Management Pack Templates**, click **Web Application Availability Monitoring**, and then, in the tasks pane,

click the **Add Monitoring Wizard**. Click **Web Application Availability Monitoring**, and then click **Next**.

Location of Web Application Availability Monitoring



2. On the **General** page, enter a friendly name and description for your test and the management pack, which stores settings that are specific to this version of the template. Click **Next**

   Tip
   It is important to give your tests names you can easily recognize as this will help you identify them later when you begin monitoring.

3. On the **What to Monitor** page, enter the URLs you want to monitor. You can add URLs to the list by typing, pasting, or importing a file (such as a spreadsheet) into the table, including the appropriate protocol (http:// or https://). You can paste entire rows as pairs of comma-separated values (CSV) that are in the format “Name, URL”, or you can paste just the list of URLs.
   - To type or paste a URL, click in the **Name** and **URL** boxes, respectively, and follow the examples on the page to enter the information.
   - To import names and URLs from another source, click **Add** and follow the instructions to browse and select to the file you want to import.

   Tip
   Group URLs by web application. Example: **Microsoft website** would be the name of many URLs to test from various locations. This keeps the application, **Microsoft website**, the focus of the monitoring rather than the many URLs you

are testing for this application. This strategy takes advantage of the dashboard monitoring views, which show the **Web application state** by application name and state so you can easily see the overall health of your monitored application and separate problems related to external factors, such as Internet or network problems, from application or service problems.

4. On the **Where to Monitor From** page, select the locations from which you want the URLs monitored.
5. To monitor from internal locations, use the dropdown menu to select to run tests from a server agent or a resource pool. Above the **Internal locations** field, click **Add** and select the internal locations (server names) you want to monitor from and add those to your list of **Selected locations**. Click **OK**

   Note
   The **Select internal locations** page verifies the version of health service on the agents and only Operations Manager agents are shown. If the version is not verifiable or not supported, the agents will not be displayed.
6. The **View and Validate Tests** page shows a summary of all internal tests that will be run. You can only validate a configuration of internal tests. To validate an internal test configuration, select a test and click **Run Test**. If you want to change the default settings for the tests, performance data, and alerts for all tests (external and internal) created in this template, click **Change Configuration**. For more information, see the “Configuring alerts and performance data collection” in this document. When you have validated your tests, click **Next** to see the **Test Results** page of the test configuration you created with this template.

   Tip
   Validate internal test configurations before exiting the wizard so you can make sure that the response you get is the one you expect.
7. On the **Test Results** page, the **Summary** tab shows if your test succeeded and whether any of your error criteria failed. To see more details, click through the **Details**, **HTTP Request**, and **HTTP Response** tabs. Click **Close** to return to the **View and Validate Tests** page where you can either choose to reconfigure your tests, or, if the test results look good, click **Create** to initiate the live testing.

To configure alerts and performance data collection

1. Configure alerts and performance during test configuration. To configure alerts, on the **View and Validate Tests** page, click **Change Configuration**. Here you can set the criteria that are most important for you to monitor. These are the URL monitoring performance counters you can set and a description of what each tracks. Most of these are collected by default. For detailed information about the authoring template, see Web Application Availability Monitoring Template

   Base page (the page served by the request URL)

   - Content size: Size of the response body received.
   - DNS resolution time: Time taken to resolve the URL domain name to the IP address.

- Content time: Base page download time (base page only).
- Download time (cumulative): Processing time for the request, such as opening a browser and waiting for all resources to load.
- TCP connect time: Time taken to establish a TCP connection to the target server and receive the initial greeting from the service.
- Time to first byte: Time take since the TCP connection is established till the first byte of response is received.
- Time to last byte (cumulative): Time from when TCP connection is established until the last byte of response is completely received.
- Response time (cumulative): DNS_RESOLUTION_TIME + TCP_CONNECT_TIME + TIME_TO_LAST_BYTE.

Total data

- Total transaction time: Same a download time for the single URL case. In multi-step (transaction) case, it's the sum of download times for all requests in the transaction (cumulative).

2. In the **Test Frequency/Performance Data Collection Interval** section, you can set your tests' frequency, how often you want performance data collected, and when the test should time out.
3. In the **Alerts** section, select the criteria that you want to use to generate an error health state, a warning health state, and the number of consecutive times criteria should fail before an alert is generated. When you monitor your alerts, here is how they will appear based on your alert configuration:
   - Healthy state=Green
   - Error state=Yellow
   - Warning state=Red

   Tip
   If you are monitoring a vertical website or an application, you can focus alerts on application state by setting up a summary alert for an application, rather than choosing to receive an alert for each URL test for an application. To do this, select the **Generate a single summary alert** checkbox. This will reduce the number of alerts you receive and keep the focus of your alerts the overall state of the application. You can further reduce alerts by raising the threshold for how many failures you want to have before receiving an alert. Together, these two approaches will focus your alerts on what is most important to you: How well the application is running, given the performance you require.
4. You also can change settings for **Http Headers**, designate a **Proxy Server** (used for internal locations only), and change other general settings. When you have finished configuring the settings for your tests, click **OK** to return to the **View and Validate Tests** page.

Monitoring Web Application Availability Tests and Alerts

To view overall web application health

1. To get a view of the general health of each application you are monitoring, in the Operations Manager console, in the navigation pane, click the **Monitoring** button, and then click **Application Monitoring**.
2. Click **Web Application Availability Monitoring**, and then click **Web Applications State**. This is the best view to see the overall health of each application.

   The alert state for each application is displayed according to the alert configurations used when you set up the tests:

   - Green=Healthy
   - Yellow=Error
   - Red=Warning
3. To see details about a particular application, double-click the test to open the **Health Explorer**.

   The Health Explorer allows you to see the health states for each criterion, so you can pinpoint what caused the application to show an error or warning.

To view alerts and alert details

1. To see active alerts for the applications you are monitoring, in the Operations Manager console, in the navigation pane, click the **Monitoring** button, and then click **Application Monitoring**.
2. Click **Web Application Availability Monitoring**, and then click **Active Alerts**. If there are alerts, you will see them listed in the **Active Alerts** pane. As with the application health, the alert state is displayed in the color according to your alert configurations.
3. To see alert details, click the alert to see the **Alert Details** pane.
4. To see more details about an alert, double-click the alert to open the **Alert Properties** page.

   On the **Alert Properties** page **General** tab, you can reassign the alert, see the alert description, and change the alert status to **New** or, if you have resolved the issue, **Closed**. Use the **Previous** and **Next** buttons to scroll through the alerts for easy review. When you are finished viewing or changing properties, click **OK** to save your changes.

To view data for individual URLs and locations

1. To get a view of each test you configured in the Web Application Availability Monitoring template, in the Operations Manager console, in the navigation pane, click the **Monitoring** button, and then click **Application Monitoring**.
2. Click **Web Application Availability Monitoring**, and then click **Test State**. If there are

alerts, you will see them listed in the **Active Alerts** pane. As with the application health, the alert state is displayed in the color according to your alert configurations.

Note

A test is one URL and one location.

3. To see the details of a particular test, double-click the test to open the **Health Explorer**.

   The Health Explorer allows you to see the health states for each criterion, so you can see in detail what caused the test to show an error or warning.

Dashboard Views for Web Application Availability Monitoring

Dashboards show your test results so you can more effectively see trends and isolate problems for certain tests, locations, and applications.

Viewing the Dashboards

To view the Web Application Availability Monitoring dashboards for internal URL tests, you need to use Operations Manager script.

To view the Summary and Details dashboards

1. From the **Start** menu, open the Operations Manager Shell.
2. Use New-SCOMLocation, Get-SCOMAgent, and Set-SCOMLocation to add a location, get an Operations Manager agent, and then associate the location with the agent. Here is an example using Seattle, WA as a location:

```
PS C:\> $Location = New-SCOMLocation -DisplayName "Seattle,
WA" -Latitude 47.6063889 -Longitude -122.330833

PS C:\> $Agent = Get-SCOMAgent -Name "Server01.Contoso.com"

PS C:\> Set-SCOMLocation -Location $Location -Agent $Agent
```

   For more information about adding a location, see New-SCOMLocation. For more information about getting an Operations Manager agent, see Get-SCOMAgent. For more information about associating a location with an agent, see Set-SCOMLocation.
3. After you run the commands, in the Operations Manager console, in the navigation pane, click the **Monitoring** button, and then click **Application Monitoring**.
4. Expand **Web Application Availability Monitoring**, click **Active Alerts**, **Test State**, or **Web Application Status** to display alerts or status for the category.
5. From any of these views (alert, test state or web application), click to highlight the application you want to see a summary of and follow the procedure to view the

dashboards in this topic.

The Summary Dashboard

If you want to check to see if an application is available, the Summary Dashboard is a helpful view. It displays a world map, the locations you are monitoring from, and the rollup test status from each location. You can then click the location or select several locations to compare.

To check the overall status of a web application using the Summary Dashboard

1. In the Operations Manager console, in the navigation pane, click the **Monitoring** button, and then click **Application Monitoring**.
2. Expand **Web Application Availability Monitoring**, and then click **Active Alerts**, **Test State**, or **Web Application Status** to display alerts or status for the category.
   - **Active Alerts** displays all alerts for all web applications (templates) or tests.
   - **Test State** displays the state of each test, which is based on how you configured the tests. You can click State, Display Name, and Context column headings to sort the test state list accordingly. For example, if you sort by Context, this groups the list by web applications, so you can see the state of the tests for each web application.
   - **Web Application Status** displays the worst rollup of tests for each web application. This is a quick way to check whether an application is having any issues.
3. From any of these views (alert, test state or web application), click to highlight an entry for the application you want to see a summary of. Then, in the **Tasks** pane, in the **Navigation** section, click **Summary Dashboard**. This displays a dashboard for the entire application—a world map that shows all locations the application is being tested from and the worst rollup status of all of the tests from each location. For example, red means that at least one test from that location has failed and green means that no tests have failed.
4. To see the test status for all tests from a given location, click that location and the test status displays below.
5. If you want to investigate a particular test, or group of tests, click to highlight the tests you want to investigate and in the **Tasks** pane, in the **Navigation** section, click **Detailed Dashboard – List**. This opens detailed views into the item you clicked. For more information, see the details dashboard section below.

The Details Dashboard

If you want to investigate a particular test or alert, use the Detailed Dashboard – List. For each web application, you choose the location and which tests in that location you want to investigate. Six key metrics are shown, which you can use to pinpoint and isolate issues and compare the performance of pages from your web applications or compare your pages to competitors' pages.

To pinpoint problems using the Details Dashboard

1. Begin the same way you opened the Summary Dashboard. In the Operations Manager

console, in the navigation pane, click the **Monitoring** button, and then click **Application Monitoring**.

2. Expand **Web Application Availability Monitoring**, and then click **Active Alerts**, **Test State**, or **Web Application Status** to display alerts or status for the category.
3. From any of these views (alert, test state or web application), click to highlight the application you want to see a summary of, and in the **Tasks** pane, in the **Navigation** section, click **Detailed Dashboard - List**.

   Tip
   If you are already viewing the Summary Dashboard, you can go directly to the Detailed Dashboard by clicking to highlight a test or group of tests and then in the **Tasks** pane, in the **Navigation** section, clicking **Detailed Dashboard**.
4. In the section with the name of your application, for example **Bing template** select the locations you want to see more details about.
5. In the **Test Status** section, the check boxes act as a legend for the tests you want to investigate in the performance graphs. For example, you can select the same page being tested from different locations to see how the pages are performing for the different locations. Selection (blue highlighting) determines which tasks are available and can be run.

Health Explorer

As its name implies, Health Explorer allows you to see more details about the health status of a web application availability test running against a URL from a particular location. Health Explorer shows you when a test changed state from, for example, healthy to unhealthy.

To view the context of a problem using Health Explorer

1. To open Health Explorer for a particular test, highlight an alert, test state, or web application status item, and in the **Tasks** pane, click **Health Explorer**. If you are already in a dashboard view, you can also open Health Explorer in the Summary Dashboard and Detailed Dashboard by right-clicking an entry, and then clicking **Health Explorer**.
2. In **Health Explorer**, in the pane named with your test, click to highlight an item you want to investigate.
3. Click the **State Change Events** tab to see details on when a state changed from healthy to unhealthy.
4. In the **State Change Events Details** pane, you can see the error details that caused the health state change of your test.

   Tip
   It is a good idea to check Health Explorer frequently because it shows you details about the context and sequence of status changes and errors.

Reporting for Web Application Availability Monitoring

Web Application Availability Monitoring introduces to two new report tasks: Test Availability and Test Performance. The Test availability reporting shows measures reflecting how available the web application was over time. The Test Performance report shows selected objects and performance counter values over time to relate how well a web application has performed. These two reports directly reflect the web application monitoring for Web Application Availability is integrated into the Operations Manager console, you can run these two new reports just as you would run the other standard Operations Manager reports.

To run the Test Availability report

1. You can run the Test Availability report from several locations:
   - In the Operations Manager console, in the navigation pane, click the **Monitoring** button, click **Application Monitoring**, click **Web Application Availability Monitoring**, and then click **Active Alerts**, **Test State**, or **Web Application Status** to display alerts or status for the category. Highlight one or more web applications, alerts, or test states, and then, in the **Tasks** pane, in the **Report Tasks** section, click **Test Availability**.
   - If you want to add more objects, click **Add Object**, and in the **Add Object** page, filter your search or just click **Search** to see all tests in for the web application that you have selected. Click the available items you want to include in your report and click **Add**. Click **OK**.
   - In the **Summary Dashboard** view, click to highlight an item in the **Test Status**, and then run the report task from the **Tasks** pane.
   - In the **Details Dashboard**, click to highlight an item, and then run the report task from the **Tasks** pane.
2. In the **Aggregation** section of the **Test Availability** report configuration page, select how often you want information aggregated and a time and date range.

   Note
   The data warehouse only aggregates data hourly for 100 days. After 100 days, data are aggregated daily.
3. Select the aspects, such as **Unplanned Maintenance**, that you would like to include in the report, and then click **Run** to generate the report.
4. In the report, click a plus sign to see details. To see a graph of the data, click the **Availability Tracker** link.

To run the Test Performance report

1. You can run the Test Performance report from several locations:
   - In the Operations Manager console, in the navigation pane, click the **Monitoring**

button, click **Application Monitoring**, click **Web Application Availability Monitoring**, and then click **Active Alerts**, **Test State**, or **Web Application Status** to display alerts or status for the category. Highlight one or more web applications, alerts, or test states, and then, in the **Tasks** pane, in the **Report Tasks** section, click **Test Performance**.

- If you want to add more objects, click **Add Object**, and in the **Add Object** page, filter your search or just click **Search** to see all tests in for the web application that you have selected. Click the available items you want to include in your report and click **Add**. Click **OK**.
- In the **Summary Dashboard** view, click to highlight an item in the **Test Status**, and then run the report task from the **Tasks** pane.
- In the **Details Dashboard**, click to highlight an item, and then run the report task from the **Tasks** pane.

2. In the **Aggregation** section of the **Test Performance** report configuration page, select how often you want information aggregated and a time and date range.

   Note
   The data warehouse only aggregates data hourly for 100 days. After 100 days, data are aggregated daily.

3. To generate the report, click **Run**.
4. In the report, click a plus sign to see details.

Web Application Transaction Monitoring Template

The *Web Application Transaction Monitoring* template lets you test a website or web-based application by sending requests over HTTP, validating their response, and measuring their performance. This can be a simple test to determine if the website is responding, or it can be a complex set of requests to simulate a user who is performing such actions as logging on to the site and browsing through a set of pages.

The HTTP requests are sent from one or more Watcher Nodes. The website that is being monitored can reside on any computer whether it has an agent for Operations Manager installed. It can be an external website, but it must be accessible from the watcher nodes. Each watcher node must have an Operations Manager agent installed.

Scenarios

Use the **Web Application Transition Monitoring** template for monitoring the availability and performance of any website or web-based application to test both general availability and

functionality. For internal websites, you can use watcher nodes in different network segments to ensure that the site is available to each segment.

In addition to general availability, you can check the functionality of the website by testing different pages and features. For example, you could check a logon process by performing a test logon with a test user account every few minutes. You could test the functionality of a search page by performing a sample search after the test user account is logged on. You can then analyze the HTML that is returned from these pages to verify whether the page functioned as expected. In addition to testing this functionality, you can analyze the time it takes to fill the request to measure the performance.

Web Application Transaction Monitoring Template Topics

The **Web Application Transaction Monitoring** is more complex than the other management pack templates and supports a variety of monitoring scenarios. The following topics provide details on the different tools and procedures that you can use for different scenarios.

- How to Create a Single URL Web Application Monitor

  This procedure explains how to run the *Web Application Transaction Monitoring* wizard to create a simple **Web Application Transaction Monitoring** template that monitors a single URL. You can either use this simple monitor with no modification or insert additional requests once it is completed.
- How to Capture Web Application Recording
- This procedure explains how to use the **Web Recorder** to record a browser session with multiple requests. You can either use this session with no modification or edit the application and request settings once it is completed.
- How to Edit Settings or Requests in a Web Application

  This topic includes procedures for editing a web application and its contained requests and for creating additional requests in an existing template.
- How to Replace Parameters in a URL Request
- This topic includes a method to retrieve information from one request and use it in a subsequent request.

How to Create a Single URL Web Application Monitor

The most basic **Web Application Transaction Monitoring** template includes a single request. This may be sufficient for testing the general availability of a website, or as the basis for creating a more complex monitoring scenario by adding requests either manually or by capturing them in a browser session.

To create a single URL web application transaction monitoring template

1. Start the Operations console with an account that has Author user rights in the management group.
2. Open the **Authoring** pane.
3. Right-click **Management Pack Templates**, and then select **Add Monitoring Wizard**.
4. On the **Select Monitoring Type** page, select **Web Application Transaction Monitoring**, and then click **Next**.
5. On the **General Properties** page, do the following:
   a. In the **Name** and **Description** boxes, type a name and an optional description.
   b. Select a management pack in which to save the monitor, or click **New** to create a new management pack. For more information, see Selecting a Management Pack File.
   c. Click **Next**.
6. On the **Web Address** page, do the following:
   a. In the **URL** box, specify that the request uses http or https.
   b. Type the URL to connect to.
   c. Click the **Test** button to perform a test connection to the URL. If the connection succeeds, click **Details** to inspect the response time and other details of the connection. This information can be valuable if you decide to manually edit the request after the template is created.

      Note
      The test is performed from the workstation that you are using to run the wizard. If this workstation cannot access the website, this test fails. When the template is completed, the test is run from the watcher nodes that you specify.

   d. Click **Next**.
7. On the **Watcher Node** page, do the following:
   a. Select one or more Watcher Nodes to run the web requests.
   b. Specify the frequency to run the web request in the **Run this query every** box.
   c. Click **Next**.
8. On the **Summary** page, review the summary of the monitor, and then click **Create**.

See Also

How to Edit Settings or Requests in a Web Application

How to Capture Web Application Recording

How to Capture Web Application Recording

The fastest and easiest way to create a **Web Application Transaction Monitoring** template with multiple requests is to record a session from Internet Explorer. Using the **Web Recorder**, you can interactively record a sequence of actions that are stored in the request sequence with default settings. After the session has been recorded, you can manually edit the individual requests if any of them require unique configuration.

You can run the **Web Recorder** to create a **Web Application Transaction Monitoring** template, or you can run it from an existing template to add additional requests.

To record a new web application

1. Start the Operations console with an account that has Author user rights in the management group.
2. Open the **Authoring** pane, expand **Management Pack Templates**, and then click **Web Application Transaction Monitoring**.
3. In the **Actions** pane, click **Record a browser session**.
4. In the **Web Application Editor** dialog box, do the following:
   a. Type a name and optionally a description of the recording. The name appears in the **Monitoring** pane.
   b. Select a management pack in which you want to save your Web Application object, and then click **OK**. For more information, see Selecting a Management Pack File.
5. Click **Start capture**.

   Follow the steps in To use the Web Recorder.

To add a web recording to an existing browser session

1. Start the Operations console with an account that has Author user rights in the management group.
2. Open the **Authoring** pane, expand **Management Pack Templates**, and then click **Web Application Transaction Monitoring**.
3. Select the template that you want to edit, and then click **Edit Web Application settings**.
4. Select the location in the browser session to include the recorded requests.
5. Click **Start capture** in the **Actions** pane.

   Follow the steps in To use the Web Recorder.

To use the Web Recorder

1. When you start the capture, Internet Explorer opens with the **Web Recorder** in the navigation pane. If you do not see the **Web Recorder**, see Troubleshooting Web Capture.
2. In the browser window, follow the actions that you want to be monitored. For example, you might click some links or add a product to a shopping cart. As you perform actions,

they are recorded in the **Web Recorder** pane.

3. When you have completed the recording, click **Stop** in the **Web Recorder** pane. Internet Explorer closes, and the actions you performed are added to the **Web Application Editor**.
4. Optionally, click **Run Test** in the **Actions** pane to immediately run the recorded actions and view the results. At this point, you might encounter the following errors:
   - If the web application requires authentication, running a test of the web application might fail. While running the test, credentials that have been configured for this web application are not used. If the site you are testing does not explicitly require authentication, the test might still succeed. In the **Actions** pane, under **Web Application**, you can click **Configure Settings** for any website to select authentication settings.
   - If you see an error message that the server name or address cannot be resolved, but you can access the web application through Internet Explorer while not recording a session, you might have to configure your proxy settings. In the **Actions** pane, under **Web Application**, you can click **Configure Settings** for any website to select authentication settings.
5. Optionally, add requests or edit captured requests by using the **Insert request** or the **Properties** options in the **Actions** pane.

   For more information, see How to Edit Settings or Requests in a Web Application.

See Also

Troubleshooting Web Capture

Troubleshooting Web Capture

When you select an option to capture a browser session in Operations Manager, the **Web Recorder** should start, and requests should be recorded as you select them in the browser. If **Web Recorder** does not work correctly, check the following sections to determine a potential cause and to resolve it.

Enabling Third-Party Browser Extensions

Internet Explorer must be configured to allow third-party extensions on the computer that you are using to perform the capture.

To enable third-party browser extensions

1. In Internet Explorer, click **Tools**, and then click **Internet Options**.
2. Click the **Advanced** tab.
3. Under **Settings**, under **Browsing**, select **Enable third-party browser extensions**.

Run As Administrator

If you are using Windows 7 or Windows Server 2008 R2, or if you are using the Windows Vista or Windows Server 2008 operating system with User Account Control (UAC) enabled, Internet Explorer must be running as an administrator, or the requests will not be added to the **Web Recorder**. Because the Operations console is starting Internet Explorer, you have to start the Operations console as an administrator.

To run the Operations console as administrator

1. Click **Start**, then **All Programs**, then **System Center Operations Manager 2012**.
2. Right-click the **Operations console** icon.
3. Click **Run as administrator**.

X64 Version of Internet Explorer

If you are running the Operations console on a 64-bit operating environment, the Web Recorder might not be displayed when Internet Explorer starts because the x64 version of the add-on was registered and is not used in the x86 version of Internet Explorer. You have to use the x64 version of Internet Explorer for the capture process.

To perform the capture with the x64 version of Internet Explorer

1. After you start Internet Explorer from the Operations console, close Internet Explorer.
2. Click the **Start** button, and on the **Start** menu, point to **All Programs**, and then click **Internet Explorer (64-bit)**.

See Also

How to Capture Web Application Recording

How to Edit Settings or Requests in a Web Application

You can use the Web Application Editor to manually create or edit a request in a **Web Application Transaction Monitoring** template. For editing a particular request, there is no difference whether the request was created manually or by capturing a browser session. For detailed information about the properties that you can set for the request, see Web Application Request Properties.

To open the Web Application Editor

1. Start the Operations console with an account that has Author credentials in the

management group.

2. Open the **Authoring** workspace.
3. In the **Authoring** navigation pane, expand **Management Pack Templates**, and then click **Web Application Transaction Monitoring**.
4. Select the template that you want to edit, and then click **Edit Web Application settings**.

Use one of the following procedures to edit the settings that you want.

To edit the settings for a Web Application

1. With the **Web Application Editor** open, set the properties of the application and then click **Apply**. For detailed information about the different options, see Web Application Properties.

To edit an existing request in a Web Application

1. With the **Web Application Editor** open, select the request that you want to edit.
2. In the **Actions** pane, click **Properties**.
3. Set the properties of the request and then click **OK**. For detailed information about the different options, see Web Application Request Properties.
4. Click **Apply** to save the web application settings.

To add a request to a Web Application

1. With the **Web Application Editor** open, select the location in the browser session where you want to insert the request.
2. In the **Actions** pane, click **Insert Request**.
3. Type the URL of the request in the **Request URL** box.
4. Optionally, set other properties of the request, and then click **OK**. For detailed information about the different options, see Web Application Request Properties.

See Also

Web Application Properties

Web Application Request Properties

How to Capture Web Application Recording

Web Application Properties

The following sections describe the settings available for a **Web Application Transaction Monitoring** template in Operations Manager. You can set the properties of these requests by using the procedure in How to Edit Settings or Requests in a Web Application. Each section in this topic represents a tab in the **Web Application Properties** dialog box.

General Tab

Use the **General** tab to specify the general details of the application. The various options are explained in the following table.

Item	Description
Web Application Name	The name of the application that appears in the Operations console.
Description	Optional description of the application that appears in the **Details** pane in the Operations console.
Retry Count	Number of times to retry connecting to a site if the first attempt fails.
Management Pack	The management pack in which the **Web Application Transaction Monitoring** template is stored. This cannot be changed.
Authentication Method	Specifies the authentication method to use for the website. If no authentication is required, select **None**.
User Account	The Run As account to use for authenticating on the site. Only existing accounts that match the selected authentication method are listed. For more information about Run As accounts, see Managing Run As Accounts and Profiles.
Use a proxy server to connect	Select this option if the watcher nodes must connect to the website through a proxy server.
Address	The address of the proxy server if one is required.
Port	The port for the proxy server if one is required.
Authentication Method	Specifies the authentication method to use for the proxy server. If no authentication is required, select **None**.
User Account	The Run As account to use for authenticating on the proxy server. Only existing accounts that match the selected authentication method are listed. For more information about Run As accounts, see Managing Run As Accounts and Profiles.

Watcher Node Tab

Use the **Watcher Node** tab to specify the watcher nodes that you want to use for this web application and the frequency that you want to run the web application. For more information about watcher nodes, see Watcher Nodes.

Performance Criteria Tab

Use the **Performance Criteria** tab to enable the **Transaction response time** monitor for the application that monitors for the transaction time of all of the requests in the browser session. The various options are explained in the following table.

Item	Description
Error Transaction Response Time	Select this option and provide a criteria and number of seconds if you want to monitor for a critical state. If the time to process the complete set of requests matches this criteria, the monitor is set to a critical state.
Warning Transaction Response Time	Select this option and provide a criteria and number of seconds if you want to monitor for a warning state. If the time to process the complete set of requests matches this criteria, and the error criteria is not also true, the monitor is set to a warning state.

Performance Counter Tab

Use the **Performance Counter** tab to enable collection of performance counters for the web application. The various options are explained in the following table.

Item	Description
Transaction Response Time	If this option is selected, then the collective time to process all the requests in the browser session is collected.
Request Performance Counters	Select the performance counters that are collected for the application. Any selected counters are collected as an aggregate for all requests in the browser session. Each will also be added to the list of counters for every

Item	Description
	request in the browser session.
Reduction Factor	Select to reduce the number of counters selected for the web application and the requests. It specifies how many query intervals must be completed before each collection. If the value is 1, the counters are collected every time the browser session is run. If it is 2, the counters are only collected every second time the browser session is run, and so on.

See Also

How to Edit Settings or Requests in a Web Application

Web Application Request Properties

Web Application Request Properties

The following sections describe the settings available for each request in a **Web Application Transaction Monitor** template in Operations Manager. You can set the properties of these requests by using the procedure in How to Edit Settings or Requests in a Web Application. Each section in the following sections represents a tab in the **Request Properties** dialog box.

General Tab

Use the **General** tab to specify the general details of the request. The different options are explained in the following table.

Item	Description
Request URL	The URL that you are requesting. You can specify whether the protocol will be http or https.
HTTP Method	The method to use for the request. Most requests use a GET method. The POST method is typically used when selecting an option to submit information to a website, such as clicking a button to submit a name and password.

Item	Description
HTTP Version	The version of HTTP that the request specifies to the receiving website.
Request Body	Only enabled when the **HTTP method** is POST. This is the body of the request that the post submits.
Insert Parameter	There is an **Insert parameter** button for both the **Request URL** and the **Request Body**. Use these options to replace part of the text with a variable that is populated from a previous request. For more information, see How to Replace Parameters in a URL Request.

HTTP Headers Tab

The **HTTP Headers** tab is used to define the different fields that will be included in the header of the request. If the request is from a recorded session, it includes the headers that your browser used. If you manually created the request, it includes a default set of headers and values. You can use the **Edit** button to modify an existing header field or the **Add** button to add a new field. The **Insert parameter** options are used to replace part of the text with a variable that is populated from a previous request. For more information, see How to Replace Parameters in a URL Request.

Performance Counter Tab

The **Performance Counter** tab lets you select the performance counters that will be collected for the request. Any selected counters are added to the list of counters specified in the **Web Application** settings which enable the counter for an aggregate of all requests in a browser session. The value for any selected counter is collected every time that the request is made.

Monitoring

Use the **Monitoring** tab to control certain monitoring settings for the request and to specify the details of the request that will be collected when one of the monitors enters a warning or critical state. You can view this collected information in the **State Change Events** tab of the **Health Explorer** for the monitor. The different options are described in the following table.

Item	Description
Monitor SSL health on secure sites	If the request is using https, monitors that measure the health of the related Secure

Item	Description
	Sockets Layer (SSL) certificates.
Enable health evaluation and performance collection for resources	If selected, a monitor is enabled that displays the status of the resources for the page. Instead of measuring every resource, the total of all resources is evaluated. If this option is not selected, the resource monitor does not function for the request.
Enable health evaluation and performance collection for Internal links	Enables the collection of the status of each internal link and includes internal links in the evaluation of the **Links Status Code** monitor for the request. An internal link is a link that refers to a location on the same page.
Enable health evaluation and performance collection for External Links	Enables the collection of the status of each external link and includes external links in the evaluation of the **Links Status Code** monitor for the request. An external link is a link that refers to a location outside the current page.
Link traversal	Specifies the number of levels of external links to collect. If the value is 0, only the links on the page itself are evaluated. If the value is 1, the links on each target page are evaluated. If the value is 2, the links on those target pages are evaluated, and so on.
Process response body	Specifies whether to evaluate the response body. You must select this value if you want to use content matching or parameter extraction for the request to work. You can clear this option if you only want to perform simple tests for the page such as monitoring status code and response time.
Response body collection	Specifies whether to collect the body of the request response. Select one of the following options: • **Always collect** if you want to collect the response body any time any monitor for the request enters a warning or error state. • **Do not collect** if you never want to collect the response body.

Item	Description
	• **Collect on content match criteria** if you want to collect the response body only when the Content Match monitor enters a warning or critical state.
Collect headers	If selected, the header of the request is collected.
Collect link headers	If selected, the header of each link is collected.
Collect resource headers	If selected, the header of each resource is collected.

Custom Error

The **Custom Error** tab lets you specify error criteria for the request by using information that is not available in the **Request Details** pane of the **Web Application Editor**. You can either provide simple criteria by using a single metric, or you can use multiple metrics to specify complex logic. Use the **Insert** button to add a criterion or a group specifying **AND** or **OR** logic. If the criteria that you specify resolve to `true` when the request is run, the monitor indicates an error for the web application.

Custom Warning

The **Custom Warning** tab lets you specify error criteria for the request by using information that is not available in the **Request Details** pane of the **Web Application Editor**. You can either provide simple criteria by using a single metric, or you can use multiple metrics to specify complex logic. Use the **Insert** button to add a criterion or a group specifying **AND** or **OR** logic. If the criteria that you specify resolve to `true` when the request is run, the monitor indicates a warning for the web application.

Extraction Rules

The **Extraction Rules** tab lets you extract a string of text from the body of the response of the request to use in one or more subsequent requests. For more information, see How to Replace Parameters in a URL Request.

See Also

How to Edit Settings or Requests in a Web Application

Web Application Properties

How to Replace Parameters in a URL Request

When you capture a web application by using the Web Application Editor, it can include unique information in one or more requests that changes each time you connect to the application. This information is typically included in the response to a request and then used by one or more subsequent requests.

For example, an application might create a unique session ID when a user logs on. This session ID must be included in each request after the logon process. Without the correct session ID, each of these requests fails. Because you do not know what this value is until the first request is run, it cannot be explicitly included in the configuration of the request. If you create the web application by recording a browser session, the session ID is collected in the URL of each request. However, when the application is run, the requests fail because the session ID will have a value that is different from the recorded session ID.

To configure such an application, you can extract a context parameter from the body of the response of one request and use the value of that parameter in one or more subsequent requests. You then replace the explicit value in subsequent requests with a variable that represents the parameter. Each time the synthetic transaction is run, the parameter is populated in the request where it is defined. When the variable is used in the subsequent requests, it is replaced with the collected value before the request is sent to the application.

A single application can use any number of context parameters. Any number of requests can use a single parameter but must be run after the request where the parameter is defined.

Session ID Example

Consider the example where an application creates a session ID when a user logs on. This session ID is required in each request after the logon page. To implement this scenario, you have to capture the session ID when it is first generated, and then use that value in each subsequent request.

You start by using the process described in How to Capture Web Application Recording to capture the logon and subsequent actions. The recorded session for logging on to the application and performing some actions might look similar to the following example.

```
http://www.myapp.com/home.aspx

http://www.myapp.com/search.aspx?query=testing&sessionid=32793279321721

http://www.myapp.com/results.aspx?sessionid=32793279321721

http://www.myapp.com/submit.aspx?sessionid=32793279321721
```

In this request sequence, the session ID is created by the first request and used in the second, third, and fourth requests. When you run this monitor, it fails because the first request generates a new session ID that could not match the session ID that was used when the session was captured.

To configure this request sequence with parameter replacement, you have to create an extraction rule on the first request to create a context parameter for the session ID. The extraction rule inspects the body of the request to locate the value for the `sessionid` variable. You would then modify the subsequent requests to use this parameter instead of the value for the session ID.

The modified requests look similar to the following example.

```
http://www.myapp.com/home.aspx

http://www.myapp.com/search.aspx?query=testing&sessionid=$ParametersContext/sessionID$

http://www.myapp.com/results.aspx?sessionid=$ParametersContext/sessionID$

http://www.myapp.com/submit.aspx?sessionid=$ParametersContext/sessionID$
```

Creating an Extraction Rule

Context parameters are collected by an *extraction rule*, and each extraction rule collects a single context parameter. You create an extraction rule in the **Properties** dialog box of the request that initially generates the required data. To identify the value to extract, you must view the body of the response returned from the particular request. You can either view the source of the page returned in the browser or use a tool that lets you inspect the details of HTTP responses. You cannot view the text by using the Web Application Editor.

When you have identified the request that contains the information you have to extract, you view the **Extraction Rules** tab in the properties of that request and create one or more extraction rules. The details of each extraction rule are shown in the following table.

Option	Description
Context parameter name	Enter the name to give the context parameter.
Starts with	Enter the text in the body of the response that identifies the start of the parameter value. You should specify enough characters to ensure that the string is unique. The value for the parameter starts immediately after the last specified character.
Ends with	Enter the text in the body of the response that identifies the end of the parameter value. The value for the parameter ends immediately before the first specified character.
Index	If the text in the **Starts with** box occurs more than one time, this value indicates which value to use. If the text only appears one time, or the first occurrence of it shows the text to extract,

Option	Description
	the value should be 0. If the second value should be extracted, the value should be 1, and so on.
Ignore case during search for matching text	Specifies whether to ignore the case of the characters being searched by the **Starts with** and **Ends with** boxes.
Perform URI encoding of extracted strings	Specifies whether to encode the extracted string after it is collected.

Inserting a Parameter into a Request

You use a parameter in a request by replacing the explicit value with a variable representing the parameter. The format of the variable is `$ParametersContext/<ContextParameterName>$`. When the request is run, the variable is replaced with the data extracted by the parameter.

You can insert the variable into the request by using one of the two following methods:

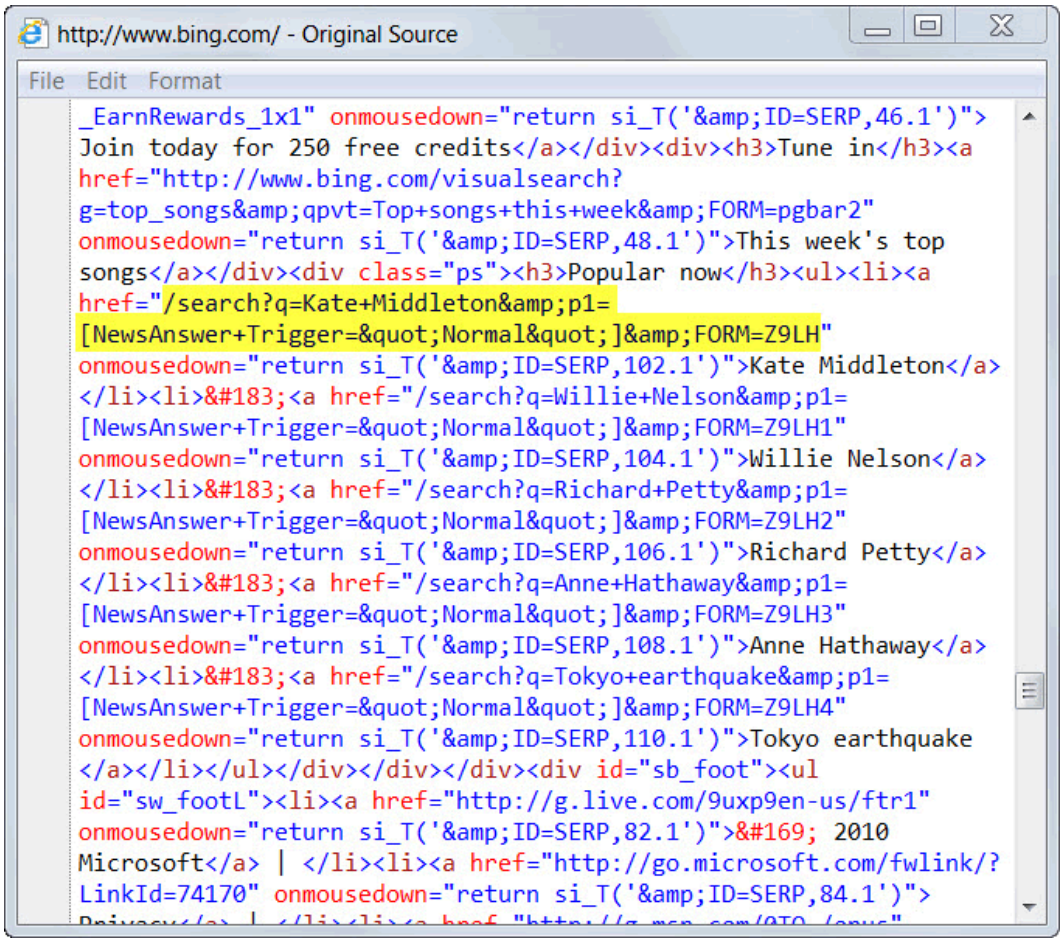
- In the **Request Properties** dialog box, click the **General** tab, and then click **Request URL** to modify the request URL for the request.
- In the **Request Properties** dialog box, click the **General** tab, and then click the **Insert parameter** button. Use the **Insert Parameter** dialog box for the request. This is accessed from the **Insert parameter** button on the **General** tab in the **Request Properties** dialog box for the request.

Sample Web Application Using Parameter Extraction

The following procedure provides an example of using parameter extraction in a web application. This example performs a query for the first entry in the **Popular Now** section of the Bing home page. Because this value changes regularly, you have to first connect to the main page and collect the search term from the body of the response. You then use this term to build the request to perform the actual search.

The main Bing page is shown below with the **Popular Now** section highlighted.

To determine where in the response body the search term appears, you can view the source of the page. A portion of the source is shown below with the HTML code of the **Popular Now** section. In this HTML code, you only need the search string which is highlighted in the following illustration. The request is formed from **http://www.bing.com** followed by this string.

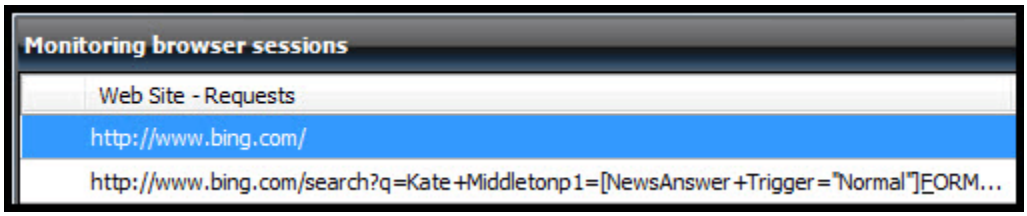


You could just pull out the term itself, but it is more straightforward to include the entire string in the parameter. This string is preceded by the characters **<h3>Popular now</h3>
<a href="** and ends with the next occurrence of **"**. Those are the values that you will use when you define the parameter extraction.

To record a sample web application

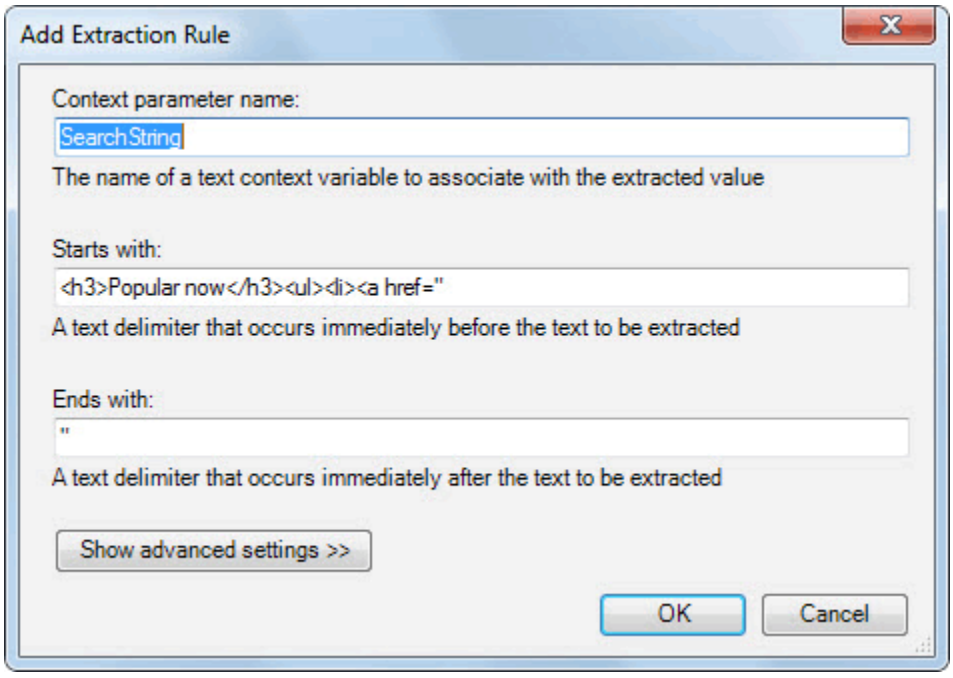
1. Use the procedure in How to Capture Web Application Recording to record a web application.
2. While recording, connect to **http://www.bing.com**.
3. Optionally, use the option on your browser to view the source of the Bing home page and locate the **Popular Now** section of the HTML code.
4. Click the first search term under **Popular Now**.
5. Save the recording to the web application.
6. Remove the last request because this is not required. To remove the last request, select the request, and then click **Delete** in the **Actions** pane. The resulting requests should

look similar to the following URLs:



To create an extraction rule

1. Select the first request, and then click **Properties** in the **Actions** pane.
2. Select the **Extraction Rules** tab.
3. Click **Add**. The **Add Extraction Rule** dialog box opens.
4. In the **Add Extraction Rule** dialog box, in the **Context parameter name** box, type **SearchString**.
5. In the **Starts with** box, type **<h3>Popular now</h3>
<a href="**.
6. In the **Ends with** box, type **"**. The extraction rule should look similar to the following illustration.

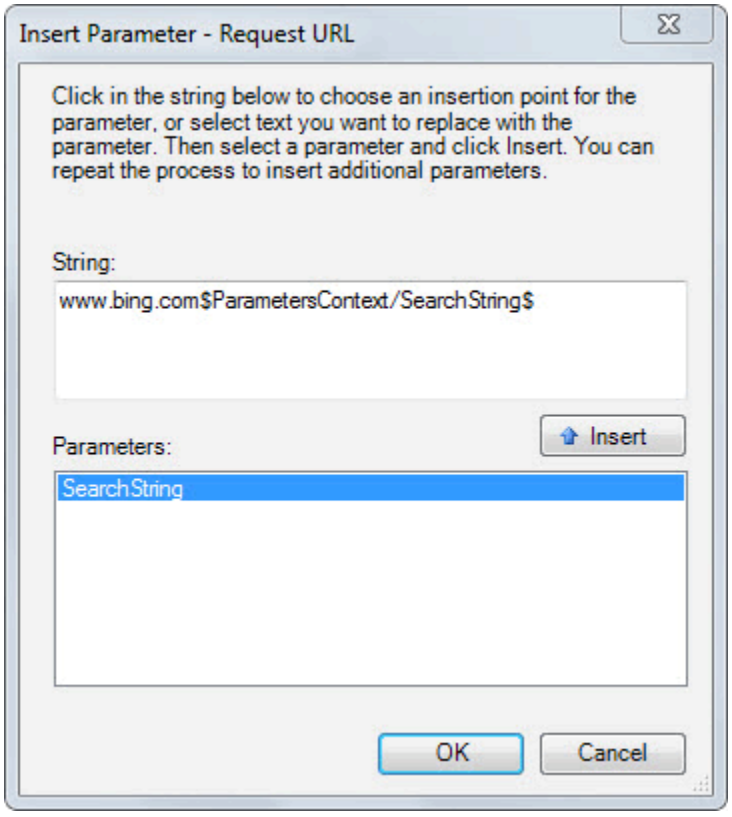


7. Click **OK** to save and close the extraction rule.

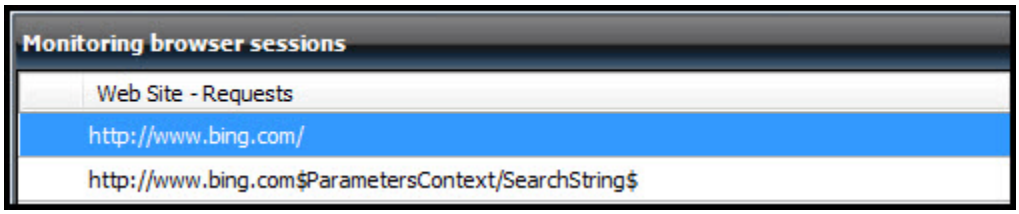
8. Click **OK** to save and close the request.

To insert a parameter into a request

1. Select the second request, and then click **Properties** in the **Actions** pane.
2. On the **General** tab, click **Insert parameter**.
3. In the **String** box, delete all text after **www.bing.com/**.
4. With the cursor positioned at the end of the URL, just after **www.bing.com**, select **SearchString** in the **Parameters** box, and then click **Insert**. This inserts the variable `$ParametersContext/SearchString$`. The final request looks similar to the following illustration.



5. Click **OK** to close the dialog box.
6. Click **OK** to save and close the request. The modified request sequence should look similar to the following illustration.



7. Click **Apply** to apply the changes, and then close the **Web Application Editor**.

Windows Service Template

The *Windows Service* template lets you find and monitor instances of a particular service installed on a Windows-based computer. The template locates computers that are running the service and then applies monitors and rules to test its availability and collect performance data. The only information that you have to provide is the name of the service and the types of monitoring that you want to perform.

Scenarios

Use the **Windows Service** template for any application that uses a service because typically the basic health of the service is critical to the health of the application. You can simply provide the name of the service and have it discovered and monitored on any computer where the application is installed.

Monitoring Performed by Windows Service Template

Depending on your selections in the Windows Service Template wizard, the monitoring performed by the created monitors and rules can include any of the following settings.

Type	Description	Enabled?
Monitors	Running state of the service	Enabled.
	CPU utilization of the service	Enabled if **CPU Usage** monitoring is selected in the wizard.
	Memory usage of the service	Enabled if **Memory Usage** monitoring is selected in the wizard.

Type	Description	Enabled?
Collection Rules	Collection of events indicating a change in service's running states.	Enabled.
	Collection of CPU utilization for the service	Enabled if **CPU Usage** monitoring is selected in the wizard.
	Collection of memory usage for the service	Enabled if **Memory Usage** monitoring is selected in the wizard.
	Collection of Handle Count for the service	Disabled. Can be enabled with an override.
	Collection of Thread Count for the service	Disabled. Can be enabled with an override.
	Collection of Working Set for the service	Disabled. Can be enabled with an override.

Wizard Options

When you run the **Windows Service** template, you have to provide values for options in the following tables. Each table represents a single page in the wizard.

General Options

The following options are available on the **General Options** page of the wizard.

Option	Description
Name	The name used for the service. This name is displayed in the Operations console for the wizard.
Description	Optional description of the service.
Management Pack	Management pack to store the class and monitors that the template creates. If you create any additional monitors or rules that use the service as a target class, they have to be stored in the same management pack. For more information about management

Option	Description
	packs, see Selecting a Management Pack File.

Service Details

The following options are available on the **Service Details** page of the wizard.

Option	Description
Service name	The name of the service. This name is searched on the agent-managed computer to determine whether it is installed.
Targeted group	The service is only discovered on computers that are included in the specified group.
Monitor only automatic service	If selected, only those services that are set to start automatically when Windows starts are monitored. Any services with their startup value set to manual or anything other than Automatic are not monitored.

Performance Data

The following options are available on the **Performance Data** page of the wizard.

Option	Description
Generate an alert if CPU usage exceeds the specified threshold	Specifies if CPU usage should be monitored. A monitor is created to set an error state on the object and generate an alert when the specified threshold is exceeded. A rule is created to collect CPU usage for analysis and reporting.
CPU Usage (percentage)	If CPU usage is monitored, this option sets the threshold. If the percentage of total CPU usage exceeds the threshold, the object is set to an error state and an alert is generated.
Generate an alert if memory usage exceeds the specified threshold	Specifies whether memory usage should be monitored. A monitor is created to set an error state on the object and generate an alert when the specified threshold is exceeded. A rule is created to collect CPU usage for analysis and

Option	Description
	reporting.
Memory Usage (MB)	If memory usage is monitored, this option sets the threshold. If the percentage of total CPU usage exceeds the threshold, the object is set to an error state and an alert is generated.
Number of samples	If CPU usage or memory is monitored, this option specifies the number of consecutive performance samples that must be exceeded before the object is set to an error state and an alert is generated. Specifying a number greater than 1 for this option limits the noise from monitoring by ensuring that an alert is not generated when the service only briefly exceeds the threshold. The larger the value that you set, the longer the period of time before you receive an alert. A typical value is 2 or 3.
Sample Interval	If CPU usage or memory is monitored, this option specifies the length of time between performance samples. A smaller value for this option reduces the time for detecting a problem but increases overhead on the agent and the amount of data collected for reporting. A typical value is between 5 and 15 minutes.

Additional Monitoring

In addition to performing the specified monitoring, the **Windows Service** template creates a class that you can use for additional monitors and workflows. Any monitor or rule that is using this class runs on any agent where the service is installed. If it creates Windows events that indicate an error, for example, you could create a monitor or rule that detects the particular event and uses the service' class as a target.

Creating and Modifying Windows Service Templates

To create a Windows Service template

1. Determine the target group for the monitor by using the following logic:
   - If you want to discover the service on all Windows-based computers in the management group, you do not have to create a group. You can use the existing group **All Windows Computers**.
   - If you only want the service to be discovered on a certain group of computers, either ensure that an appropriate group exists or create a new group by using the procedure in **How to Create Groups in Operations Manager 2012**.
   - If the service you are monitoring is in a cluster, create a group with objects of the class **Virtual Server** representing the nodes of the cluster that contains the service.
2. Start the **Add Monitoring** wizard.
3. On the **Select Monitoring Type** page, select **Windows Service**, and then click **Next**.
4. On the **General Properties** page, in the **Name** and **Description** boxes, type a **name** and description for this new monitor.
5. Select a management pack in which to save the monitor, or click **New** to create a new management pack. For more information, see Selecting a Management Pack File.
6. Click **Next**.
7. In the **Service Name** box, type the name of the specific service that you want to monitor, or click the ellipse (**…**) button to browse for the service. You can select any computer that has the service installed.
8. Under **Targeted Group**, specify the group from step 1 of this procedure.
9. Clear the **Monitor only automatic services** option if you want the monitor to apply to services that are not configured to start automatically. If the service that you are monitoring is in a cluster, clear this option.
10. Click **Next**.
11. Select the performance counters and thresholds that you want to monitor. For more detailed information, see the Wizard Options section.
12. If you have selected performance counters, specify the monitoring interval.
13. Click **Next**.
14. Review the summary of the monitor, and then click **Create**.

To modify an existing Windows Service template

1. Open the Operations console with a user account that has Author credentials.
2. Open the **Authoring** workspace.
3. In the **Authoring** navigation pane, expand **Management Pack Templates**, and then select **Windows Service**.
4. In the **Windows Service** pane, locate the monitor to change.
5. Right-click the monitor, and then select **Properties**.
6. Enter the changes that you want, and then click **OK**.

Viewing Windows Service Monitors and Collected Data

To view all Windows Service monitors

1. Open the Operations console.
2. Open the **Monitoring** workspace.
3. In the **Monitoring** navigation pane, select **Windows Service and Process Monitoring**, and then click **Windows Service State**.

To view the state of each monitor

1. In the **Windows Service State** pane, right-click an object. Select **Open**, and then click **Health Explorer**.
2. Expand the **Availability** and **Performance** nodes to view the individual monitors.

To view the performance collected for a service

1. In the **Windows Service State** pane, right-click an object. Select **Open**, and then click **Performance**.
2. In the **Legend** pane, select the counters that you want to view.
3. Use options in the **Actions** pane to modify the Performance view.

Monitors and Rules

Monitors and rules are the primary elements for measuring health and detecting errors in Operations Manager and provide similar yet distinct functionality. Monitors set the state of an object while rules create alerts and collect data for analysis and reporting. Each monitor and rule is primarily defined by the source of the data that is used to perform its required functionality and the logic used to evaluate this data.

Although they provide different functionality, monitors and rules both use a common set of sources that provide the data to evaluate. For example, a monitor may use a performance counter to set the state of a particular object. A rule may access the same performance counter in order to store its value for analysis and reporting.

Monitors

A monitor measures the health of some aspect of a managed object. There are three kinds of monitors as shown in the following table:

Health State

Monitors each have either two or three health states. A monitor will be in one and only one of its potential states at any given time. When a monitor loaded by the agent, it is initialized to a healthy state. The state will change only if the specified conditions for another state are detected.

The overall health of a particular object is determined from the health of each of its monitors. This will be a combination of monitors targeted directly at the object, monitors target at objects rolling up to the object through a dependency monitor, dependency monitors targeted at those objects, and so on. This hierarchy is illustrated in the Health Explorer of the Operations console. The policy for how health is rolled up is part of the configuration of the aggregate and dependency monitors.

When you create a monitor, you must specify a condition for each of its health states. When one of those conditions is met, the monitor changes to that state. Each of the conditions must be unique such that only one can be true at a particular time. When a monitor changes to a Warning or Critical state, then it can optionally generate an alert. When it changes to a Healthy state, then any previously generated alert can optionally be automatically resolved.

Types of Monitors

Monitor	Description
Unit Monitors	Measures some aspect of the application. This might be checking a performance counter to determine the performance of the application, running a script to perform a synthetic transaction, or watch for an event that indicates an error. Classes will typically have multiple unit monitors targeted at them to test different features of the application and to monitor for different problems.
Dependency Monitors	Provides health rollup between different classes. This allows the health of an object to depend on the health of another kind of object that it relies on for successful operation.
Aggregate Monitors	Provides a combined health state for similar monitors. Unit and dependency monitors will typically be configured under a particular aggregate monitor. In addition to providing better general organization of the many different monitors targeted at a particular class, aggregate monitors provide a unique health

Monitor	Description
	state for different categories of the class.

Note

When the term *monitor* is alone, it typically refers to a unit monitor. Aggregate and dependency monitors will typically be referred to with their full name.

The following diagram shows an example of the Health Explorer for the **Windows Server** class. This shows the use of the different kinds of monitors contributing to an overall health state.

Sample Health Explorer

Rules

Rules do not affect the health state of the target object. They are used for one of three functions as described in the following table:

Monitor	Description
Alerting Rules	Alerting rules create an alert when a particular event is detected. This can be any of the different kinds of events shown in Data Sources. Alerting rules do not affect health state.

Monitor	Description
Collection Rules	Collection rules collect events or performance data to the Operations Manager database and data warehouse. They do not create alerts or set health state. Collection rules can use each of the data sources shown in Data Sources. The data will be converted to either an event or to performance data depending on the particular kind of collection rule you are creating. For some wizards, you will need to provide the specific information from the data source that will be used for different properties of the data being collected.
Command Rules	Command rules will run a script or command on a schedule. They do not create alerts or collect any data.

Should you create a monitor or a rule?

Unit monitors and rules in Operations Manager are similar. They are both workflows that run on an agent, they both can generate an alert when a particular condition is met, and they both use a similar set of data sources to detect these conditions. As a result, it can be difficult to determine if you want to create a monitor or rule for a particular scenario.

Use the following criteria to determine which one to create for different conditions.

Create a monitor if…

- You want to affect the health of an object. In addition to generating an alert, a monitor will affect the health state of its target object. This is displayed in state views and availability reports.
- You want to automatically resolve an alert when the error condition has been cleared. An alert from a rule cannot be automatically cleared since a rule has no way of detecting that the problem has been resolved. A monitor can detect that the problem has been resolved when the condition for its healthy state is met, and the alert can automatically be resolved.
- You are creating an alert based on a performance threshold. There are no rules available to generate an alert from a performance threshold. A monitor should be used for this scenario anyway since you can use the condition where the performance counter is under the defined threshold.
- You have a condition that requires more complex logic than is possible with rules. The Operations console provides a variety of options for setting the health state of a monitor but

only simple detection for a rule. If you need more complex logic for a rule but don't have a method to detect the monitor's healthy state, then you can create a monitor using Manual or Timer reset. See Event Monitor Reset for more information.

Note
Using the Viso Management Pack Designer you can create custom rules using the same logic available in the Operations console for monitors.

Create a Rule if…

- You want to collect performance counters or events for analysis and reporting. Monitors only collect this information when it initiates a change in health state. If you want to collect the information you need to create a collection rule.

  If you want to both collect a performance counter and set a threshold for it to set a health state, then create both a rule and a monitor using the same performance counter.
- You want to generate an alert that is not related to health state of an object.

Monitors and Rules Topics

Monitors and rules are described in the following topics.

- Data Sources

  Describes the concept of a data source and lists the different kinds of data sources available for monitors and rules.
- Expressions

  Describes how to create an expression for different kinds of monitors and rules.
- Alerts

  Describes how to configure alerts created by monitors and rules.
- Event Monitors and Rules

  Describes monitors and rules that use different kinds of events and provides details and procedures for creating them using wizards in the Operations console.
- Performance Monitors and Rules

  Describes monitors and rules that collect and monitor performance and provides details and procedures for creating them using wizards in the Operations console.
- Script Monitors and Rules

  Provides the details of how to write a monitoring script and how to create monitors and rules using scripts.
- Dependency Monitors

  Describes monitors that allow the health of one kind of object to be dependent on the health of another object.
- Aggregate Monitors

Describes monitors that consolidate the health of other monitors for a particular kind of object.

Data Sources

Monitors and rules in Operations Manager each start with a *data source* which defines where it will get the data to evaluate or collect. The first decision to make when you are defining a rule or monitor is the data source that it will use. The most straightforward method to answer this question is to determine where the information is that you want to collect or that indicates the condition you want to detect.

For example, an application may create an event in the Windows Event Log when a particular error occurs. You could create a rule that watches for this particular event and generates an alert when it detects one. If detection of the event is not possible through an event, a log, or a performance counter, then you may need to run a script on a periodic basis to retrieve the required information.

The same set of data sources is available for both monitors and rules as shown in the table below.

Type	Data Source		Description
Event Monitors and Rules	Windows Events		Events in the Windows event log matching specified criteria.
	Text Logs		Text log file that has a single line per entry.
	WMI Events		Events created by Windows Management Instrumentation (WMI).
	SNMP Events		Traps sent from an SNMP device.
	Syslog Events		Events from Unix systems and other devices.
Performance Monitors and Rules	Windows Performance Collection Rules		Monitor a threshold or collect a performance value from Windows.
	WMI Performance	Monitor a threshold or collect a performance value from a WMI	

Type	Data Source		Description
		query.	
Script Monitors and Rules	Script Monitors	Monitor a value from a script that runs on a schedule.	
	Script Collection Rules	Collect events or performance data from a script that runs on a schedule.	

Expressions

Wizards for creating monitors and rules will often require you to enter an expression that specifies criteria for the data being collected. The monitor or rule will only apply if the expression is true.

For example, you might have a rule that creates an alert for a particular event. You don't want an alert for every single event that writes to the event log, so you specify the event number and event source in the expression. The rule will analyze all events that are written to the event log, but it will only generate an alert for those events with the specified source and number.

An expression may be simple with only a single criterion, or it may be a compound expression with multiple criteria and complex logic. Most expressions that you create will have only one or two criteria with very few using complex logic.

The syntax that you use for the expression will be different for different kinds of data sources. For some data source, you will be able to select criteria for a dialog box which keeps you from having to understand the underlying syntax. For other data sources, you will have to know the appropriate syntax and type it in. The following sections provide you with the details of the criteria for each data source.

Criteria Syntax

A single piece of criteria is comprised of a *Parameter Name*, an *Operator*, and a *Value*. Each of these is described in detail in the following sections.

Parameter Name

The *parameter name* specifies a parameter from the data source for the rule or monitor. The syntax of the parameter name will be different depending on the type of data being collected. The syntax of the parameter name will be different depending on the type of data being collected.

The sections below provide the parameter name syntax for different kinds of data sources.

Windows Events

Windows events provide a prompt in the expression dialog box to select individual properties so you will typically not have to understand the actual syntax. The list of properties with their description is at Windows Events.

Event Description is not included in the dropdown list for property name. It can be used by typing in **EventDescription**. Before using Event Description though, you should verify whether the information that you are using in the description is available in parameters. Event descriptions are often made up of standard text with unique information included through parameters. Parameters are more efficient that the full description since they contain a specific piece of information.

Text Logs

Text Logs do not provide a prompt for the parameter name, so you need to type it in using the appropriate syntax. There are two types of text logs: Generic Text Logs where each line is processed as a single entry and Generic CSV Text Logs which use a delimiter to separate the fields of each entry.

For a Generic Text Log, the entire entry is referred to with a single parameter using the following syntax:

```
Params/Param[1]
```

For a Generic CSV Text Log, each field of the entry is referred to with a separate parameter for each field of the entry using the following syntax where # refers to the number of the field starting with 1:

```
Params/Param[#]
```

Further details on text log expressions are available at Text Log Expressions.

WMI Events

WMI Events do not provide a prompt for the parameter name, so you need to type it in using the appropriate syntax.

The properties available for a WMI event will vary, depending on the kind of event being monitored. The data will be in the form of a property bag that has a collection of properties for one or more WMI class instances. WMI events created by using a query that uses either __InstanceCreationEvent or __InstanceDeletionEvent will have a single collection called TargetInstance with the instance being either created or deleted. WMI events created by using __InstanceModificationEvent will have an additional collection called PreviousInstance.

The syntax for properties from a WMI event is as follows:

```
Collection[@Name='TargetInstance']/Property[@Name='Caption']
```

Further details on WMI Events are available at WMI Events.

Syslog Events

Syslog Events do not provide a prompt for the parameter name, so you need to type it in using the appropriate syntax. The syntax for the properties of a syslog event is simply the name of the property. These properties are listed in Syslog Events.

SNMP Events

SNMP probes and traps do not provide a prompt for the parameter name, so you need to type it in using the appropriate syntax. The syntax for the properties in the header of an SNMP probe or trap is simply the name of the property.

When a single OID is used:

SnmpVarBinds/SnmpVarBind/ElementName

When you have multiple OIDs and want to refer to each by its numeric order. The first OID is 1, the second is 2, and so on:

SnmpVarBinds/SnmpVarBind[#]/ElementName

When you have multiple OIDs and want to refer to each by the specific OID:

SnmpVarBinds/SnmpVarBind[OID="OID"]/ElementName

Further details on SNMP events are listed in SNMP Events.

Scripts

Scripts do not provide a prompt for the parameter name, so you need to type it in using the appropriate syntax. Monitoring scripts output information in the form of a property bag that includes one or more values. The parameter specifies the name of one of the values from the property bag using the following syntax:

Property[@Name="PropertyName"]

Further details on monitoring scripts are available at Script Monitors and Rules.

Operator

The *operator* specifies the comparison that will be performed between the value from the data property specified in **Parameter Name** and the value specified in **Value**. Possible values are shown in the following table.

Operator	Description
Equals	The string or number specified in the data is exactly equal to the string or number specified in Value. If this is a string value, the comparison is not case sensitive.
Does not equal	The string or number specified in the data is not exactly equal to the string or number specified

Operator	Description
	in Value. If this is a string value, the comparison is not case sensitive.
Greater than	The value in the data is greater than the number specified in Value.
Greater than or equal to	The value in the data is greater than or equal to the number specified in Value.
Less than	The value in the data is less than the number specified in Value.
Less than or equal to	The value in the data is less than or equal to the number specified in Value.
Contains	The string specified in Value appears somewhere in the data.
Does not contain	The string specified in Value does not appear somewhere in the data.
Matches wildcard	The string specified in Value matches the string including wildcard. The wildcard character is * and represents any number of characters.
Does not match wildcard	The string specified in Value does not match the string including wildcard. The wildcard character is * and represents any number of characters.
Matches regular expression	The string in the data matches the regular expression specified in Value.
Does not match regular expression	The string in the data does not match the regular expression specified in Value.

Value

The value can be specific text or a number typed into the Value field. For example, a particular event might be defined by its source and number. These are both constant values that can be typed into the Value field.

A value can also come from a property on the target object. Any property on the target object or on any of the object's parents can be used. You can view a list of the properties and their values for any object by viewing the object in the **Discovered Inventory** view.

Target properties have different values for different objects. For example, you might use **Logical Disk (Server)** as a target and require the total size of the disk in the criteria. Logical disks have a

property called **Size (Mbytes)** that stores the total size of the disk. The value of this property will be different for different disks in the management group. When you use a target variable for the value, it will be evaluated separately for each object.

You can select a target property by clicking the ellipse button on the right of the criteria line. This will display a list of all available properties for the object that you selected for the target and that objects parents. If you select one of these properties, the appropriate target variable will be added to the criteria.

Examples

Windows Events

The following expression identifies a Windows event with a source of Contoso and an event number of 100.

Parameter Name	Operator	Value
AND group (all of these are true)		
Event ID	Equals	100
Event Source	Equals	Contoso

The following expression identifies a Windows event with a source of Contoso, an event number of 100, and the word “Error” in parameter 1.

Parameter Name	Operator	Value
AND group (all of these are true)		
Event ID	Equals	100
Event Source	Equals	Contoso
Parameter 1	Equals	Error

The following expression identifies a Windows event with a source of Contoso, an event number of 100, and the word “Error” anywhere in the description.

Parameter Name	Operator	Value
AND group (all of these are true)		

Parameter Name	Operator	Value
Event ID	Equals	100
Event Source	Equals	Contoso
EventDescription	Contains	Error

Text Logs

The following expression identifies an entry in a generic text log that contains the word “Error”.

Parameter Name	Operator	Value
Params/Param[1]	Contains	Error

The following expression identifies an entry in a generic csv text log that contains the word “Error” in the third field.

Parameter Name	Operator	Value
Params/Param[3]	Equals	Error

Scripts

The following expression identifies a numeric value from a script called “PerfValue” that is between 10 and 20.

Parameter Name	Operator	Value
AND group (all of these are true)		
Property[@Name="PerfValue"]	Greater than	10
Property[@Name="PerfValue"]	Less than	20

Alerts

Alerts in Operations Manager can be generated from either monitors or rules. While the Operations console does not distinguish between each type, there are distinct differences between the two that you should understand when defining monitors and rules. The sections

below provide the alert properties that you will need to define when you configure a monitor to generate an alert or if you create an alerting rule.

Alerts from Monitors

An alert will only be generated from a monitor if each of the following is true:

- The monitor is configured to generate an alert.
- The health state of the monitor changed from a Healthy State to a Warning or Error state, depending on the possible health states of the monitor.
- An open alert does not already exist for the same object created by the same monitor.

Alerts are only generated from a monitor when the health state of the monitor changes from a Healthy state. Even though the criteria for the error condition may occur multiple times, multiple alerts will not be generated once the health state of the monitor is set to Warning or Critical. Only after the health state of the monitor returns to Healthy and the error condition occurs again will a new alert be generated.

For example, consider a Windows Event monitor that is configured to set a Critical state when an event with number 101 is detected and reset the monitor when an event with number 100 is detected. When the first event 101 is created, the monitor is set to a Critical state and an alert is generated. Even though you may close the alert, if an additional event 101 is detected a new alert is not created because the monitor did not change its state. Only after the monitor is reset, either by detecting an event 100 or by you manually resetting it, and an event 101 is detected will an alert be generated.

Alert Name

The name of the alert is a single line of static text and cannot include any variables.

Priority and Severity

The Alert severity defines the alert as either Information, Warning, or Critical. This severity does not have to match the severity of the health state triggering the alert. The severity of the alert is identified by an icon in the Operations console and is used by views and notification subscriptions. The alert priority is inaccessible in the Operations console but is used primarily for notification subscriptions.

Alert Description

The alert description may have several lines of text that includes a combination of static text and variables. The most common kind of variable in the alert description will be $Data variables to include different information from the monitor's data source in the description of the alert. The properties that are available will depend on the kind of data source being used.

The table below provides syntax and examples of variables in alerts created from monitors.

Data Source	Syntax	Examples
Windows Event	$Data/Context/<Property Name>$	$Data/Context/EventDescription$
	$Data/Context/Params/Param[#]$	$Data/Context/Params/Param[2]$
Text Log	$Data/Context/<Property Name>$	$Data/Context/LogFileName$
	$Data/Context/Params/Param[1]$	$Data/Context/Params/Param[1]$
Delimited Text Log	$Data/Context/<Property Name>$	$Data/Context/LogFileName$
	$Data/Context/Params/Param[#]$	$Data/Context/Params/Param[2]$
WMI Event	$Data/Context/Collection[@Name='<TargetInstance\|PreviousInstance>']/Property[@Name='<PropertyName>']$	$Data/Context/Collection[@Name='TargetInstance']/Property[@Name='Name']$
Windows Performance	$Data/Context/<PropertyName>]$	$Data/Context/Value$
WMI Performance	$Data/Context/<PropertyName>]$	$Data/Context/Value$
Monitoring Script	$Data/Context/Property[@Name='<PropertyName>']$	$Data/Context/Property[@Name='Result'>']$

Automatic Alert Resolution

Monitors that create alerts can be configured to automatically resolve the alert when the monitor returns to a healthy state. This means that any unresolved alert for the monitor represents a problem that still exists. There is no configuration this requirement other than confirming the option that automatic resolution be performed.

Note
Automatic alert resolution cannot be performed with rules because rules do not have any means of detecting that the problem has been corrected.

Alerts from Rules

An alert will only be generated from a rule under the following conditions:

- The rule is configured to generate an alert.
- The criteria defined in the rule is true.
- An open alert does not already exist that matches the alert's suppression configuration.

The table below discusses the ability of each type of rule to generate an alert.

Rule Type	Alert Capabilities
Event Rules	Alert rules can be created for each event data source. The criteria that is specified to determine when an alert should be created is the same as the criteria for a state change in the event monitors.
Performance Rules	You cannot create an alert rule based on a performance counter. A monitor should be used instead because a success condition is usually detectable from a performance counter and is usually related to some health state of the target class.
Scripting Rules	You cannot create an alert rule based on a script. A monitor should be used instead because a script will typically provide a return value for both and error and a healthy state in such a way that a success condition is usually detectable and related to some health state of the target class.

Alert Name

The name of the alert is a single line of static text and cannot include any variables.

Priority and Severity

The Alert severity defines the alert as either Information, Warning, or Critical. This severity does not have to match the severity of the health state triggering the alert. The severity of the alert is identified by an icon in the Operations console and is used by views and notification subscriptions. The alert priority is inaccessible in the Operations console but is used primarily for notification subscriptions.

Alert Description

The alert description may have several lines of text that includes static text or variables. The most common kind of variable in the alert description will be $Data variables to include different information from the rule's data source in the description of the alert. The properties that are available will depend on the kind of data source being used. Each section of Data Sources includes a list of the properties available for different data sources.

The following table provides syntax and examples of variables in alerts created from rules:

Data Source	Syntax	Examples
Windows Event	$Data/<Property Name>$	$Data/EventDescription$
	$Data/Params/Param[#]$	$Data/Params/Param[2]$
Text Log	$Data/EventData/DataItem/<PropertyName>$	$Data/EventData/DataItem/LogFileName$
	$Data/EventData/DataItem/Params/Param[1]$	$Data/EventData/DataItem/Params/Param[1]$
Delimited Text Log	$Data/EventData/DataItem/<PropertyName>$	$Data/EventData/DataItem/LogFileName$
	$Data/EventData/DataItem/Params/Param[#]$	$Data/EventData/DataItem/Params/Param[2]$
WMI Event	$Data/EventData/DataItem/Collection[@Name='<TargetInstance \| PreviousInstance>']/Property[@Name='<PropertyName>']$	$Data/EventData/DataItem/Collection[@Name='TargetInstance']/Property[@Name='Name']$
Syslog Event	$Data/EventData/DataItem/<PropertyName>$	$Data/EventData/DataItem/Facility$

Alert Suppression

Alert suppression refers to logic that is defined on alert rules to suppress the creation of an alert when a corresponding alert is still open. This prevents alert storms where multiple alerts are created for the same issue. Because the issue has already been identified with an open alert,

creation of additional alert creates unnecessary noise with minimal value. When the condition for an alerting rule is met but an existing alert is already open, instead of creating an additional alert suppression will increase the repeat count of the existing alert.

In order to define suppression on an alerting rule, the fields must be specified that identify a matching alert. Before an alerting rule creates a new alert, it will check whether an open alert exists with values for the fields that are defined for suppression that match the values in the same fields of the new alert. If an alert with matching values for each of these fields is open, then a new alert is not created.

The minimum number of fields that uniquely identify the alert should be specified for alert suppression. This will typically be the computer name in addition to the fields used for the criteria of the rule. For example, suppression on event rules can frequently be achieved by using the following fields:

- Logging Computer
- Event Source
- Event Number

If the rule is targeted at a class that has multiple instances on an agent, however, then a parameter might be required to uniquely identify the event in the criteria of the rule. If this is the case, then the same parameter should be specified in the alert suppression.

Note

Alert suppression is not available for monitors because it is not required. Monitors only generate alerts when their state changes from healthy to warning or critical. Even if the detected issue occurs again when the monitor is already in the negative state, then no alert is generated because the monitor state does not change. A new alert is only generated if the monitor returns to a healthy state before the problem occurs.

Event Monitors and Rules

Event monitors and rules rely on the application they are monitoring to create an event of some kind in response to a problem or other interesting occurrence. The monitor or rule continuously watches the data source for an event matching specific criteria and immediately takes an appropriate response. The basic logic and configuration of event rules and monitors are similar except for the initial configuration of the data source that they are retrieving the event from.

Types of Event Monitors and Rules

The table below lists the kinds of events that can be used for monitors and rules in an Operations Manager management pack. Each is discussed in more detail in their own topic.

- Windows Events

  Events in a Windows event log.

- Text Logs

Text log file that has a single line per entry. The log can be a simple text log where each line is considered a single entry or a delimited text log where a single character is used to separate different fields of data.

- WMI Events

  Events created by Windows Management Instrumentation (WMI).
- Syslog Events

  Events from Unix systems and other devices that send syslog messages.
- SNMP Events

  SNMP traps that are sent to an agent or SNMP probes that are periodic requests for information from a device.
- UNIX/Linux Shell Command Alerts

  Events that are detected through the execution of an UNIX/Linux command, script, or one-line sequence of multiple commands (using pipeline operators).

Windows Events

Many Windows-based applications post information to events in a Windows event log. This could be a standard log such as **Application** or a log specific to the application being monitored. These events follow a standard format and frequently contain detailed information about the particular issue. If the application you are monitoring creates a Windows event in response to a particular issue, then this likely be the most effective way to detect the issue in an Operations Manager management pack.

When you create a rule or monitor that uses a Windows event, Operations Manager continuously monitors the log and immediately responds when an event matching the specified criteria is detected. These events are persisted meaning that they are available after they are initially created. Operations Manager will record the last position that it read in the log and continue from that position the next time it reads the log. If the health service on the agent is not running when a particular event is created, Operations Manager will detect it the next time that the agent is started.

Windows Event Wizards

The table below lists the wizards that are available for Windows events.

Management Pack Object	Wizards Available
Monitors	Simple Event Detection using each of the standard Event Monitor Reset methods
	Repeated Event Detection using each of the standard Event Monitor Reset methods

Management Pack Object	Wizards Available
	Missing Event Detection using each of the standard Event Monitor Reset methods
	Correlated Event Detection using each of the standard Event Monitor Reset methods
	Correlated Missing Event Detection using each of the standard Event Monitor Reset methods
Rules	Alert Generating Windows event rule
	Event collection Windows event rule

Windows Event Wizard Options

When you run a Windows event rule or monitor wizard, you will need to provide values for options in the following tables. Each table represents a single page in the wizard.

General

The **General** page includes general settings for the rule or wizard including its name, category, target, and the management pack file to store it in.

Option	Description
Name	The name used for the rule or monitor. For a rule, the name appears in the **Rules** view in the **Authoring** pane. When you create a view or report, you can select this name to use the data collected by it. For a monitor, the name appears in the Health Explorer of any target objects.
Description	Optional description of the rule or monitor.
Management Pack	Management pack file to store the rule or monitor. For more information on management packs, see Selecting a Management Pack File.
Rule Category (Rules only)	The category for the rule. For an event collection rule, this should be **Event Collection**. For an alerting rule, this should be **Alert**.

Option	Description
Parent Monitor (Monitors only)	The aggregate monitor that the monitor will be positioned under in the Health Explorer. For more information, see Aggregate Monitors.
Target	The class to use for the target of the rule or monitor. The rule or monitor will be run on any agent that has at least one instance of this class. For more information on targets, see Understanding Classes and Objects.
Rule is enabled Monitor is enabled	Specifies whether the rule or monitor is enabled.

Event Log Type

The **Event Log Type** page includes the name of the event log where you expect the event to be created. There will be a single **Event Log Type** page for a collection or alerting rule and for a monitor using manual or timer reset. For a monitor using **Windows Event Reset**, you will have to define the log for both the error condition and for the healthy condition. You will typically specify the same log for both conditions, but a different log could be used for each.

You can type in the name of the event log in the **Log name** box, or you can click the ellipse button and select a log.

Event Expression

In addition to the name of the log to retrieve events from, workflows using a Windows event must specify sufficient criteria to identify the particular events that relate to the issue being identified. Frequently, the **Event ID** and the **Event Source** will be sufficient for this purpose. This depends on the kind of information that the application provides in the particular event in addition to the target that is being used for the monitor. If the class being used as the target for the monitor is expected to have multiple instances on a particular agent, then these two properties are probably insufficient for uniqueness. Unless the criteria included a key property for the target class then the criteria would possibly apply to all instances.

There will be a single **Event Log Type** page for each Event Log Type Page collection or alerting rule and for a monitor using manual or timer reset. For a monitor using **Windows Event Reset**, you will have to define the log for both the error condition and for the healthy condition. You will typically specify the same log for both conditions, but a different log could be used for each.

The following table lists the properties available from Windows Events. These properties can be accessed for setting criteria in monitors and rules and can be included in alert descriptions.

Expression	Description
Event Source	Source of the event. Generally used in the criteria of the monitor or rule.
Logname/Channel	Name of the event log such as Application or System.
Logging Computer	Name of the computer logging the event.
Event ID	Number of the event.
Event Category	Category of the event.
Event Level	Severity of the event that uses one of the following values. Success (0) Error (1) Warning (2) Information (4) Success Audit (8) Failure Audit (16)
User	Name of the user account that was used to create the event.
EventDescription	Full event description.
Parameter	Collection of event parameters.

Auto Reset Timer

The **Auto Reset Timer** page is only available for timer reset monitors. It allows you to set the time that must pass after the alert is created before the alert is automatically resolved.

Configure Health

The **Configure Health** page is only available for monitors. It allows you to specify the health state that will be set for each of the events. For a manual reset monitor, the **Manual Reset** condition will be **Healthy**, and you can specify whether the **Event Raised** condition will set the monitor to a **Warning** or a **Critical** state. For a **Timer Reset** or a **Windows Event Reset**, you can specify the health state set by each event. The first event will typically set the monitor to **Warning** or **Critical** while the second event or the timer will set the monitor to **Healthy**.

Configure Alerts

The **Configure Alerts** page is only available for monitors and alerting rules. Its options are explained in Alerts.

Creating Windows Event Monitors

How to create a Windows event monitor

Use the following procedure to create an event monitor in Operations Manager with the following details:

- Runs on all agents with a particular service installed.
- Sets the monitor to a **critical** state when an event in the **Application** event log with an event source of **EventCreate**and an event number of **101** is detected.
- Sets the monitor to a **healthy** state when an event in the **Application** event log with an event source of **EventCreate**and an event number of **102** is detected.

Note
EventCreate is used as the event source so that the EventCreate utility can be used to create a test event. This utility is available on any Windows Computer and creates test events with a source of **EventCreate**. If you have another method of creating test events, then you can use a different source.

To create an event monitor

1. If you don't have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. Create a new target using the process in To create a Windows Service template. You can use any service installed on a test agent for this template.
3. In the Operations console, select the **Authoring** workspace.
4. Select **Management Pack Objects**.
5. Right-click **Monitors**, select **Create and Monitor**, and then select **Unit Monitor**.
6. On the **Monitor Type** page, do the following:
    a. In the **Select the type of monitor to create** box, expand **Windows Events** and then **Simple Event Detection**.
    b. Select **Windows Event Reset**.
    c. In the **Management Pack** dropdown list, select the management pack for the application.
    d. Click **Next**.
7. On the **General** page, do the following:
    a. In the **Name** box, type **Error event 101** or another name for the monitor. This is the text that will appear in the Health Explorer.

b. Click **Select**.
c. In the **Select Items to Target** dialog box, select the name that you used for the Windows Service template in step 2.
d. The **Parent monitor** box should show **Availability**. You can select a different parent monitor.
e. Ensure that **Availability** is selected for the **Parent monitor**.
f. The **Monitor is enabled** box should be checked so that the monitor is enabled.
g. Click **Next**.

8. On the **Event Log (Unhealthy Event)** page, do the following:
   a. In the **Log Name** box, keep the default value of **Application**.
   b. Click **Next**.
9. On the **Event Expression (Unhealthy Event)** page, do the following:
   a. For the **Event ID** value, type **101**
   b. For the **Event Source** value, type **EventCreate**
   c. Click **Next**.
10. On the **Event Log (Healthy Event)** page, do the following:
    a. In the **Log Name** box, keep the default value of **Application**.
    b. Click **Next**.
11. On the **Event Expression (Healthy Event)** page, do the following:
    a. For the **Event ID** value, type **102**
    b. For the **Event Source** value, type **EventCreate**
    c. Click **Next**.
12. On the **Configure Health** page, do the following:
    a. For **FirstEventRaised**, change the **Health State** to **Critical**.
    b. For the **Event Source** value, type **EventCreate**
    c. Click **Next**.
13. On the **Configure Alerts** page, do the following:
    a. Select **Generate alerts for this monitor**.
    b. Click **Create**.

See Also

Event Monitors and Rules

Event Monitor Logic

Event Monitor Reset

Alerts

Text Logs

A *text log* is a text file that an application uses to log event information. In order to use a text log data source in a management pack, each entry in the log must be on a single line. If the log file does not fit this requirement, then a Script Monitors and Rules has to be created to read the log.

Applications that use log files frequently create a new file each day or when one file reaches a certain size. To support this functionality, monitors and rules specify a **Directory** and a **Pattern** for the text logs being monitored. Directory is the path of the directory where the text logs will be located. This must be an absolute path without wildcard characters. A $Target variable could also be used if the path to the log files is stored in a property of the target class. Pattern is the name of the log file including wildcard characters as appropriate.

For example, an application might create a log file each day with the date included in the name as in **log20100316.txt**. A pattern for such a log might be **log*.txt** which would apply to any log file following the application's naming scheme.

A text log can be defined as either a *Generic Text Log* or *Generic CSV Text Log*. CSV refers to Comma Separated Values, although you can specify any character as the delimiter. The two kinds of files are also referred as a *Simple Text Log* and a *Delimited Text Log*. With a simple text log, each line is considered a single entry. With a delimited text log, a single character is used to separate different fields of data, and each field can be analyzed separately.

Text Log Wizards

The table below lists the wizards that are available for both simple and delimited text files.

Management Pack Object	Wizards Available
Monitors	Simple Event Detection using each of the standard Event Monitor Reset methods
	Repeated Event Detection using each of the standard Event Monitor Reset methods
Rules	Alert Generating rule
	Event collection rule

Text Log Wizard Options

When you run a text log wizard, you will need to provide values for options in the following tables. Each table represents a single page in the wizard.

General

The **General** page includes general settings for the rule or wizard including its name, category, target, and the management pack file to store it in.

Option	Description
Name	The name used for the rule or monitor. For a rule, the name appears in the **Rules** view in the **Authoring** pane. When you create a view or report, you can select this name to use the data collected by it. For a monitor, the name appears in the Health Explorer of any target objects.
Description	Optional description of the rule or monitor.
Management Pack	Management pack to store the rule. For more information on management packs, see Selecting a Management Pack File.
Rule Category (Rules only)	The category for the rule. For a collection rule, this should be **Event Collection**. For an alerting rule, this should be **Alert**.
Parent Monitor (Monitors only)	The aggregate monitor that the monitor will be positioned under in the Health Explorer. For more information, see Aggregate Monitors.
Target	The class to use for the target of the rule or monitor. The rule or monitor will be run on any agent that has at least one instance of this class. For more information on targets, see Understanding Classes and Objects.
Rule is enabled Monitor is enabled	Specifies whether the rule or monitor is enabled.

Application Log Data Source

There will be a single application log data source page for a collection or alerting rule and for a monitor using manual or timer reset. For a monitor using event reset, you will have to define the log for both the error condition and for the healthy condition. You will typically specify the same log for both conditions, but a different log could be used for each.

The following table lists the settings that must be provided for an application log data source:

Property Name	Description
Directory	Directory that the log file is located in. This must be a single directory with no wildcards
Pattern	Name of the log file. This can include wildcards if the name of the log file will change. Use the ? wildcard to represent a single character. Use the * wildcard to represent multiple characters.
Separator (Delimited Logs only)	The character that is used to separate the
UTF8	

Event Expression

There will be a single expression page for a collection or alerting rule and for a monitor using manual or timer reset. For a monitor using event reset, you will have to define an expression for both the error condition and for the healthy condition.

The expression for a text log rule or monitor will include criteria that matches text in the log entry. For a Generic Text Log this includes a search of the whole log entry treated as a single line. For a delimited log file, this will include a search of one or more of the included fields. The contents of a text log are included in the parameters of the event. For a generic text log, this is referenced by the parameter **Params/Param[1]**. A delimited log uses the same variable by using the index number of the required parameter. The first field would be referenced with **Params/Param[1]**, the second field would be referenced with **Params/Param[2]**, and so on.

The following table lists the common properties available from text log monitors and rules:

Property Name	Description
Directory	Directory that the log file is located in.
Pattern	Name of the log file that the event was taken from.
Param[1]	Complete entry in a generic text log.
Param[#]	Specific parameter in a generic CSV text log. # represents the number of the field.

For more information about expressions, see Expressions.

Auto Reset Timer

The **Auto Reset Timer** page is only available for timer reset monitors. It allows you to set the time that must pass after the alert is created before the alert is automatically resolved.

Configure Health

The **Configure Health** page is only available for monitors. It allows you to specify the health state that will be set for each of the events. For a manual reset monitor, the **Manual Reset** condition will be **Healthy**, and you can specify whether the **Event Raised** condition will set the monitor to a **Warning** or a **Critical** state. For a **Timer Reset** or an **Event Reset**, you can specify the health state set by each event. The first event will typically set the monitor to **Warning** or **Critical** while the second event or the timer will set the monitor to **Healthy**.

Configure Alerts

The **Configure Alerts** page is only available for monitors and alerting rules. Its options are explained in Alerts.

Creating Text Log Rules and Monitors

Use the following procedure to create a text log alerting rule in Operations Manager with the following details:

- Runs on all agents with a particular service installed.
- Looks for a comma delimited log file with the naming pattern MyApp*.log in the c:\logs directory.
- Generates an alert if the word “error” appears in the log message.
- Includes the error message in the alert description.
- The format of each line of the text file is as follows: Date,Time,Message

To create a delimited text log alert rule

1. If you don’t have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. Create a new target using the process in To create a Windows Service template. You can use any service installed on a test agent for this template.
3. In the Operations console, select the **Authoring** workspace, and then select **Rules**.
4. Right-click **Rules** and select **Create a new rule**.
5. On the **Rule Type** page, do the following:
   a. Expand **Alert Generating Rules**, expand **Event Based**, and then click **Generic CSV Text Log (Alert)**.
   b. Select the management pack from step 1.
   c. Click **Next**.

6. On the **General** page, do the following:
    a. In the **Rule Name** box, type **MyApplication Delimited Log Error**.
    b. In the **Rule Category** box, select **Alert**.
    c. Next to **Rule Target** click **Select** and then select the name of the target that you created in step 2.
    d. Leave **Rule is enabled** selected.
    e. Click **Next**.
7. On the **Application Log Data Source** page, do the following:
    a. In the **Directory** box, type **c:\logs**.
    b. In the **Pattern** box, type **MyApp*.log**.
    c. In the **Separator** box, type a COMMA.
    d. Click **Next**.
8. On the **Build Event Expression** page, do the following:
    a. Click **Insert**.
    b. In the **Parameter Name** box type **Params/Param[3]**.
    c. In the **Operator** box select **Contains**.
    d. In the **Value** box type **error**.
    e. Click **Next**.
9. On the **Configure Alerts** page, do the following:
    a. In the **Alert name** box, type **Error found in MyApplication delimited text log.**.
    b. Click the ellipse button to the right side of the **Alert description** box.
    c. Clear the text in the **Value** box.
    d. Select Data, then Params, then Param.
    e. Replace the text **<<INT>>** with **1**.
    f. Move to the end of the line and press the SPACE bar.
    g. Select Data, then Params, then Param.
    h. Replace the text **<<INT>>** with **2**.
    i. Move to the end of the line and press the ENTER key.
    j. Select Data, then Params, then Param.
    k. Replace the text **<<INT>>** with **3**.
    l. Click **OK**.
10. Click **Finish**.

See Also

Event Monitors and Rules

Event Monitor Reset

Repeating Events

WMI Events

WMI events are created from WMI queries that detect particular actions in the operating system or in applications that create their own WMI events. These events can be used to detect such actions as a process ending, a file being created, or a registry key being modified. WMI events are not persisted. Therefore, any WMI events that are created when the agent service is not running are lost.

Note
This guide assumes knowledge of how to build a WMI notification query. For a an overview of this topic and sample queries see Unlocking the Mystery of WMI Events in MOM.

WMI Event Wizards

The table below lists the wizards that are available for WMI events.

Management Pack Object	Wizards Available
Monitors	Simple Event Detection using each of the standard Event Monitor Reset methods
	Repeated Event Detection using each of the standard Event Monitor Reset methods
Rules	Alert Generating WMI event rule
	Event collection WMI event rule

WMI Event Wizard Options

When you run a WMI event rule or monitor wizard, you will need to provide values for options in the following tables. Each table represents a single page in the wizard.

General

The **General** page includes general settings for the rule or monitor including its name, category, target, and the management pack file to store it in.

Option	Description
Name	The name used for the rule or monitor. For a

Option	Description
	rule, the name appears in the **Rules** view in the **Authoring** pane. When you create a view or report, you can select this name to use the data collected by it. For a monitor, the name appears in the Health Explorer of any target objects.
Description	Optional description of the rule or monitor.
Management Pack	Management pack file to store the rule or monitor. For more information on management packs, see Selecting a Management Pack File.
Rule Category (Rules only)	The category for the rule. For an event collection rule, this should be **Event Collection**. For an alerting rule, this should be **Alert**.
Parent Monitor (Monitors only)	The aggregate monitor that the monitor will be positioned under in the Health Explorer. For more information, see Aggregate Monitors.
Target	The class to use for the target of the rule or monitor. The rule or monitor will be run on any agent that has at least one instance of this class. For more information on targets, see Understanding Classes and Objects.
Rule is enabled Monitor is enabled	Specifies whether the rule or monitor is enabled.

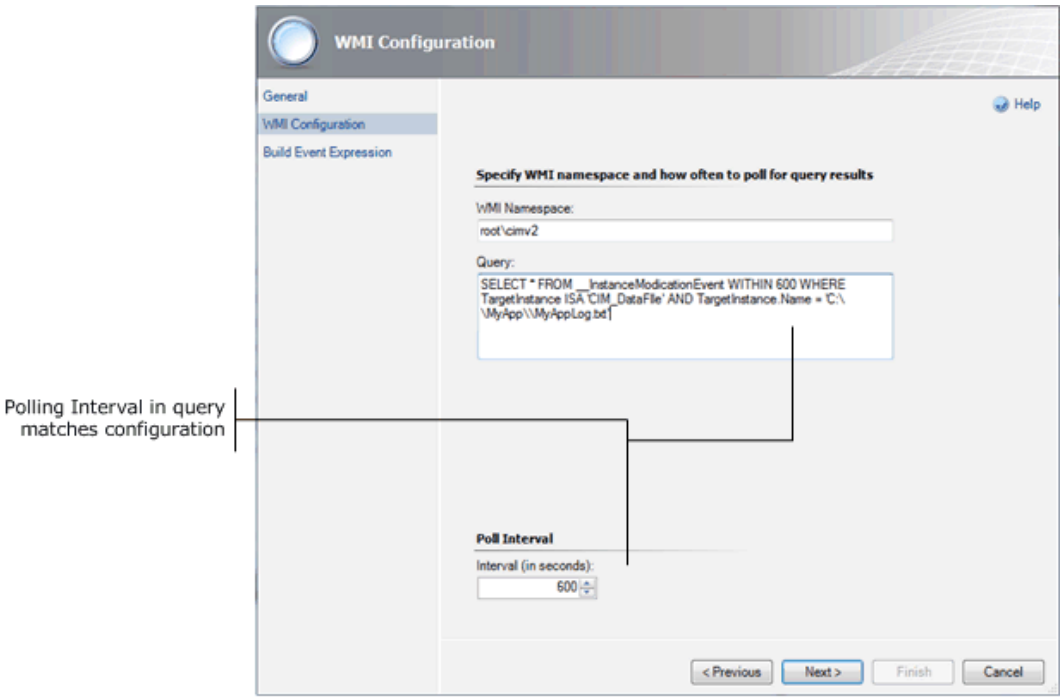
WMI Configuration / WMI Event Provider

The **WMI Configuration** Page allows you to provide the WMI namespace, query, and poll interval. There will be a single **WMI Configuration** page for a collection or alerting rule and for a monitor using manual or timer reset. For a monitor using **WMI Event Reset**, there will be a **WMI Event Provider** page to define the query for both the error condition and for the healthy condition.

Option	Description
WMI Namespace	The namespace containing the class that is used in the WMI query.

Option	Description
Query	WMI notification query that looks for the occurrence of a particular WMI event.
Poll Interval	Specifies how frequently Operations Manager will poll WMI for the occurrence of the event. This value should be the same as the value used in the WITHIN clause of the notification query.

WMI matching poll intervals



Build Expression

The **Build Expression** page allows you to define a filter for the data coming from the WMI query. There will be a single **Build Expression** page for a WMI event monitor using manual or timer reset. For a monitor using **WMI Event Reset**, there is an expression for each health state.

Because criteria can be specified in the WHERE clause of the WMI query, an expression is frequently not required in a WMI event monitor. It is only required if the query is expected to return multiple records. WMI event rules rely on the criteria in the query itself and don't allow an expression. The Operations console wizards though require that criteria be specified in WMI

Event monitors. If no criteria is required, then dummy criteria must be specified in the wizard and then removed by viewing the properties of the monitor after it is created.

The properties available for a WMI event will vary, depending on the kind of event being monitored. The properties available will also vary, depending on the properties of the WMI class included in the query. The data will be in the form of a property bag that has a collection of properties for one or more WMI class instances. WMI events created by using a query that uses either __InstanceCreationEvent or __InstanceDeletionEvent will have a single collection called TargetInstance with the instance being either created or deleted. WMI events created by using __InstanceModificationEvent will have an additional collection called PreviousInstance.

The syntax for properties from a WMI event is as follows:

```
Collection[@Name='TargetInstance']/Property[@Name='Caption']
```

For example, the following WMI query monitors for the change in a file that is named c:\MyApp\MyAppLog.txt.

```
SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA
'CIM_DataFIle' AND TargetInstance.Name = 'C:\\MyApp\\MyAppLog.txt'
```

Assuming that data is added to the file changing the file size and triggering the query, examples of properties from this query are shown in the following table:

Property	Syntax
Original file size	Collection[@Name=’PreviousInstance’]/Property[@Name='FileSize']
New file size	Collection[@Name=’TargetInstance’]/Property[@Name='FileSize']

Auto Reset Timer

The **Auto Reset Timer** page is only available for timer reset monitors. It allows you to set the time that must pass after the alert is created before the alert is automatically resolved.

Configure Health

The **Configure Health** page is only available for monitors. It allows you to specify the health state that will be set for each of the events. For a manual reset monitor, the **Manual Reset** condition will be **Healthy**, and you can specify whether the **Event Raised** condition will set the monitor to a **Warning** or a **Critical** state. For a **Timer Reset** or an **WMI Event Reset**, you can specify the health state set by each event. The first event will typically set the monitor to **Warning** or **Critical** while the second event or the timer will set the monitor to **Healthy**.

Configure Alerts

The **Configure Alerts** page is only available for monitors and alerting rules. Its options are explained in Alerts.

Creating WMI event monitors and rules

The following procedure shows how to create a WMI event monitor in Operations Manager with the following details:

- Runs on all agents with a particular service installed.
- Sets the monitor to a **critical** state when Notepad is started on the agent computer.
- Sets the monitor to a **healthy** state when Notepad is ended on the agent computer.

Note

This example is not meant to illustrate a real world scenario since there would be minimal value in monitoring when Notepad is started. It does through represent a common scenario of monitoring two different WMI events in a monitor. Using Notepad provides a sample that is easy to test by starting and stopping Notepad on the agent computer.

To create a WMI event monitor

1. If you don't have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. Create a new target using the process in To create a Windows Service template. You can use any service installed on a test agent for this template.
3. In the Operations console, select the **Authoring** workspace.
4. Right-click **Monitors**, select **Create a Monitor**, and then select **Unit Monitor**.
5. On the **Monitor Type** page, do the following:
   a. Expand **WMI Events**, then **Simple Event Detection**, and then **WMI Event Reset**.
   b. Select the management pack from step 1.
   c. Click **Next**.
6. On the **General** page, do the following:
   a. In the **Name** box, type **MyApplication WMI Event Error**.
   b. Click **Select** next to the **Monitor Target** box.
   c. Next to **Monitor Target** click **Select** and then select the name of the target that you created in step 2.
   d. In the **Parent Monitor** box, select **Availability**.
   e. Leave the **Monitor is enabled** box checked , select and click **Next**.
7. On the **First WMI Event Provider** page, do the following:
   a. In the **WMI Namespace** box, type **root\cimv2**.
   b. In the **Query** box, type the following WMI query.

```
Select * From __InstanceCreationEvent WITHIN 60 Where
```

```
TargetInstance ISA 'Win32_Process' and TargetInstance.Name =
'notepad.exe'
```

c. In the **Poll Interval** box, type **60**.

d. Click **Next**.

8. On the **Build First Expression** page, do the following:

Note

In this example, criteria is included in the WMI query, so no expression is required in the monitor. Since the WMI event wizard in the Operations console requires an expression for each event, dummy expressions will be provided to complete the wizard and then deleted once the monitor is created.

a. Click **Insert**.

b. In the **Parameter Name** box type **Dummy**.

c. In the **Operator** box select **Equals**.

d. In the **Value** box type **Dummy**.

e. Click **Next**.

9. On the **Second WMI Event Provider** page, do the following:

a. In the **WMI Namespace** box, type **root\cimv2**.

b. In the **Query** box, paste the following WMI query.

```
Select * From __InstanceDeletionEvent WITHIN 60 Where
TargetInstance ISA 'Win32_Process' and TargetInstance.Name =
'notepad.exe'
```

c. In the **Poll Interval** box, type **60**.

d. Click **Next**.

10. On the **Second Expression** page, do the following:

a. Click **Insert**.

b. In the **Parameter Name** box type **Dummy**.

c. In the **Operator** box select **Equals**.

d. In the **Value** box type **Dummy**.

e. Click **Next**.

11. On the **Configure Health** page, do the following:

a. Next to **FirstEventRaised**, change the **Health State** to **Critical**.

b. Click **Next**.

12. On the **Configure Alerts** page, do the following:

a. Check **Generate alerts for this monitor**

b. In the **Generate an alert when** box, select **The monitor is in a critical health state**.

c. Leave the box selected to automatically resolve the alert.

d. In the **Alert name** box, type **Notepad process detected**

e. Click the ellipse button next to **Alert description**.

f. Clear the contents of the **Value** box and then type **Path of executable:** .

g. Click **Data**, then **Collection**, then **Property**.

h. In the variable, replace **<<INT>>** with "TargetInstance" and **<<STRING>>** with **ExecutablePath**. The final text in the **Value** box should be **Path of executable: $Data/Context/Collection["TargetInstance"]/Property[@Name="ExecutablePath"]$**

i. Click **OK**.

13. Click **Create**.
14. Right-click **MyApplication WMI Event Error** and select **Properties**.
15. On the **First Expression** tab, click **Delete**.
16. On the **Second Expression** tab, click **Delete**.
17. Click **OK**.

See Also

Event Monitors and Rules

Event Monitor Reset

Repeating Events

Alerts

Syslog Events

Syslog events can be used to collect messages from Unix systems and other devices in Operations Manager. Syslog rules can be run on an agent that is the receiver of messages from one or more devices. When the rule is run, the agent will listen for messages on UDP port 514. This is the only port that can be used.

Target

Rules and monitors run on the agent computer of each instance of the target class, and they usually access data on the local computer. SNMP rules and monitors typically work with information from a computer or device different from the one running the monitors or rules. For SNMP traps, the monitor or rule needs to be running on the agent that receives the trap. The device needs to be configured to deliver traps to this agent. For SNMP probes, the monitor or rule needs to be running on any agent that is authorized to access the device with SNMP. The device may need to be configured to allow communication from this agent.

Network devices that are discovered with the Discovery Wizard are managed by a resource pool that you specify during the discovery process. A resource pool contains one or more management servers. You can use the classes for these devices as targets, and the rule or monitor will run on each computer in the resource pool. In this case, the device will need to send

SNMP traps to each of the computers in the pool and allow access to each computer in the pool for SNMP probes.

Syslog Event Wizards

The table below lists the wizards that are available for both simple and delimited text files.

Management Pack Object	Wizards Available
Monitors	None
Rules	Alert Generating rule
	Event collection rule

Syslog Event Wizard Options

When you run a Syslog event rule wizard, you will need to provide values for options in the following tables. Each table represents a single page in the wizard.

General

The **General** page includes general settings for the rule including its name, category, target, and the management pack file to store it in.

Option	Description
Name	The name used for the rule. The name appears in the **Rules** view in the **Authoring** pane. When you create a view or report, you can select this name to use the data collected by it.
Description	Optional description of the rule.
Management Pack	Management pack file to store the rule or monitor. For more information on management packs, see Selecting a Management Pack File.
Rule Category (Rules only)	The category for the rule. For an event collection rule, this should be **Event Collection**. For an alerting rule, this should be **Alert**.
Parent Monitor (Monitors only)	The aggregate monitor that the monitor will be positioned under in the Health Explorer. For

Option	Description
	more information, see Aggregate Monitors.
Target	The class to use for the target of the rule. The rule will be run on any agent that has at least one instance of this class. For more information on targets, see Understanding Classes and Objects.
Rule is enabled	Specifies whether the rule is enabled.

Build Event Expression

The **Build Event Expression** page allows you to filter for specific events to be collected or to generate an alert. The Syslog data properties are shown in the following table:

Property Name	Description
Facility	The facility of the event that uses one of the values from the table that follows.
Severity	Numeric value that indicates the severity of the event using one of the following values: 0 - Emergency 1 - Alert 2 - Critical 3 - Error 4 - Warning 5 - Notice 6 - Info 7 - Debug
Priority	Numeric priority of the message.
PriorityName	Text description of the priority level.
TimeStamp	Time that the message was sent.
HostName	Name of the device sending the message.
Message	Text of the message

Important

The event expression will almost always contain the Host Name in addition to one or more properties depending on the criteria that you require. Since a single management server may receive messages from multiple network devices, it must be able to determine which device sent a particular event. If the Host Name is not in the criteria, then a single event will most likely create a separate alert for each device.

Facility Values

The value for the **facility** property defines the part of the system that the message originated from. It will have one of the values from the following table:

Facility	Description	Value
0	Kernel	Kernel messages
1	User	User-level messages
2	Mail	Mail System
3	Daemons	System daemons
4	Auth	Security and authorization
5	Syslog	Syslog internal messages
6	LPR	Line printer subsystem
7	News	Network news
8	UUCP	Unix-to-Unix copy program
9	Cron	Cron daemon
10	Auth2	Security and authorization
11	FTP	FTP daemon
12	NTP	Network time subsystem
13	LogAudit	Audit level
14	LogAlert	Message alert
15	Cron2	Cron daemon
16	Local0	Local use 0
17	Local1	Local use 1
18	Local2	Local use 2
19	Local3	Local use 3
20	Local4	Local use 4

Facility	Description	Value
21	Local5	Local use 5
22	Local6	Local use 6
23	Local7	Local use 7

Configure Alerts

The **Configure Alerts** page is only available for monitors and alerting rules. Its options are explained in Alerts.

Creating Syslog Event Rules

The following procedure shows how to create a Syslog event alerting rule in Operations Manager with the following details:

- Runs on all network devices.
- Generates an alert for any message with a severity of error or worse.

To create a Syslog event alerting rule

1. If you don't have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. In the Operations console, select the **Authoring** workspace, and then select **Rules**.
3. Right-click **Rules** and select **Create a new rule**.
4. On the **Rule Type** page, do the following:
   a. Expand **Alert Generating Rules**, expand **Event Based**, and then click **Syslog (Alert)**.
   b. Select the management pack from step 1.
   c. Click **Next**.
5. On the **General** page, do the following:
   a. In the **Rule Name** box, type **Alert on syslog message**.
   b. In the **Rule Category** box, select **Alert**.
   c. Next to **Rule Target** click **Select**.
   d. Select **View all targets**.
   e. In the list of targets, select **Node** and then click **OK**.
   f. Leave **Rule is enabled** selected.
   g. Click **Next**.
6. On the **Build Event Expression** page, do the following:
   a. Click **Insert**.

b. In the **Parameter Name** box type **Severity**.
c. In the **Operator** box select **Less than or equal to**.
d. In the **Value** box type **3**.
e. Click **Insert**.
f. In the **Parameter Name** box type **HostName**.
g. In the **Operator** box select **Equals**.
h. Click the ellipse button next to **Value** and click **SNMP Agent Address**.
i. Click **Next**.

7. On the **Configure Alerts** page, do the following:
   a. In the **Alert name** box, type **Syslog error message received**
   b. In the **Alert description** box, type **$Data/EventData/DataItem/Message$**.
   c. Click **Create**.

See Also

Event Monitors and Rules

Alerts

SNMP Events

SNMP monitors and rules in Operations Manager allow you to retrieve messages from computers and devices that support Simple Network Management Protocol (SNMP). You can create rules and monitors that either wait for an SNMP trap to be sent or that retrieve information on a periodic basis using an SNMP probe.

Target

Rules and monitors run on the agent computer of each instance of the target class, and they usually access data on the local computer. SNMP rules and monitors typically work with information from a computer or device different from the one running the monitors or rules. For SNMP traps, the monitor or rule needs to be running on the agent that receives the trap. The device needs to be configured to deliver traps to this agent. For SNMP probes, the monitor or rule needs to be running on any agent that is authorized to access the device with SNMP. The device may need to be configured to allow communication from this agent.

Network devices that are discovered with the Discovery Wizard are managed by a resource pool that you specify during the discovery process. A resource pool contains one or more management servers. You can use the classes for these devices as targets, and the rule or monitor will run on each computer in the resource pool. In this case, the device will need to send SNMP traps to each of the computers in the pool and allow access to each computer in the pool for SNMP probes.

SNMP Event Wizards

The table below lists the wizards that are available for both simple and delimited text files.

Management Pack Object	Wizards Available
Monitors	SNMP probe monitor with single event reset
	SNMP trap monitor with single event reset
Rules	Alert Generating SNMP trap rule
	Event collection SNMP probe rule
	Event collection SNMP trap rule
	Performance collection SNMP probe rule

SNMP Event Wizard Options

When you run an SNMP monitor wizard, you will need to provide values for options in the following tables. Each table represents a single page in the wizard.

General

The **General** page includes general settings for the rule or wizard including its name, category, target, and the management pack file to store it in.

Option	Description
Name	The name used for the rule or monitor. For a rule, the name appears in the **Rules** view in the **Authoring** pane. When you create a view or report, you can select this name to use the data collected by it. For a monitor, the name appears in the Health Explorer of any target objects.
Description	Optional description of the rule or monitor.
Management Pack	Management pack file to store the rule or monitor. For more information on management packs, see Selecting a Management Pack File.
Rule Category (Rules only)	The category for the rule. For an event collection rule, this should be **Event**

Option	Description
	Collection. For a performance collection rule, this should be **Performance Collection**. For an alerting rule, this should be **Alert**.
Parent Monitor (Monitors only)	The aggregate monitor that the monitor will be positioned under in the Health Explorer. For more information, see Aggregate Monitors.
Target	The class to use for the target of the rule or monitor. The rule or monitor will be run on any agent that has at least one instance of this class. For more information on targets, see Understanding Classes and Objects. If you are monitoring a network device discovered in the Discovery Wizard, then use the class for the device or one of its components, depending on what the monitor most applies to.
Rule is enabled Monitor is enabled	Specifies whether the rule or monitor is enabled.

SNMP Probe / SNMP Trap Provider

SNMP probe rules have an **SNMP Probe** page, while SNMP trap rules have an **SNMP Trap Provider** page. SNMP monitors will have two of the appropriate page, one to define the healthy state and the other to define the warning or critical state. The page defines the community string and OID of the SNMP probe or trap.

Option	Description
Frequency (Probe only)	The frequency that the probe is run. A frequency that is configured too low can result in excess overhead on the device being monitored. A frequency that is configured too high can result in the monitor not detecting a problem quickly. A frequency from 2 minutes to 15 minutes is a common range.
Community string	If **Use discovery community string** is selected, then the community of the target device is used. If **Use custom community string** is selected, then you can specify a

Option	Description
	community string.
Object Identifier	For a probe, one or more Object Identifiers (OID) to retrieve from the device. A value for each one will be collected and available for evaluation in the expression. Most rules and monitors will use a single OID, but multiple OIDs can be used. For a trap, one or more Object Identifiers (OID) to listen for from the device. Most rules and monitors will use a single OID, but multiple OIDs can be used.
All Traps (Trap only)	If select, the **Object Identifier** list is disabled, and all traps from the target object will be collected, regardless of the OID.

Build Expression (Monitors Only)

SNMP monitors have a **Build Expression** page for each of the **SNMP Probe** or **SNMP Trap Provider** pages. The expression evaluates the SNMP data returned to determine the health state of the monitor.

For more information about expressions, Expressions.

The **Parameter Name** in each expression requires a variable referring to a piece of data from the SNMP probe or trap. The data that is available includes header information and a data element for each OID specified. The header information is shown in the following table:

Data Item	Description
Source	IP address of the device.
Destination	IP address of the agent receiving the event
CommunityString	Encrypted community string
ErrorCode	Error code returned by the request
Version	Version of SNMP used

The information in each data element is shown in the following table:

Data Item	Description
OID	OID of the data element

Data Item	Description
Syntax	Indicates the success or failure of the SNMP operation. If successful, the property is set to a value indicating the data type of the value. If unsuccessful, the property is set to a data type indicating the error. The specific values are listed in the documentation for the SNMP Probe Module.
Value	The value of the data element.

To refer to the OID data elements, you can use the following syntax:

Syntax	Example	Description
SnmpVarBinds/SnmpVarBind/<ElementName>	SnmpVarBinds/SnmpVarBind/Value	Use this syntax when a single OID is used.
SnmpVarBinds/SnmpVarBind[#]/<ElementName>	SnmpVarBinds/SnmpVarBind[2]/Value	Use this syntax when you have multiple OIDs and want to refer to each by its numeric order. The first OID is 1, the

Syntax	Example	Description
		second is 2, and so on.
SnmpVarBinds/SnmpVarBind[OID="<OID>"]/<ElementName>	SnmpVarBinds/SnmpVarBind[OID="1.3.6.1.2.1.1.5.0"]/Value	Use this syntax when you have multiple OIDs and want to refer to each by the specific OID.

Configure Health

The **Configure Health** page is only available for monitors. It allows you to specify the health state that will be set for each of the events. The first event will typically set the monitor to **Warning** or **Critical** while the second event or the timer will set the monitor to **Healthy**.

Configure Alerts

The **Configure Alerts** page is only available for monitors and alerting rules. Its options are explained in Alerts.

Creating SNMP Monitors and Rules

Creating an SNMP Rule

Use the following procedure to create an SNMP performance collection rule in Operations Manager with the following details:

- Runs on all network devices by using Node for the target.
- Collects the number of open TCP connections (OID 1.3.6.1.2.1.6.9.0) every 10 minutes.

To create an SNMP Performance Collection Rule

1. If you don't have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. In the Operations console, select the **Authoring** workspace, and then select **Rules**.
3. Right-click **Rules** and select **Create a new rule**.
4. On the **Rule Type** page, do the following:
   a. Expand **Collection Rules**, expand **Performance Based**, and then click **SNMP Performance**.
   b. Select the management pack from step 1.
   c. Click **Next**.
5. On the **General** page, do the following:
   a. In the **Rule Name** box, type **Collect Open TCP Connections**.
   b. In the **Rule Category** box, select **Performance Collection**.
   c. Next to **Rule Target** click **Select** and then select **Node**.
   d. Leave **Rule is enabled** selected.
   e. Click **Next**.
6. On the **SNMP Probe** page, do the following:
   a. In the **Frequency** box, **10 minutes**.
   b. In the **Object Identifier** box, type **1.3.6.1.2.1.6.9.0** and press ENTER.
   c. Click **Create**.

Creating an SNMP Monitor

Use the following procedure to create an SNMP trap monitor Operations Manager with the following details:

- Runs on all network devices by using Node for the target.
- Monitors for the status of a port. Link down is indicated with OID .1.3.6.1.6.3.1.1.5.3. Link up is indicated with OID .1.3.6.1.6.3.1.1.5.4.
- Monitors port 16 only. This is indicated by Object Identifier .1.3.6.1.2.1.2.2.1.8.16 with a value of 2 for link down and Object Identifier .1.3.6.1.2.1.2.2.1.8.16 with a value of 1 for link up.
- Includes the OID and value for the first four entries in the SNMP data.

To create an SNMP Trap monitor

1. If you don't have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. In the Operations console, select the **Authoring** workspace.
3. Right-click **Monitors**, select **Create a Monitor**, and then select **Unit Monitor**.
4. On the **Monitor Type** page, do the following:
   a. Expand **SNMP**, then **Trap Based Detection**, then **Simple Trap Detection**, and then

SNMP Trap Monitor.

b. Select the management pack from step 1.

c. Click **Next**.

5. On the **General** page, do the following:
   a. In the **Name** box, type **Port active**.
   b. Click **Select** next to the **Monitor Target** box.
   c. Select **Node** and click **OK**.
   d. In the **Parent Monitor** box, select **Availability**.
   e. Leave the **Monitor is enabled** box checked, select and click **Next**.
6. On the **First SnmpTrapProvider** page, do the following:
   a. In the **Object Identifier** box, type **.1.3.6.1.6.3.1.1.5.3** and press ENTER.
   b. Click **Create**.
7. On the **Build First Expression** page, do the following:
   a. Click **Insert**.
   b. In the **Parameter Name** box type **SnmpVarBinds/SnmpVarBind[OID=".1.3.6.1.2.1.2.2.1.8.16"]/Value**.
   c. In the **Operator** box select **Equals**.
   d. In the **Value** box type **2**.
   e. Click **Next**.
8. On the **Second SnmpTrapProvider** page, do the following:
   a. In the **Object Identifier** box, type **.1.3.6.1.6.3.1.1.5.4** and press ENTER.
   b. Click **Create**.
9. On the **Build Second Expression** page, do the following:
   a. Click **Insert**.
   b. In the **Parameter Name** box type **SnmpVarBinds/SnmpVarBind[OID=".1.3.6.1.2.1.2.2.1.8.16"]/Value**.
   c. In the **Operator** box select **Equals**.
   d. In the **Value** box type **1**.
   e. Click **Next**.
10. On the **Configure Health** page, do the following:
    a. Next to **FirstEventRaised**, change the **Health State** to **Critical**.
    b. Click **Next**.
11. On the **Configure Alerts** page, do the following:
    c. .a. Check **Generate alerts for this monitor**
    b. In the **Generate an alert when** box, select **The monitor is in a critical health state**.
    c. Leave the box selected to automatically resolve the alert.
    d. In the **Alert name** box, type **Port active**
    e. Click the ellipse button next to the **Alert description** box.

f. Clear the contents of the **Value** box.
g. Click **Data** and then **Source**. Press ENTER.
h. Click **Data** and then **Destination**. Press ENTER.
i. Click **Data**, then **SnmpVarBinds**, then **SnmpVarBind**, and then **OID**.
j. In the variable, change **[<<INT>>]** to **[1]**.
k. Type a space after the variable.
l. Click **Data**, then **SnmpVarBinds**, then **SnmpVarBind**, and then **Value**.
m. In the variable, change **[<<INT>>]** to **[1]**.
n. Repeat the previous steps to add the OID and value for entries 2, 3, and 4.
o. Click **OK**.

12. Click **Create**.

See Also

Monitoring Networks by Using Operations Manager

How to Discover Network Devices in Operations Manager

Event Monitor Logic

Event monitors in System Center 2012 – Operations Manager use one of the event data sources to identify a particular event that indicates an issue. As soon as the specific data source that holds the required information is identified, the logic used to determine different health states must be determined. In addition to the logic that indicates whether an error condition has occurred, additional logic must be defined to determine when the state should be changed back to a healthy condition.

The different kinds of logic that can be used to detect an error condition by using events are listed in the following table. See the individual topic for each condition for details on how its logic is implemented. As noted in the table, some logic can only be used with Windows events.

Logic	Data Sources	Description
Simple Event	All	Detects an error state from the occurrence of a single event. There is no individual topic for this logic.
Repeating Events	All	Detects an error state from one or more occurrences of a particular event in a specified time window.

Logic	Data Sources	Description
Correlated Events	Windows Events	Detects an error state from the occurrence of two events in a specified time window.
Correlated Missing Events	Windows Events	Detects an error state from an expected event not being detected in a particular time window after the occurrence of another event.
Missing Events	Windows Events	Detects an error state from an expected event not being detected in a particular time window.

Repeating Events

Repeated event detection in Operations Manager uses one or more occurrences of a particular event in a time window to indicate an error condition in a monitor. Repeated event logic is available for the following monitors:

- Windows Events
- Text Logs
- WMI Events

This typically applies to conditions in an application where a single event on its own can be ignored, but multiple occurrences of that event in a particular time window indicate a potential error. There are different algorithms that can be used for this detection, depending on the logic that best identifies the specific application issue. The following are details of the different algorithms:

Trigger on Timer

Trigger on timer consolidation of events uses a specified time window and is not dependent on the number of events received. A single event can trigger an error in the health state as in simple detection. Unlike simple detection which sets the health state immediately upon detection of the specified event, however trigger on timer consolidation waits until a specified time window to set the health state of the monitor. The time window can be a rotating time duration of specified length or a specific window based on day of the week.

Trigger on timer consolidation is useful for errors that should only be detected in a certain time window. Used with a time window based on a specific time of day, this disables the monitor

outside that time period. It can also have the effect of delaying the change of state for a particular time during which an event that indicates a healthy state could be received. In this case, the health state would never be changed.

Trigger on Count

Trigger on count consolidation of events lets a monitor require multiple occurrences of the same event in a specified time window before it changes the health state to an error. The time window can be rotating time duration of specified length or a specific window based on day of the week.

Trigger on count consolidation resembles trigger on timer consolidation except that multiple occurrences of the event are required instead of just one. When the time window is reached, the event count is returned to zero, and the specific number of events must detected before the time window expires again for the health state to be changed.

Trigger on Count, Sliding

Trigger on count, sliding consolidation of events is similar to trigger on count consolidation except that the time window is reset every time that the specified event is received. The time window only expires if the time is reached after the occurrence of the last event.

Trigger on count, sliding consolidation is useful for error conditions that are detected by a certain number of events in a particular length of time. By using trigger on count consolidation, some events could be received in one time window and then other events received in the next time window with the result that the health state is never changed. Using trigger on count, sliding consolidation, the time window depends on when the event occurs preventing this condition.

Repeated Events Example

To help with understanding the different algorithms used for repeated event detection, the following table shows the effect on health state for monitors based on the different kinds of consolidation. This is based on a repeated event monitor that uses the following details:

- Consolidation interval: 2 minutes
- Compare count: 3 (ignored by Trigger on Timer)
- Health state on repeated event: Critical
- Reset Logic: Event reset using Event 3

Time	Event	Trigger on Timer	Trigger on Count	Trigger on Count, Sliding
00:00:00	-	Healthy	Healthy	Healthy
00:01:00	Event 1	Healthy	Healthy	Healthy
00:02:00	-	Healthy	Healthy	Healthy

Time	Event	Trigger on Timer	Trigger on Count	Trigger on Count, Sliding
00:02:30	-	Healthy	Healthy	Healthy
00:03:00	-	Critical	Healthy	Healthy
00:03:30	Event 3	Healthy	Healthy	Healthy
00:04:00	Event 1	Healthy	Healthy	Healthy
00:04:30	-	Healthy	Healthy	Healthy
00:05:00	Event 1	Critical	Healthy	Healthy
00:05:30	-	Critical	Healthy	Healthy
00:06:00	-	Critical	Healthy	Healthy
06:30:00	Event 1	Critical	Healthy	Healthy
07:00:00	Event 1	Critical	Healthy	Critical
07:30:00	-	Critical	Healthy	Critical
00:08:00	Event 1	Critical	Healthy	Critical
00:08:30	-	Critical	Critical	Critical
00:09:00	Healthy	Critical	Healthy	Healthy

- Using trigger on timer, a critical state is set at 00:03:00 event though the event is received at 00:01:00 because the time window starts when the monitor is loaded. The start is reset to healthy at 00:03:30, but the critical state is again triggered at 00:05:00 from the time window started at 00:03:00.
- Using trigger on count, the event at 00:05:00 does not trigger a critical state because the time window started by the event at 00:01:00 would have expired at 00:03:00. This event is instead part of the time window started by the event at 00:04:00 which expires at 00:06:00. The monitor triggers a critical state at 00:08:30 because of the 3 events detected in the time window started with the event at 00:06:30.
- Using trigger on count, sliding, each occurrence of Event 1 starts its own window. The critical state is triggered at 00:07:00 from the 3 events detected in the time window started with the event at 00:05:00.

Creating Repeated Event Monitors

The following procedure describes how to create a repeating event monitor with the following details:

- Positioned under the Availability aggregate monitor.

- Sets the monitor to a critical state when three events with source **EventCreate** and number **201** are detected in the Application event log within 10 minutes.
- Resets after fifteen minutes of no event being received.
- Creates an alert when the monitor enters a critical state.

Note

EventCreate is used as the event source so that the EventCreate utility can be used to create a test event. This utility is available on any Windows Computer and creates test events with a source of **EventCreate**. If you have another method of creating test events, then you can use a different source.

To create a repeating event monitor

1. If you don't have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. Create a new target using the process in To create a Windows Service template. You can use any service installed on a test agent for this template.
3. In the Operations console, select the **Authoring** workspace.
4. Select **Management Pack Objects**.
5. Right-click **Monitors**, select **Create and Monitor**, and then select **Unit Monitor**.
6. On the **Monitor Type** page, do the following:
   a. In the **Select the type of monitor to create** box, expand **Windows Events** and then **Repeated Event Detection**.
   b. Select **Timer Reset**.
   c. In the **Management Pack** dropdown list, select the management pack for the application.
   d. Click **Next**.
7. On the General page, do the following:
   a. In the **Name** box, type **Repeated error event 201** or another name for the monitor. This is the text that will appear in the Health Explorer.
   b. Click **Select**.
   c. In the **Select Items to Target** dialog box, select the name that you used for the Windows Service template in step 2.
   d. The **Parent monitor** box should show **Availability**. You can select a different parent monitor.
   e. Ensure that **Availability** is selected for the **Parent monitor**.
   f. The **Monitor is enabled** box should be checked so that the monitor is enabled.
   g. Click **Next**.
8. On the **Event Log Name** page, do the following:
   a. In the **Log Name** box, keep the default value of **Application**.
   b. Click **Next**

9. On the **Event Expression** page, do the following:
    a. For the **Event ID** value, type **201**
    b. For the **Event Source** value, type **EventCreate**
    c. Click **Next**.
10. On the **Repeated Settings** page, do the following:
    a. For the **Counting Mode**, select **Trigger on count, sliding**.
    b. For the **Compare Count**, type **3**.
    c. Select **Based on items occurrence within a time interval**.
    d. For the **Interval**, type **10** and select **Minutes**.
    e. Click **Next**.
11. On the **Auto Reset Timer** page, do the following:
    a. For **Specify wait time**, select **15 minutes**.
    b. Click **Next**
12. On the **Configure Health** page, do the following:
    a. For **Timer Event Raised**, leave the **Health State** as **Healthy**.
    b. For **Repeated Event Raised**, set the **Health State** to **Critical**.
    c. Click **Next**.
13. On the **Configure Alerts** page, do the following:
    a. Check **Generate alerts for this monitor**.
    b. For **Generate an alert when:** leave the default of **The monitor is in a critical health state**.
    c. Leave the box **Automatically resolve the alert when the monitor returns to a health state** checked.
    d. For the **Alert name**, leave the default which is the name of the monitor or replace it with different text. This will be the name of the alert that appears in the Operations console when the alert is created.
    e. Leave the default **Priority** of **Medium**.
    f. Leave the default **Severity** of **Critical**. Note that you can change the alert severity to Warning even though the monitor is set to Critical
    g. In the **Alert description** box, type **Event 201 was detected $Data/Context/Count$ times between $Data/Context/TimeWindowStart$ and $Data/Context/TimeWindowEnd$. The first event was at $Data/Context/TimeWindowStart$. The last event was at $Data/Context/TimeWindowEnd$.**. Rather than typing in each of the $Data variables, you can select them by clicking the ellipse button and then selecting **Data** and the property.
    h. Click **Create**.

See Also

Event Monitors and Rules

Windows Events

Text Logs

WMI Events

Correlated Events

A correlated event monitor in Operations Manager uses two separate events in a particular time period to detect a single issue. This kind of monitor supports conditions where an issue cannot be identified by a single event alone.

When the first event is detected, a timer is triggered. If the second event is received within that period, the state change is triggered. If the second event is not received in the period, the timer is reset until the first event is received again. The monitor may be configured to better tune the specific conditions that must be met in order to perform correlation. These options include the following:

- Whether the events must be in chronological order. One of the events may always be expected before the other one, or they may be expected in either order.
- Whether the first or last occurrence of the first event should be used. If the first occurrence is specified, then each occurrence of the first event will have its own time window and search for corresponding occurrences of the second event. With the last occurrence specified, if the first event reoccurs with the time window, then the time window is extended based on the last event. The monitor can also be configured to reset the time window every time that the first event occurs. When the time window is reset, all previous occurrences of both events are ignored.
- The number of occurrences of the second event that must be received to trigger the state change. Instead of changing the health state after receiving a single instance of the two events, multiple instances of the second event may be required.
- Properties between the first and second event that must match for correlation to be performed. Instead of detecting two occurrences of each event, additional comparison may be required to determine whether the events are related. The monitor can, for example, confirm that a particular parameter matches between the two events to make sure that they match.

Correlated Events Example

The following table provides an example of a correlated event monitor by using the first and the last occurrence of the first event. The monitor uses the following details:

- Event Log A: Event 1
- Event Log B: Event 2

- Correlation interval: 2 minutes
- Number of occurrences of Event 2: 3
- Health state on correlation: Critical
- Reset Logic: Event reset using Event 3

Time	Event	First Occurrence	Last Occurrence
00:00:00	-	Healthy	Healthy
00:01:00	Event 1	Healthy	Healthy
01:30	Event 2	Healthy	Healthy
00:02:00	Event 2	Healthy	Healthy
00:02:30	-	Healthy	Healthy
00:03:00	Event 1	Healthy	Healthy
00:03:30	Event 2	Healthy	Healthy
00:04:00	Event 2	Healthy	Healthy
00:04:30	Event 1	Healthy	Healthy
00:05:00	Event 2	Critical	Healthy
05:30:00	Event 3	Healthy	Healthy
06:00:00	Event 1	Healthy	Healthy
06:30:00	Event 2	Healthy	Healthy
07:00:00	Event 1	Healthy	Healthy
07:30:00	Event 2	Healthy	Healthy
08:00:00	Event 2	Critical	Healthy
08:30:00	Event 2	Critical	Critical
09:00:00	Event 3	Healthy	Healthy

- The First Occurrence does not trigger a critical state when Event 2 is detected at 00:03:00 because the timer was reset at 00:03:00 which is 2 minutes after the first occurrence of Event 1 at 00:01:00.
- The First Occurrence triggers a critical state at 00:05:00 because Event 2 is detected 3 times within the 2 minutes since the first occurrence of Event 1 at 00:03:00. Event 1 starts a new time window at 00:03:00 because the time window from Event 1 at 00:01:00 would have expired.
- The First Occurrence triggers a critical state at 00:08:00 because Event 2 is detected 3 times within 2 minutes from Event 1 at 00:06:00.

- The First Occurrence resets its state to healthy at 00:05:30 and 00:09:00 because Event 3 is detected.

See Also

Event Monitors and Rules

Windows Events

Missing Events

Instead of detecting a particular event to identify an error condition, a missing event monitor in Operations Manager uses the absence of a particular event in a particular time window to determine an error. This supports applications that are expected to generate an informational event that indicates a successful operation or the success of a particular action.

For example, consider an application that performs a scheduled data transfer each evening and creates an event when it has completed successfully. A missing event monitor could be created that searches for the event in a particular time window each evening. If the event is detected, then the monitor remains in a healthy state. If it is not found, then it enters error state that indicates that the last transfer did not occur successfully.

Missing Event Example

The following table provides an example of a missing event monitor by using the following details:

- Event: Event 1
- Fixed Schedule: Su-Sa 2:00 AM – 3:00 AM
- Health state on missing event: Critical
- Reset Logic: Event reset using Event 3

Time	Event	Health State
00:00:00	-	Healthy
00:01:00	Event 1	Healthy
00:02:00	-	Healthy
00:03:00	-	Critical
00:04:00	-	Critical
00:05:00	Event 3	Healthy

- The critical state is triggered at 00:03:00 when Event 1 is not detected within the specified window.

See Also

Event Monitors and Rules

Windows Events

Correlated Missing Events

A correlated missing event monitor in Operations Manager determines an error by the absence of a particular event after the occurrence of another. This resembles the missing event monitor except that instead of searching for the missing event in a particular time window, the monitor searches for the event in a particular time after another event is first detected.

For example, consider an application that performs a backup each evening and creates an event when it starts and a second event when it has completed successfully. A correlated missing event monitor could be created that searches for the event in a particular time window each evening. If both events are detected, then the monitor remains in a healthy state. If the first is found, then the timer starts. If the time is reached before the second event is detected, then the state change is triggered to indicate that the last backup did not occur successfully.

Correlated Missing Events Example

The following table provides an example of a correlated missing event monitor by using the first and the last occurrence of the first event. The monitor uses the following details:

- Missing Event Log A: Event 1
- Missing Event Log B: Event 2
- Correlation interval: 2 minutes
- Number of occurrences of Event 2: 3
- Health state on correlation: Critical
- Reset Logic: Event reset using Event 3

Time	Event	First Occurrence	Last Occurrence
00:00:00	-	Healthy	Healthy
00:01:00	Event 1	Healthy	Healthy
1:30	Event 2	Healthy	Healthy
00:02:00	Event 2	Healthy	Healthy
00:02:30	Event 1	Healthy	Healthy
00:03:00	-	Critical	Healthy
00:03:30	Event 2	Critical	Healthy

Time	Event	First Occurrence	Last Occurrence
00:04:00	Event 2	Critical	Healthy
00:04:30	-	Critical	Critical
00:05:00	Event 3	Healthy	Healthy

- The First Occurrence triggers a critical state at 00:03:00 because Event 2 has not been detected 3 times in the 2 minute interval since the first occurrence of Event 1 at 00:01:00.
- The Last Occurrence does not trigger a critical state at 00:03:00 because Event 1 occurs at 00:02:30 resetting the timer. The critical state is not triggered until 00:04:30 when Event 2 has not been detected in the 2 minutes interval since the last occurrence of Event 1 at 00:02:30.
- The single occurrence of Event 3 at 00:05:00 resets both monitors to healthy.

See Also

Event Monitors and Rules

Windows Events

Event Monitor Reset

Unlike other kinds of monitors in System Center 2012 – Operations Manager, it may be difficult to define the criteria to return an event monitor to a healthy state. This is because applications often generate an event when a problem occurs but do not create a corresponding event when the problem has been corrected. For this reason, you have the following options for setting the healthy state for an event monitor.

Reset Logic	Description
Event Reset	A single specific event indicates that monitor should be reset.
Manual Reset	The monitor is never automatically reset. The user must manually reset the monitor.
Timer Reset	The monitor is automatically reset after a specified time.

Each of these methods is discussed at length in the following sections:

Event Reset

With *event reset*, the monitor is reset when a single occurrence of a specific event is detected. The event must be the same type as the event used for detecting the error condition. For example, a Windows event monitor might specify an event with a particular event source and number to indicate an error condition. Another Windows event with the same event source but a different number might indicate that the error in the application was corrected.

Event reset can only be used if the application provides an event indicating the particular error was corrected. Many applications create an event when an error occurs but may not create a corresponding event that indicates that the error was corrected. Event reset cannot be used in this case.

Manual reset

With *manual reset*, the monitor never returns to a healthy state automatically. The user must determine whether the problem was corrected and then select the monitor in the Health Explorer and select **Reset Health**.

The advantage to this strategy is that a monitor can be used for issues that do not create an event that indicates a healthy state. The monitor can affect the health state of the managed object instead of creating a simple alert from a rule. The downtime will be recorded for the object in the State Change Events in the Operations Console and in any availability reports.

There are multiple implications of this strategy that should be considered. The first is the additional work required from the user because the monitor will never automatically reset. It can also result in too much downtime being recorded if the user waits a long time before performing the reset. The problem may have been corrected fairly quickly, but the healthy state will not be recorded until the user performs the reset.

Use of manual reset should be especially cautioned for monitors where there is a potential for a single problem to affect multiple instances of the target class. Because users cannot reset the monitor for multiple instances in the Operations Console, the user would be required to manually open the Health Explorer for each instance to perform this action. Depending on the number of instances, this could result in significant effort for the user.

Timer Reset

A timer reset acts the same as a manual reset except that if the user does not manually reset the monitor after a specified time, it will reset automatically. One use of this kind of reset is for issues that continuously log error events until the problem is corrected. Instead of using another event to indicate that the problem was corrected, the previously detected error event for a specified period can be used as the success criteria.

The timer reset can be used in the place of a manual reset providing the advantage of automatically resetting after a while if the user does not perform a manual reset.

Which reset should I use?

- If the application you're monitoring creates an event when the problem has been corrected, use Event Reset. This is the preferred method since the monitor will return to a healthy state as soon as soon as is appropriate without any user intervention. Any alert generated from the monitor can also be closed automatically.
- If the application you're monitoring does not create an event when the problem has been corrected, then you should use Manual Reset or Timer Reset. Refer to the descriptions of each above to determine which strategy is most appropriate for your specific purposes.

See Also

Event Monitors and Rules

Windows Events

Text Logs

UNIX/Linux Shell Command Alerts

UNIX/Linux shell commands can be used to detect events and generate alerts. When the rule is run, the provided command is executed on the agent, and if the output matches the provided filter, the alert is generated.

Target

Rules and monitors run on the agent computer of each instance of the target class, and they usually access data on the local computer. The target must be a UNIX and Linux computer type, such as **UNIX/Linux Computer**, **Linux Computer**, etc.

UNIX/Linux Shell Command (Alert) Wizard Options

When you run a UNIX/Linux Shell Command rule wizard, you will need to provide values for options in the following tables. Each table represents a single page in the wizard.

Rule Type

The Rule Type page includes basic settings for the rule including its type and the management pack file to store it in.

Option	Description
Select the type of rule to create	To create an alert-generating rule based on the execution of an UNIX/Linux shell command, select **UNIX/Linux Shell Command (Alert)**.

Option	Description
Management Pack	Management pack file to store the rule or monitor.For more information on management packs, see Selecting a Management Pack File.

General

The General page includes general settings for the rule including its name, category, target, and the management pack file to store it in.

Option	Description
Name	The name used for the rule. The name appears in the **Rules** view in the **Authoring** pane. When you create a view or report, you can select this name to use the data collected by it.
Description	Optional description of the rule.
Rule Category	The category for the rule. For a performance collection rule, this should be **Performance Collection**. For an alerting rule, this should be **Alert**.
Rule Target	The class to use for the target of the rule. For more information on targets, see Understanding Classes and Objects.
Rule is enabled	If checked, the rule is enabled and the shell command will run according to the schedule. If unchecked, the rule is not enabled and the script will not run. The rule can be enabled for a group of target objects by creating an override to enable the rule.

Schedule

The following options are available on the Schedule page of the wizard.

Option	Description
Run every	Frequency that the script should be run. This should typically not be less than 5 minutes.

Option	Description
Synchronize at	If enabled, the schedule will be synchronized to occur at the specified time.

UNIX/Linux Shell Command

The following options are available on the **Shell Command Details** page of the wizard.

Option	Description
Command	The shell command to execute. This can be the full path to a program or script, a command, or a one-line sequence of multiple commands (using pipeline operators).
Run As Profile	Either the “UNIX/Linux Action Account” or “UNIX/Linux Privileged Account” profile. Select the profile that associates the required account credentials with the task target. The associated account will be used to execute the command.
Timeout (seconds)	The number of seconds that the command can run before the agent stops it. This prevents problem commands from running continuously and putting excess overhead on the agent computer.

Filter Expression

The Filter Expression page allows you to filter for output to generate an alert. The alert is generated only if the output of the shell command matches the filter expression.

Property Name	Description
Filter one or more events	An expression that filters output of the shell command. For more information on building expressions see Expressions The Parameter Name syntax for command execution output is: **StdOut**: //*[local-name()="StdOut"]**StdErr**: //*[local-name()="StdErr"]**Return Code**: //*[local-name()="ReturnCode"]

Configure Alerts

The Configure Alerts page is used to define alert properties for the rule. Its options are explained in Alerts.

Creating UNIX/Linux Shell Command (Alert) Rules

The following procedure shows how to create an UNIX/Linux shell command alerting rule in Operations Manager with the following details:

1. Runs on all UNIX/Linux Computers every 15 minutes
2. Generates an alert if the file “/tmp/error” exists

To create a UNIX/Linux shell command alerting rule

1. If you don’t have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. In the Operations console, select the **Authoring** workspace, and then select **Rules**.
3. Right-click **Rules** and select **Create a new rule**.
4. On the **Rule Type** page, do the following:
   a. Expand **Alert Generating Rules**, expand **Event Based**, and then click **UNIX/Linux Shell Command (Alert)**.
   b. Select the management pack from step 1.
   c. Click **Next**.
5. On the **General** page, do the following:
   a. In the **Rule Name** box, type **Alert on Error File Exists**.
   b. In the **Rule Category** box, select **Alert**.
   c. Next to **Rule Target** click **Select** and then select **UNIX/Linux Computer**.
   d. Leave **Rule is enabled** selected.
   e. Click **Next**.
6. On the **Schedule** page, do the following:
   a. In the **Run Every** boxes, input **15** and **Minutes**.
   b. Click **Next**.
7. On the **Shell Command Details** page, do the following:
   a. In the **Command** box, type **ls /tmp/error | wc –l**. This command sequence will return a 1 if the file “/tmp/error” exists, and a 0 if it does not.
   b. In the **Run As Profile** box, select the **UNIX/Linux Action Account** profile.
   c. In the **Timeout (Seconds)** box, input **120**.
   d. Click **Next**.
8. On the **Filter Expression** page, do the following:
   a. Configure an **And** expression with the entries:
      i. **//*[local-name()=”StdOut”] equals 1**

ii. //*[local-name()=”ReturnCode”] equals 0

b. This will trigger an alert whenever the value of the shell command output is **1**, and the command executed successfully.

9. On the **Configure Alerts** page, do the following:
   a. In the **Alert name** box, type **Error File Found**.
   b. In the **Alert description** box, type **The file /tmp/error was found on the computer:**
   c. Click the **[…]** button.
   d. Click **Target** and select **Network Name**.
   e. Click **OK**.
   f. Click **Create**.

See Also

Event Monitors and Rules

Alerts

Performance Monitors and Rules

Performance counters are numeric data that is used to measure the performance of some aspect of the application. Performance data usually comes from Windows performance counters but can also come from WMI and from scripts. Measuring and collecting performance data with scripts is covered in Script Monitors and Rules.

Performance Monitors and Rules Topics

Details on each performance data source are provided in the following sections. This includes the information that is required to retrieve the required data, properties available in the resulting data, and what workflows the performance data source supports.

- Performance Monitors

  Details on the different types of calculations that can be performed for performance monitors.
- Windows Performance Collection Rules

  Rules and monitors using Windows performance counters which are sampled at specified intervals.
- WMI Performance

  Rules and monitors that run a WMI query at specified interval and uses the value of a numeric property for performance data.
- UNIX/Linux Shell Command Performance Collection Rules

  Rules that execute a UNIX/Linux command, script, or one-line sequence of multiple commands (using pipeline operators) and collect the output as numerical performance data.

Performance Monitors

Multiple kinds of calculations may be performed to determine the threshold for a performance monitor in Operations Manager. These threshold types are listed in the following table:

Threshold Type	Number of States	Description
Average Threshold	2	Compare the average of multiple collected values to a threshold.
Consecutive Samples	2	Compare several consecutive values to a threshold. All collected values must match the threshold criteria.
Delta Threshold	2	Compare the change between two consecutive values to a threshold.
Double Threshold	3	Compare a single collected value to two thresholds with one that indicates a Warning state and the other that indicates a Critical state.
Simple Threshold	2	Compare a single collected value to a threshold.

Each kind of logic is described in detail in the following sections:

Simple Threshold

The *simple threshold* type is the most basic kind of performance threshold. A single numeric value is provided for the threshold. This threshold is compared to the measured value of the performance data.

Simple threshold supports a two state monitor. One state is set by a performance value equal to or less than the threshold. The other state is set by a performance value greater than the threshold.

Double Threshold

The *double threshold* type is similar to the simple threshold type but allows for two thresholds to be specified. Each threshold is compared to the measured value of the performance data.

Double threshold supports a three state monitor. One state is set by a performance value less than the low threshold. Another state is set by a performance value that is greater than or equal to the low threshold or one that is less than or equal to the high threshold. Another state is set by a value that is greater than the high threshold.

The following table provides an example of a double monitor by using the following details:

- Sample rate: 5 minutes
- Low threshold value: 10
- High threshold value: 15
- Over Upper Threshold State: Critical
- Between Thresholds State: Warning
- Under Lower Threshold State: Healthy

Time	Value	State
00:00:00	5	Healthy
00:05:00	10	Warning
00:10:00	12	Warning
00:15:00	9	Healthy
00:20:00	12	Warning
00:25:00	16	Critical
00:30:00	15	Critical
00:35:00	8	Healthy

- The warning threshold is first exceeded at 00:05:00, but the value does not exceed the critical threshold.
- The critical threshold is first exceeded at 00:25:00 when the state is changed from warning to critical.
- The state is returned to a healthy state at 00:15:00 and 00:35:00 when the sampled value is less than the warning threshold.

Average Threshold

The *average threshold* type calculates the average of a specified number of consecutive samples and compares it to the specified threshold.

Average threshold supports a two state monitor. One state is set by an average performance value equal to or less than the threshold. The other state is set by an average performance value greater than the threshold.

The following table provides an example of an average threshold monitor by using the following details:

- Sample rate: 5 minutes
- Threshold value: 10
- Number of samples: 3
- Over Threshold State: Critical
- Under Threshold State: Healthy

Time	Value	Average	State
00:00:00	5	-	Healthy
00:05:00	10	-	Healthy
00:10:00	12	9.0	Healthy
00:15:00	9	10.3	Critical
00:20:00	12	11.0	Critical
00:25:00	14	11.7	Critical
00:30:00	11	12.3	Critical
00:35:00	4	9.7	Healthy

- Because the specified number of samples for the average calculation is 3, no value is evaluated until the third sample.
- The value of 12 sampled at 00:10:00 exceeds the threshold value, but the calculated average from the last 3 samples is 9.0, which is under the threshold. The state is not changed.
- The value of 9 sampled at 00:15:00 does not exceed the threshold. But the calculated average from the last 3 samples is 10.3 which does exceed the threshold. The state is changed.
- The monitor does not return to a healthy state until 00:35:00 when the average from the last 3 samples drops the under the threshold value.

Consecutive Samples

The *consecutive threshold* type compares the threshold value to the performance counter for several consecutive samples. This supports monitors that should not be triggered by only a single value exceeding a threshold. The threshold must be exceeded multiple consecutive times to trigger a change in state.

Consecutive threshold supports a two state monitor. One state is set by the value being either greater than or less than the threshold value for each consecutive sample. The other state is set by a single sample not matching the other criteria.

The following table provides an example of a consecutive sample monitor by using the following details:

- Sample rate: 5 minutes

- Threshold value: greater than or equal to 10
- Number of samples: 3
- Over Threshold State: Critical
- Under Threshold State: Healthy

Time	Value	State
00:00:00	5	Healthy
00:05:00	10	Healthy
00:10:00	12	Healthy
00:15:00	9	Healthy
00:20:00	12	Healthy
00:25:00	14	Healthy
00:30:00	11	Critical
00:35:00	8	Healthy

- The threshold is exceeded by the values sampled at 00:05:00 and 00:10:00, but the value at 00:15:00 is under threshold and resets the count.
- The value at 0:30:00 is the first time that 3 consecutive values have been sampled that exceed the threshold, so the state is changed.
- The single value at 00:35:00 is under the threshold and resets the monitor to a healthy state.

Delta Threshold

The *delta threshold* type compares the threshold value to the difference between two performance values. This might be two consecutive values or two values separated by a specified number of samples.

Delta threshold supports a two state monitor. One state is set by the difference of two values being greater than the threshold value. The other state is set by the difference of two samples being equal to or less than the threshold value.

The following table provides an example of a delta threshold monitor by using the following details:

- Sample rate: 5 minutes
- Threshold value: 10
- Number of samples: 3
- Over Threshold State: Critical
- Under Threshold State: Healthy

Time	Value	Delta	
00:00:00	7	-	Healthy
00:05:00	8	-	Healthy
00:10:00	13	-	Healthy
00:15:00	16	9	Healthy
00:20:00	21	13	Critical
00:25:00	24	11	Critical
00:30:00	25	9	Healthy

- Because the specified number of samples that the delta should be calculated from the current sampled value to the value 3 samples behind, no value is evaluated until the fourth sample.
- The delta calculation exceeds the threshold value at 00:20:00, and the state is changed.
- The monitor is reset at 00:30:00 when the delta calculation falls under the threshold.

To Create

Windows Performance Collection Rules

To define a collection rule in Operations Manager based on a Windows performance counter, the object name and counter name of the performance counter to sample must be defined with a frequency that specifies how frequently to sample the data. The instance name only has to be specified if the same counter will be collected for multiple objects on the same agent. If this is the case, a $Target variable will typically be used for the value in the instance name in order to differentiate between the performance values for different objects. The counter must be available on the agent computer that is running the rule or an error will be created in the Operations Manager event log on the agent.

Windows Performance Collection Wizard Options

When you run the Windows performance collection wizard, you will need to provide values for options in the following tables. Each table represents a single page in the wizard.

General

The **General** page includes general settings for the rule including its name, category, target, and the management pack file to store it in.

Option	Description
Rule Name	The name used for the rule. This appears in the **Rules** view in the **Authoring** pane. When you create a view or report, you can select this name to use the data collected by it.
Description	Optional description of the rule.
Management Pack	Management pack to store the rule. For more information on management packs, see Selecting a Management Pack File.
Rule Category	The category for the rule. For a performance collection rule, this should be **Performance Collection**.
Rule target	The class to use for the target of the rule. The rule will be run on any agent that has at least one instance of this class. For more information on targets, see Understanding Classes and Objects.

Performance Counter

The **Performance Counter** page includes the definition of the performance counter to collect and the frequency it should be collected.

Option	Description
Object	Text for the Object name. This is required. You can type in the name of the object or select a property from the target.
Counter	Name of the performance counter.
Instance	Text for the Instance name. This only required if the performance counter has multiple instances. You can type in the name of the instance or select a property from the target.
Include all instances for the selected counter	If select, the **Instance** box is disabled and the value for each instance of the performance counter is collected.
Interval	Specifies the frequency to collect the performance counter.

Optimized Collection

The **Optimized Collection** page allows to you to enable and configure optimized collection for the counter. If you select optimization for a collection rule, a value is only collected if it differs from the previous sample by a specified tolerance, either an absolute value or a percentage. This helps reduce network traffic and the volume of data stored in the Operations Manager database. Optimization should be used for performance counters that are expected to only change gradually. For counters that are expected to very significantly from one value to the next, optimized collection should be disabled.

Option	Description
Use Optimization	Specifies whether optimization should be enabled for the counter. If it is disabled, then every sampled value will be collected.
Absolute number	Specifies a value that the number must vary between the current sample and the previous sample for the value to be collected. The value can change in either positive or negative direction.
Percentage	Specifies a percentage of the previous sample that the difference between the current value and the previous value must be for the value to be collected. The change can be in either positive or negative direction.

Creating Windows Performance Collection Rules

Use the following procedures to create a Windows performance collection rule in Operations Manager with the following details:

- Runs on all agents with a particular service installed.
- Collects the % Privileged Time for the selected service.

To create a Windows performance collection rule in Operations Manager

1. If you don't have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. Create a new target using the process in To create a Windows Service template. You can use any service installed on a test agent for this template.
3. In the Operations console, select the **Authoring** workspace, and then select **Rules**.

4. Right-click **Rules** and select **Create a new rule**.
5. On the **Rule Type** page, do the following:
   a. Expand **Collection Rules**, expand **Performance Based**, and then click **Windows Performance**.
   b. Select the management pack from step 1.
   c. Click **Next**.
6. On the **General** page, do the following:
   a. In the **Rule name** box, type **% Privileged Time**.
   b. In the **Rule Category** box, select **Performance Collection**.
   c. Next to **Rule Target** click **Select** and then select the name of the target that you created in step 2.
   d. Leave **Rule is enabled** selected.
   e. Click **Next**.
7. On the **Performance Counter** page, do the following:
   a. Click **Select**.
   b. In the **Select Performance Counter** dialog box, type a computer name or browse to a **Computer** that has the performance counter installed.

      Note
      The name of the computer is not recorded in the rule. The computer is only used to retrieve the details of the performance counter.

   c. In the **Object** dropdown, select **Process**.
   d. In **Select counter from list**, select **% Privileged Time**.
   e. Click **OK**.
   f. Clear the text in the **Instance** box.
   g. Click the arrow to the right of the **Instance** box and select **Service Name (Windows Service)**.

      Note
      You can also select the name of the service process when you select the counter. The strategy used here is to use the $Target variable to use the Service Name property of the target class. This will resolve to the name of the service when the rule runs. This is to illustrate the use of $Target variables.

   h. Leave the **Interval** at its default value of **15 minutes**.
   i. Click **Next**.
8. On the **Optimized Performance Collection Settings** page, do one of the following:
   - Leave the **Use Optimization** option unselected.

     Note
     If you select optimization for a collection rule, a value is only collected if it

differs from the previous sample by a specified tolerance, either an absolute value or a percentage. This helps reduce network traffic and the volume of data stored in the Operations Manager database. Optimization should be used for performance counters that are expected to only change gradually. In this example, the privileged time of the process is expected to vary significantly between samples so it would not benefit from optimized collection.

- Click **Create**.

See Also

Performance Monitors and Rules

Performance Monitors

WMI Performance

WMI performance refers to numeric data that is retrieved from a WMI query. This lets performance data be retrieved that is not available from a performance counter and without using the complexity and overhead of a script. The monitor or rule runs the query on a specified schedule and maps the value of the specified numeric field into the value property of the performance data.

For example, a monitor might have to track the size of a particular file. This might be a log file that indicates a particular problem when it exceeds a particular size. The name and size of the file could be retrieved from a query similar to the following:

```
Select Name, FileSize from CIM_DataFile Where Name = 'C:\\MyApp\\MyAppLog.txt'
```

The monitor could run this query regularly by using the FileSize property for the value of the performance data and the Name property for the Instance property.

The WMI query returns a property bag with each property returned from the query. This set of properties will vary, depending on the class returned and the properties specified in the query. For more information about property bags, see Property Bags.

Options

When you run the Windows performance collection wizard, you will need to provide values for options in the following tables. Each table represents a single page in the wizard.

General

The **General** page includes general settings for the rule including its name, category, target, and the management pack file to store it in.

Option	Description
Rule Name	The name used for the rule. This appears in the **Rules** view in the **Authoring** pane. When you create a view or report, you can select this name to use the data collected by it.
Description	Optional description of the rule.
Management Pack	Management pack to store the rule. For more information on management packs, see Selecting a Management Pack File.
Rule Category	The category for the rule. For a performance collection rule, this should be **Performance Collection**.
Rule target	The class to use for the target of the rule. The rule will be run on any agent that has at least one instance of this class. For more information on targets, see Understanding Classes and Objects.

WMI Configuration

The **Performance Counter** page includes the definition of the performance counter to collect and the frequency it should be collected.

Option	Description
WMI Namespace	The namespace containing the class used by the query.
Query	Name of the performance counter.
Query Interval	The frequency in seconds to run the query and collect the

Performance Mapper

The **Performance Mapper** page is used to define values for the properties of the performance data being collected.

Option	Description
Object	Text for the Object name. This is required. You can type in the name of the object or select a property from the target or from the property bag.
Counter	Text for the Counter name. This is required. You can type in the name of the object or select a property from the target or from the property bag.
Instance	Text for the Instance name. This only required if the target of the rule has multiple instances. You can type in the name of the object or select a property from the target or from the property bag.
Value	Numeric for the value for the performance. This will usually be a $Data variable to use a value from the property bag.

Creating WMI Performance Collection Rules

Use the following procedure to create a WMI performance collection rule in Operations Manager with the following details:

- Runs on all agents with a particular service installed.
- Collects the size of a file called C:\MyApp\MyAppLog.txt.

To create a WMI performance collection rule

1. If you don't have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. Create a new target using the process in To create a Windows Service template. You can use any service installed on a test agent for this template.
3. In the Operations console, select the **Authoring** workspace, and then select **Rules**.
4. Right-click **Rules** and select **Create a new rule**.
5. On the **Rule Type** page, do the following:
   a. Expand **Collection Rules**, expand **Performance Based**, and then click **WMI Performance**.
   b. Select the management pack from step 1.
   c. Click **Next**.
6. On the **General** page, do the following:

a. In the **Rule name** box, type **Collect File Size with WMI**.
b. In the **Rule Category** box, select **Performance Collection**.
c. Next to **Rule Target** click **Select** and then select the name of the target that you created in step 2.
d. Leave **Rule is enabled** selected.
e. Click **Next**.

7. On the **WMI Configuration** page, do the following:
   a. In the **WMI Namespace** box, type **root\cimv2**.
   b. In the **Query** box, paste the following WMI query.

```
Select Name,FileSize From CIM_DataFile Where Name =
'C:\\Logs\\MyAppFile.txt'
```

   c. In the **Query Interval** box, type **900**.
   d. Click **Next**.
8. On the **Performance Mapper** page, do the following:
   a. In the **Object** box, type **MyApplication**.
   b. In the **Counter** box, type **File Size**.
   c. In the **Instance** box, type **$Data/Property[@Name='Name']$**.
   d. In the **Value** box, type **$Data/Property[@Name='FileSize']$**.
   e. Click **Finish**.

See Also

Performance Monitors and Rules

Performance Monitors

UNIX/Linux Shell Command Performance Collection Rules

To define a collection rule in Operations Manager based on the output of an UNIX/Linux shell command, the command execution details, object name and counter name of the performance counter must be defined with a frequency that specifies how frequently to sample the data.

UNIX/Linux Shell Command Performance Collection Wizard Options

When you run the UNIX/Linux shell command performance collection wizard, you will need to provide values for options in the following tables. Each table represents a single page in the wizard.

Rule Type

The Rule Type page includes basic settings for the rule including its type and the management pack file to store it in.

Option	Description
Select the type of rule to create	To create a performance collection rule based on the execution of an UNIX/Linux shell command, select **UNIX/Linux Shell Command (Performance)**.
Management Pack	Management pack file to store the rule or monitor.For more information on management packs, see Selecting a Management Pack File.

General

The **General** page includes general settings for the rule including its name, category, target, and the management pack file to store it in.

Option	Description
Rule Name	The name used for the rule. This appears in the **Rules** view in the **Authoring** pane. When you create a view or report, you can select this name to use the data collected by it.
Description	Optional description of the rule.
Management Pack	Management pack to store the rule. For more information on management packs, see Selecting a Management Pack File.
Rule Category	The category for the rule. For a performance collection rule, this should be **Performance Collection**.
Rule Target	The class to use for the target of the rule. The rule will be run on any agent that has at least one instance of this class. For more information on targets, see Understanding Classes and Objects.
Rule is Enabled	If checked, the rule is enabled and the shell command will run according to the schedule. If unchecked, the rule is not enabled and the

Option	Description
	script will not run. The rule can be enabled for a group of target objects by creating an override to enable the rule.

Schedule

The following options are available on the **Schedule** page of the wizard.

Option	Description
Run every	Frequency that the script should be run. This should typically not be less than 5 minutes.
Synchronize at	If enabled, the schedule will be synchronized to occur at the specified time.

UNIX/Linux Shell Command

The following options are available on the **Shell Command Details** page of the wizard.

Option	Description
Command	The shell command to execute. This can be the full path to a program or script, a command, or a one-line sequence of multiple commands (using pipeline operators).
Run As Profile	Either the “UNIX/Linux Action Account” or “UNIX/Linux Privileged Account” profile. Select the profile that associates the required account credentials with the task target. The associated account will be used to execute the command.
Timeout (seconds)	The number of seconds that the command can run before the agent stops it. This prevents problem commands from running continuously and putting excess overhead on the agent computer.

Filter Expression

Shell commands used in performance collection rules must return only a single numeric value, or errors will be encountered when collecting the performance value. The **Filter Expression** page allows you to filter the command output to ensure that the command output is acceptable. It is recommended that the default expression filter is used to only collect performance data when the value is numeric and the command executed successfully.

Property Name	Description
Filter one or more events	An expression that filters output of the shell command. For more information on building expressions, see Expressions. The Parameter Name syntax for command execution output is: **StdOut**: //*[local-name()="StdOut"] **StdErr**: //*[local-name()="StdErr"] **Return Code**: //*[local-name()="ReturnCode"] The default expression filters that the StdOut value is numeric, and that the script executed successfully, with the expression definition of: **//*[local-name()=”StdOut”] Matches Regular Expression ^[-+]?\d*[0-9]*(\.[0-9]+)?[Ee]?[-+]?[0-9]*$ //*[local-name()=”ReturnCode”] Equals 0**

Performance Mapper

The **Performance Mapper** page defines the mapping of the command output to a performance counter.

Option	Description
Object	Text for the Object name. This is required. You can type in the name of the object or select a property from the target.
Counter	Name of the performance counter.
Instance	Text for the Instance name. This only required if the performance counter has multiple instances. You can type in the name of the instance or select a property from the target.
Value	The variable that defines the value collected as a performance counter value. To collect the

Option	Description
	value returned by the command as StdOut, use **$Data//*[local-name()=”StdOut”]$**. To collect the value returned by the command as ReturnCode, use **$Data//*[local-name()=”ReturnCode”]$**

Creating UNIX/Linux Shell Command Performance Collection Rules

Use the following procedures to create a Windows performance collection rule in Operations Manager with the following details:

- Runs on all UNIX/Linux Computers, every 15 minutes
- Collects the count of files in the /tmp path as a performance counter

To create an UNIX/Linux shell command performance collection rule in Operations Manager

1. If you don’t have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. In the Operations console, select the **Authoring** workspace, and then select **Rules**.
3. Right-click **Rules** and select **Create a new rule**.
4. On the **Rule Type** page, do the following:
   a. Expand **Collection Rules**, expand **Probe Based**, and then click **UNIX/Linux Shell Command (Performance)**.
   b. Select the management pack from step 1.
   c. Click **Next**.
5. On the **General** page, do the following:
   a. In the **Rule name** box, type **/tmp File Count**.
   b. In the **Rule Category** box, select **Performance Collection**.
   c. Next to **Rule Target**, click **Select** and then select **UNIX/Linux Computers**.
   d. Leave **Rule is enabled** selected.
   e. Click **Next**.
6. On the **Schedule** page, do the following:
   a. In the **Run Every** boxes, input **15** and **Minutes**.
   b. Click **Next**.
7. On the **Shell Command Details** page, do the following:
   a. In the **Command** box, type **ls /tmp | wc –l**. This command sequence will return the count of the files in /tmp.

b. In the **Run As Profile** box, select the **UNIX/Linux Action Account** profile.
c. In the **Timeout (Seconds)** box, input **120**.
d. Click **Next**.

8. On the **Filter Expression** page, do the following:
   a. Click **Next** (to use the default expression filter that validates StdOut is a numeric value, and the command executed successfully).
9. On the **Performance Mapper** page, do the following:
   a. On the **Object** line, click **[…]**.
   b. Click **Target** and select **Network Name**.
   c. Click **OK**.
   d. In the **Counter** box, type **File Count**.
   e. In the **Instance** box, type **/tmp**.
   f. In the **Value** box, type **$Data///*[local-name()='StdOut']$**
   g. Click **Create**.

See Also

Performance Monitors and Rules

Performance Monitors

Script Monitors and Rules

Monitoring scripts are used when the required data cannot be collected through other standard means such as an event or performance counter. The script collects data from information on the agent and creates a property bag by using the MOM.ScriptAPI object that is installed with the Operations Manager agent.

Monitoring scripts may be written in any script language that can access the MOM.ScriptAPI object that is installed on all Operations Manager agents. You can use the Operations console to create scripts in VBScript or JScript. To use a Windows PowerShell script, you must use another Authoring tool such as the Operations Manager R2 Authoring Console or the Visio Management Pack Designer.

Property Bags

Monitoring scripts send any output data as a property bag so that it can be evaluated in an expression for a monitor or mapped into performance data or an event for a collection rule. A property bag is a set of values that each has a name. Any name can be assigned although it is a best practice to use a name descriptive of the particular value. A property bag only exists during the life of the workflow. The next time that the workflow runs, the script is run and creates a new property bag with new values.

One property bag can have any number values, although the whole set of data may not exceed 4 MB. Most scripts will only require some values with a total size far under this limit. There is no requirement for all the values to be used by the workflow.

Scripts create property bags by using the CreatePropertyBag method on the MOM.ScriptAPI object. The workflow uses values from a property bag with a $Data variable that uses the following syntax:

```
$Data/Property[@Name="PropertyName"]
```

For example, a script creating performance data might create a property bag with values in the following table. This table shows the name of the value created by the script and the corresponding $Data variable that would be used to map the property bag data to performance data.

Property Bag Value Name	Sample Value	Variable
ObjectName	MyObject	$Data/Property[@Name='ObjectName']$
CounterName	MyCounter	$Data/Property[@Name='CounterName']$
InstanceName	MyInstance	$Data/Property[@Name='InstanceName']$
Value	10	$Data/Property[@Name='Value']$

Script Structure

The following code shows a sample monitoring script to illustrate the basic structure of a monitoring script. This sample script has the following characteristics.

- Accepts arguments for the name of the computer that is running the script and a path of the location of the application.
- Creates a property bag with the values named ComputerName, InstanceName, and PerfValue.

```
sComputerName = WScript.Arguments(0)
sApplicationPath = WScript.Arguments(1)

Set oAPI = CreateObject("MOM.ScriptAPI")
Set oBag = oAPI.CreatePropertyBag()

oBag.AddValue "ComputerName", sComputerName
```

```
oBag.AddValue "InstanceName", "MyInstance"
oBag.AddValue "Value", 1.0

oAPI.Return(oBag)
```

Details of each section of the script are discussed here.

```
sComputerName = WScript.Arguments(0)
sApplicationPath = WScript.Arguments(1)
```

The first two lines of the script accept arguments. These values would be expected to be in the Arguments parameter of the rule or monitor running the script. The script can use any number of arguments that are required for the logic of the script.

```
Set oAPI = CreateObject("MOM.ScriptAPI")
Set oBag = oAPI.CreatePropertyBag()
```

The next two lines create a property bag. These lines will also be unchanged in most monitoring scripts. The main purpose of the rest of the script will be to add values to the property bag by using data that is collected from the agent computer.

```
oBag.AddValue "ComputerName", sComputerName
oBag.AddValue "InstanceName", "MyInstance"
oBag.AddValue "Value", 1.0
```

After the property bag is created, any number of values can be added to it. You do this with the AddValue method on the property bag object by using the name of the item followed its value. This example uses explicit values. In actual monitoring script, additional code would be expected that would collect information from the agent computer to include in these values.

```
oAPI.Return(oBag)
```

After all values are added to the property bag, it is returned into the workflow. This line is required, and without it the property bag is discarded when the script ends. This method is only used when the script creates only a single property bag. For more information about scripts that return multiple property bags and conditions when such a strategy is used, refer to the Cookdown section of the System Center Operations Manager 2007 R2 Authoring Guide.

Script Arguments

Most scripts use arguments, which are values that are sent to the script from the command line when the script is run. Using arguments allows a single script to be used for multiple scenarios without modifying the script itself.

In a monitoring script, arguments are critical because there may be information that the script requires that will be different on each agent where the script runs. Any property of the target object for the monitor or rule can be used for the value of a script argument. This value is resolved individually on each agent at the time that the script is run.

Arguments are accessed in the Operations console from the **Parameters** button. Individual arguments should be separated by spaces in the order that they are accessed in the script. This is identical to the command line that would be provided if the script were run on a command line.

Each argument can be either an explicit value or a $Target variable to use the value of a property on the target object. Any $Target variables are resolved when the script is run so that the script is provided with the resolved values on the command line. You can type in the $Target variable if you know the proper syntax. It is easier though to select the property from **Target** button which will list all of the properties of the target object and its parents.

Important

Any $Target variable that might resolve to a value that includes a space should be enclosed with quotation marks. If a value includes spaces and does not have quotation marks, then it will be seen by the script as two separate arguments. The quotation marks will ensure that the value is seen as a single argument. If you select the property from **Target** menu, it will not include the quotation marks for you. You need to type these in after selecting the property.

For example, the sample script earlier expects two arguments for the computer name and the application path. Assuming this was part of a monitor or rule targeted at a class hosted by the **Windows Computer** class, the computer name could be retrieved from the PrincipalName property. If the application path were a property on the target class, then the arguments might look similar to the following example. Notice the quotation marks around the ApplicationPath property, because this could resolve to a value that contains a space.

```
$Target/Host/Property[Type="Windows!Microsoft.Windows.Computer"]/PrincipalName$
"$Target/Property[Type="MyApp.MyClass"]/ApplicationPath$"
```

Assuming that you gave the script a name of **MyScript.vbs**, the computer name was **MyServer01**, and the application path was **C:\Program Files\Contoso\My Application**, the command line that would be run for this script would be:

```
MyScript.vbs MyServer01 "C:\Program Files\Contoso\My Application"
```

Script Monitors and Rules Topics

- Script Collection Rules

  Creating a rule that uses a script to collect performance or event data.
- Script Monitors

  Creating a monitor that evaluates the results of a script to set its health state.
- UNIX/Linux Shell Command Monitors

  Creating a monitor that evaluates the output of execution of an UNIX/Linux command, script, or one-line sequence of multiple commands (using pipeline operators).

Script Collection Rules

Script collection rules run a script on a schedule and store its output as either performance data or an event. As part of creating the rule, you need to specify which property bag values from the script or properties from the target object that will be used for different properties of the event or performance data being created.

Options

When you run the script collection wizard, you will need to provide values for options in the following tables. Each table represents a single page in the wizard.

General

Option	Description
Rule Name	The name used for the rule. This appears in the **Rules** view in the **Authoring** pane.
Description	Optional description of the rule.
Management Pack	Management pack to store the monitor. For more information on management packs, see Selecting a Management Pack File.
Rule Category	The category for the rule. For an event collection rule, this should be **Event Collection**. For a performance collection rule, this should be **Performance Collection**.
Rule target	The class to use for the target of the rule. The rule will be run on any agent that has at least one instance of this class. For more information

Option	Description
	on targets, see Understanding Classes and Objects.

Schedule

The **Schedule** page defines the schedule to run the script. The script will run indefinitely according to this schedule until the rule is disabled or deleted or the management pack is uninstalled.

Option	Description
Run every	Frequency that the script should be run. This should typically not be less than 5 minutes.
Synchronize at	If enabled, the schedule will be synchronized to occur at the specified time.

Script

The **Script** page contains the body of the script itself and its parameters. You can type the script directly into the dialog box, but you will usually write it using another text editor and then copy the text of the script and paste it. This allows you to use a more functional editing tool and test the script on a command line before including it in the management pack.

Option	Description
File Name	Name of the script. Must have either a .vbs or .js extension depending on its language. There is no requirement to make this name unique because each script is provided its own temporary directory on the agent.
Timeout	The number of seconds that the script can run before the agent stops it. This prevents problem scripts from running continuously and putting excess overhead on the agent computer. The timeout value assigned to a script should allow enough time for the script to run under ordinary conditions, but should be less than the interval that the script is scheduled to run. If a script is configured to have a timeout value

Option	Description
	greater than its duration, then possibly multiple copies of the script could be running concurrently.
Script	The body of the script.
Parameters	Click to provide values for any arguments in the script. For more information, see Script Arguments.

Performance Mapper (Performance Collection Only)

The **Performance Mapper** page is used to define values for the properties of the performance data being collected.

Option	Description
Object	Text for the Object name. This is required.
Counter	Text for the Counter name. This is required.
Instance	Text for the Instance name. This only required if the target of the rule has multiple instances.
Value	Numeric for the value for the performance

Event Mapper (Event Collection Only)

The **Event Mapper** page is used to define values for the properties of the event that will be collected. The value for each field will either be an explicit string of text, a value from the property bag of the script, or the value of a property of the target object.

Option	Description
Computer	The name of the computer that the event was logged on. This will usually be a $Target variable for the Principal Name of the computer. You can select this value by clicking on the ellipse button next to the text box.
Event source	The source of the event. This will usually be an explicit value but may be a $Data variable to use the value of a property from the script.

Option	Description
Event log	The name of the event log. This will usually may be an explicit value or a $Data variable to use the value of a property from the script.
Event ID	The numeric event number. This will usually be an explicit value or a $Data variable to use the value of a property from the script.
Category	The value of the EventCategory parameter (an integer from 0 to 65535) is an index into a category dynamic-link library (DLL) message table that contains a localized string. Each publisher defines its own set of categories. These categories commonly correspond to individual components (for example: a connector, module host, or data warehouse).
Level	The severity of the event. You can select this value from the drop down list.

Creating Script Collection Rules

The following procedure creates a performance script collection rule with the following details:

- Runs on any computer with an instance of a particular service installed.
- The script accepts two parameters, one for computer name and another for the version of the application that is stored as a property on the target class.
- The script itself is only for testing and performs no real function. It simulates a script running a synthetic transaction and returning a property bag with static values.

To create a script based performance collection rule

1. If you don't have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. Create a new target using the process in To create a Windows Service template. You can use any service installed on a test agent for this template.
3. In the Operations console, select the **Authoring** workspace, and then select **Rules**.
4. Right-click **Rules** and select **Create a new rule**.
5. On the **Rule Type** page, do the following:
    a. Expand **Collection Rules**, then expand **Probe Based**, and then select **Script (Performance)**.
    b. In the **Management Pack** dropdown, select the management pack from step 1.

c. Click **Next**

6. On the **General** page, do the following:
   a. In the **Rule name** box, type **My Application Collect Script Performance**.
   b. In the **Rule Category** drop down box, select **Performance Collection**.
   c. Click **Select**.
   d. Select the name of the target you created in step 2.
   e. Click **OK**.
7. On the **Schedule** page, do the following:
   a. In the **Run every** box, type **15 minutes**.
   b. Click **Next**
8. On the **Script** page, do the following:
   a. For the **File Name** value, type **MyPerfCollectionScript.vbs**
   b. For the **Timeout** value, type **1 minutes**
   c. In the **Script** box, paste the complete contents of the following script.

```
sComputerName = WScript.Arguments(0)
sVersion = WScript.Arguments(1)

[oAPI.LogScriptEvent]
Set oAPI = CreateObject("MOM.ScriptAPI")
Set oBag = oAPI.CreatePropertyBag()
Call oBag.AddValue("ComputerName",sComputerName)
Call oBag.AddValue("InstanceName","MyInstance")
Call oBag.AddValue("Value",10)

oAPI.Return(oBag)
```

   d. Click the **Parameters** button.
   e. Select **Target**, select **(Host=Windows Computer)**, and then select **Principal Name (Windows Computer)**.
   f. Type a SPACE.
   g. Select **Target** and then **Version (My Computer Role Base)**.
   h. Click **OK**.
   i. Click **Next**.
9. On the **Performance Mapper** page, do the following:
   a. In the **Object** box type **MyApplication**.

b. In the **Counter** box type **MyCounter**.
c. In the **Instance** box type **$Data/Property[@Name=FileName]$**.
d. In the **Value** box type **$Data/Property[@Name='FileSize']$**.
e. Click **Create**.

The following procedure creates an event script collection rule with the following details:

- Runs on any computer with an instance of a particular service installed.
- The script accepts two parameters, one for computer name and another for the version of the application that is stored as a property on the target class.
- The script itself is only for testing and performs no real function. It simulates a script running a synthetic transaction and returning a property bag with static values.

To create a script based event collection rule

1. If you don't have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. Create a new target using the process in To create a Windows Service template. You can use any service installed on a test agent for this template.
3. In the Operations console, select the **Authoring** workspace, and then select **Rules**.
4. Right-click **Rules** and select **Create a new rule**.
5. On the **Rule Type** page, do the following:
   a. Expand **Collection Rules**, then expand **Probe Based**, and then select **Script (Event)**.
   b. In the **Management Pack** dropdown, select the management pack from step 1.
   c. Click **Next**
6. On the **General** page, do the following:
   a. In the **Rule name** box, type **My Application Collect Script Event**.
   b. In the **Rule Category** drop down box, select **Event Collection**.
   c. Click **Select**.
   d. Select the name of the target you created in step 2.
   e. Click **OK**.
7. On the **Schedule** page, do the following:
   a. In the **Run every** box, type **15 minutes**.
   b. Click **Next**
8. On the **Script** page, do the following:
   a. For the **File Name** value, type **MyEventCollectionScript.vbs**
   b. For the **Timeout** value, type **1 minutes**
   c. In the **Script** box, paste the complete contents of the following script.

```
sComputerName = WScript.Arguments(0)
sVersion = WScript.Arguments(1)

Set oAPI = CreateObject("MOM.ScriptAPI")
Set oBag = oAPI.CreatePropertyBag()
Call oBag.AddValue("ComputerName",sComputerName)
Call oBag.AddValue("EventID",100)
Call oBag.AddValue("ParamValue","Param1")

oAPI.Return(oBag)
```

   d. Click **Parameters**.
   e. Select **Target**, select **(Host=Windows Computer)**, and then select **Principal Name (Windows Computer)**.
   f. Type a SPACE.
   g. Select **Target** and then **Version (My Computer Role Base)**.
   h. Click **OK**.
   i. Click **Next**.
9. On the **Event Mapper** page, do the following:
   a. In the **Computer** box type **$Data/Property[@Name='ComputerName']$**.
   b. In the **Event source** box type **MyApp**.
   c. In the **Event log** box type **CustomScript**.
   d. In the **Event ID** box type **$Data/Property[@Name='EventID']$**.
   e. In the **Category** box type **0**.
   f. In the **Level** box select **Information**.
   g. Click the **Parameters** button.
   h. Type **$Data/Property[@Name='ParamValue']$**
   i. Click **OK**.
   j. Click **Create**.

See Also

Script Monitors and Rules

Script Monitors

Script monitors run a script on a schedule and use its output to determine the health state of the target object. Script monitors are useful for performing test transactions against applications or gathering information that is not accessible through other means. The results of the script are returned in a Property Bag that are evaluated against criteria to determine the resulting health state.

[Conceptual view of script monitor]

Options

When you run a script monitor wizard, you will need to provide values for options in the following tables. Each table represents a single page in the wizard.

General

Option	Description
Name	The name used for the monitor. This appears in the Health Explorer for each target object.
Description	Optional description of the monitor.
Management Pack	Management pack to store the classes, monitors, and rules created by the template. For more information on management packs, see Selecting a Management Pack File.
Monitor target	The class to use for the target of the monitor. The monitor will be run on any agent that has at least one instance of this class, and the health of those objects will be affected by the health of this monitor. For more information on targets, see Understanding Classes and Objects.
Parent Monitor	The aggregate monitor that this monitor will be placed under in the Health Explorer.
Monitor is enabled	If checked, the monitor is enabled and the script will run according to the schedule. If unchecked, the monitor is not enabled and the script will not run. The monitor can be enabled for a group of target objects by creating an override to enable the monitor.

Schedule

The **Schedule** page defines the schedule to run the script. The script will run indefinitely according to this schedule until the monitor is disabled or deleted or the management pack is uninstalled.

Option	Description
Run every	Frequency that the script should be run. This should typically not be less than 5 minutes.
Synchronize at	If enabled, the schedule will be synchronized to occur at the specified time.

Script

The **Script** page contains the body of the script itself and its parameters. You can type the script directly into the dialog box, but you will usually write it using another text editor and then copy the text of the script and paste it. This allows you to use a more functional editing tool and test the script on a command line before including it in the management pack.

Option	Description
File Name	Name of the script. Must have either a .vbs or .js extension depending on its language. There is no requirement to make this name unique because each script is provided its own temporary directory on the agent.
Timeout	The number of seconds that the script can run before the agent stops it. This prevents problem scripts from running continuously and putting excess overhead on the agent computer. The timeout value assigned to a script should allow enough time for the script to run under ordinary conditions, but should be less than the interval that the script is scheduled to run. If a script is configured to have a timeout value greater than its duration, then possibly multiple copies of the script could be running concurrently.
Script	The body of the script.

Option	Description
Parameters	Click to provide values for any arguments in the script. For more information, see Script Arguments.

Expressions

Each required expression for the monitor will have its own page in the wizard. A two state monitor will have the following expressions:

- Unhealthy Expression
- Healthy Expression

A three state monitor will have the following expressions:

- Unhealthy Expression
- Degraded Expression
- Healthy Expression

Note
Detailed information on expressions is available in Expressions.

Each expression will typically compare the value of one or more of the properties from the script's property bag to some value. Each expression must be different, and only one of the expressions should evaluate to True under any particular condition. In the next page of the wizard, you will associate each of the health states of the monitor with one of these expressions. When an expression evaluates to the True, the monitor will be set to that health state.

For example, the script might perform a test transaction against a particular application and return a single property with a value of "Good" if the transaction completed successfully, and "Bad" if the transaction failed.

Option	Description
Parameter Name	This will be a $Data variable representing the particular value that you need from the property bag. This will be in the following syntax: Property[@Name="PropertyName"]
Operator	The type of comparison to perform.
Value	The explicit value that should match the value in the property bag.

Configure Health

On this page, you map each of the expressions to a health state for the monitor. When a condition is true, the monitor is set to the health state that you define. For a three state monitor, you can typically accept the default settings. For a two state monitor, you typically only have to determine if the Unhealthy Expression should result in a Critical or Warning state.

Option	Description
Monitor Condition	Represents each of the expressions.
Health State	The health state to set the monitor to when that expression is true.

Configure Alerts

Option	Description
Generate alerts for this monitor	If checked, an alert will be created when the monitor changes from a healthy state to a warning or critical state, and all of the other options will be enabled. If unchecked, the monitor will not generate alerts when the health state is changed, and all of the other options will be disabled.
Generate an alert when	For a two-state monitor, this setting should be set to **The monitor is in a critical health state**.
Automatically resolve alert when the monitor returns to a healthy state	If checked, the alert will automatically be resolved when the monitor returns to a healthy state. If unchecked, the alert must be resolved manually.
Alert name	The name of the alert that is displayed in the console.
Alert Description	The description of the alert.
Priority	The priority of the alert: Low, Medium, or High.
Severity	The severity of the alert: Information, Warning, Critical, or matched to the health state of the monitor.

Creating a Script Monitor

The following procedure shows how to create a monitor based on a monitoring script with the following details:

The monitor created in this procedure has the following characteristics:

- Runs on any computer with an instance of a particular service installed.
- Sets the monitor to a **critical** state when the script returns a status message of Bad.
- Sets the monitor to a **healthy** state when the script returns a status message of Good.
- The script accepts an argument for the computer name of the target object's agent and for an argument specifying wherther thereturns a Good or Bad message.
- The script itself is only for testing and performs no real function. It simulates a script running a synthetic transaction.

To create a two state script monitor

1. If you don't have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. Create a new target using the process in To create a Windows Service template. You can use any service installed on a test agent for this template.
3. In the Operations console, select the **Authoring** workspace, and then select **Monitors**.
4. In the **Monitors** pane, click **Change Scope** and then select the name of the target that you created in step 2.
5. Expand the target class then expand **Entity Health**.
6. Right-click **Availability**, select **Create a Monitor**, and then select **Unit Monitor**.
7. On the **Monitor Type** page, do the following:
    a. Expand **Scripting** and then expand **Generic**.
    b. Select **Timed Script Two State Monitor**.
    c. In the **Management Pack** dropdown, select the management pack from step 1.
    d. Click **Next**.
8. On the **General** page, do the following:
    a. In the **Name** box, type **My Application Script Monitor**.
    b. The **Monitor target** box should already have the correct target class.
    c. **Parent Monitor** box should already have **Availability**.
    d. Leave the **Monitor is enabled** box selected.
    e. Click **Next**.
9. On the **Schedule** page, do the following:
    a. In the **Run every** box, type **15 minutes**.
    b. Click **Next**
10. On the **Script** page, do the following:
    a. For the **File Name** value, type **MyScript.vbs**

b. For the **Timeout** value, type **1 minutes**
c. In the **Script** box, paste the complete contents of the following script.

```
sComputerName = WScript.Arguments(0)
bTestSuccessful = WScript.Arguments(1)

Set oAPI = CreateObject("MOM.ScriptAPI")
oAPI.LogScriptEvent "MyScript.vbs",10,4, "Running script on "
& sComputerName
Set oBag = oAPI.CreatePropertyBag()
Call oBag.AddValue("ComputerName",sComputerName)
If bTestSuccessful = True Then
   Call oBag.AddValue("Result","Good")
Else
   Call oBag.AddValue("Result","Bad")
End If
oAPI.Return(oBag)
```

d. Click the **Parameters** button.
e. Select **Target**, then select **(Host=Windows Computer)**, then select **Principal Name (Windows Computer)**.
f. Type a space after the Principal Name variable and then type **False**.
g. Click **OK**.
h. Click **Next**.

11. On the **Unhealthy Expression** page, do the following:
    a. Click **Insert**.
    b. In the **Parameter Name** box type **Property[@Name='Result']**.
    c. In the **Operator** box select **Equals**.
    d. In the **Value** box type **Bad**.
    e. Click **Next**.
12. On the **Healthy Expression** page, do the following:
    a. Click **Insert**.
    b. In the **Parameter Name** box type **Property[@Name='Result']**.
    c. In the **Operator** box select **Equals**.
    d. In the **Value** box type **Good**.
    e. Click **Next**.

13. On the **Configure Health** page, do the following:
    a. Change the **Health State** for the Unhealthy condition to **Critical**.
    b. Click **Next**.
14. On the **Configure Alerts** page, do the following:
    a. Select **Generate alerts for this monitor**
    b. In the **Generate an alert when** box, select **The monitor is in a critical health state**.
    c. Leave the box selected to automatically resolve the alert.
    d. In the **Alert name** box, type **Application test failed.**
    e. Clear the existing text in the **Alert description** box and type **Result:**
    f. Click the ellipse button.
    g. Click **Data** and then **Property**.
    h. Replace **<<STRING>>** with **Result**.
    i. Click **OK**.
15. Click **Create**.

See Also

Script Monitors and Rules

UNIX/Linux Shell Command Monitors

UNIX/Linux shell command monitors run on a schedule and execute a program or script, a command, or a one-line command sequence (using pipeline operators). The output from the command is used to determine the health state of the target object. Shell command monitors are useful for custom monitoring of UNIX and Linux applications with information that is not accessible through other means.

Options

When you run an UNIX/Linux shell command monitor wizard, you will need to provide values for options in the following tables. Each table represents a single page in the wizard.

Rule Type

The **Rule Type** page includes basic settings for the rule including its type and the management pack file to store it in.

Option	Description
Select the type of monitor to create	To create a shell command monitor that evaluates for two states (healthy and error),

Option	Description
	select **UNIX/Linux Shell Command Two State Monitor**. To create a shell command monitor that evaluates for three states (healthy, warning and error), select **UNIX/Linux Shell Command Three State Monitor**.
Management Pack	Management pack file to store the rule or monitor.For more information on management packs, see Selecting a Management Pack File.

General

The **General** page includes general settings for the rule including its name, category, target, and the management pack file to store it in.

Option	Description
Name	The name used for the monitor. This appears in the **Monitors** view in the **Authoring** pane. When you view the Health Explorer for the monitoring target, you can see the health state of this monitor.
Description	Optional description of the rule.
Monitor Target	The class to use for the target of the rule. The rule will be run on any agent that has at least one instance of this class. For more information on targets, see Understanding Classes and Objects.
Parent Monitor	The aggregate monitor that this monitor will be placed under in the Health Explorer.
Monitor is enabled	If checked, the monitor is enabled and the shell command will run according to the schedule. If unchecked, the monitor is not enabled and the script will not run. The monitor can be enabled for a group of target objects by creating an override to enable the monitor.

Schedule

The **Schedule** page defines the schedule to run the script. The script will run indefinitely according to this schedule until the monitor is disabled or deleted or the management pack is uninstalled.

Option	Description
Run every	Frequency that the script should be run. This should typically not be less than 5 minutes.
Synchronize at	If enabled, the schedule will be synchronized to occur at the specified time.

UNIX/Linux Shell Command

The following options are available on the **Shell Command Details** page of the wizard.

Option	Description
Command	The shell command to execute. This can be the full path to a program or script, a command, or a one-line sequence of multiple commands (using pipeline operators).
Run As Profile	Either the “UNIX/Linux Action Account” or “UNIX/Linux Privileged Account” profile. Select the profile that associates the required account credentials with the task target. The associated account will be used to execute the command.
Timeout (seconds)	The number of seconds that the command can run before the agent stops it. This prevents problem commands from running continuously and putting excess overhead on the agent computer.

Expressions

Each required expression for the monitor will have its own page in the wizard. A two-state monitor will have the following expressions:

1. Error Expression
2. Healthy Expression

A three-state monitor will have the following expressions:

1. Error Expression
2. Warning Expression
3. Healthy Expression

Note
Detailed information on expressions is available in Expressions.

Each expression will typically compare the value of one or more of the properties from the command's output to some value. Each expression must be different, and only one of the expressions should evaluate to True under any particular condition. In the next page of the wizard, you will associate each of the health states of the monitor with one of these expressions. When an expression evaluates to the True, the monitor will be set to that health state.

Option	Description
Parameter Name	The Parameter Name syntax for command execution output is:**StdOut**: //*[local-name()="StdOut"]**StdErr**: //*[local-name()="StdErr"]**Return Code**: //*[local-name()="ReturnCode"]
Operator	The type of comparison to perform.
Value	The explicit value that should match the value in the property bag.

Configure Health

On this page, you map each of the expressions to a health state for the monitor. When a condition is true, the monitor is set to the health state that you define. For a three-state monitor, you can typically accept the default settings. For a two-state monitor, you typically only have to determine if the Unhealthy Expression should result in a Critical or Warning state.

Option	Description
Monitor Condition	Represents each of the expressions.
Health State	The health state to set the monitor to when that expression is true.

Configure Alerts

Option	Description
Generate alerts for this monitor	If checked, an alert will be created when the monitor changes from a healthy state to a warning or critical state, and all of the other options will be enabled. If unchecked, the monitor will not generate alerts when the health state is changed, and all of the other options will be disabled.
Generate an alert when	For a two-state monitor, this setting should be set to **The monitor is in a critical health state**.
Automatically resolve alert when the monitor returns to a healthy state	If checked, the alert will automatically be resolved when the monitor returns to a healthy state. If unchecked, the alert must be resolved manually.
Alert name	The name of the alert that is displayed in the console.
Alert Description	The description of the alert.
Priority	The priority of the alert: Low, Medium, or High.
Severity	The severity of the alert: Information, Warning, Critical, or matched to the health state of the monitor.

Creating an UNIX/Linux Shell Command Monitor

The following procedure shows how to create a monitor based on a monitoring shell command with the following details:

- Runs on any UNIX/Linux computer every 15 minutes
- Sets the monitor to a **Critical** state when the file “/tmp/error” exists.
- Sets the monitor to a **Healthy** state when the file “/tmp/error" does not exist.

To create a two state UNIX/Linux shell command monitor

1. If you don’t have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. In the Operations console, select the **Authoring** workspace, and then select **Monitors**.
3. Launch the **Create a Monitor** task, and select **Unit Monitor**.
4. On the **Monitor Type** page, do the following:

a. Expand **Scripting** and then expand **Generic**.
b. Select **UNIX/Linux Shell Command Two State Monitor**.
c. In the **Management Pack** dropdown, select the management pack from step 1.
d. Click **Next**.

5. On the **General** page, do the following:
   a. In the **Name** box, type **Error File Test Monitor.**
   b. Click **Select** next to the **Monitor Target** box, select **UNIX/Linux Computer**, and click **OK**.
   c. Select the **Parent Monitor** of **Availability**.
   d. Leave the **Monitor is enabled** box selected.
   e. Click **Next**.
6. On the **Schedule** page, do the following:
   a. In the **Run every** box, type **15 minutes**.
   b. Click **Next**.
7. On the **Shell Command Details** page, do the following:
   a. In the **Command** box, type **ls /tmp/error | wc –l**. This command sequence will return a 1 if the file "/tmp/error" exists, and a 0 if it does not.
   b. In the **Run As Profile** box, select the **UNIX/Linux Action Account** profile.
   c. In the **Timeout (Seconds)** box, input **120**.
   d. Click **Next**.
8. On the **Error Expression** page, enter the following **And** expression:
   a. **//*[local-name()="StdOut"] equals 1**
   b. **//*[local-name()="ReturnCode"] equals 0**
9. On the **HealthyExpression** page, enter the following **And** expression:
   a. **//*[local-name()="StdOut"] does not equal 1**
   b. **//*[local-name()="ReturnCode"] equals 0**
10. On the **Configure Health** page, do the following:
    a. Leave the **Health State** for the **StatusError** condition set to **Critical**.
    b. Click **Next**.
11. On the **Configure Alerts** page, do the following:
    a. Select **Generate alerts for this monitor**.
    b. In the **Generate an alert when** box, select **The monitor is in a critical health state**.
    c. Leave the box selected to automatically resolve the alert.
    d. In the **Alert name** box, type **Application test failed**.
    e. Clear the existing text in the **Alert description** box and type **Computer:**
    f. Click the ellipse button.
    g. Click **Target** and then select **Network Name**.
    h. Click **OK**.

i. In the **Alert description** box, add a new line and type **StdOut: $Data/Context///*[local-name()=”StdOut”]$**

12. Click **Create**.

See Also

Script Monitors and Rules

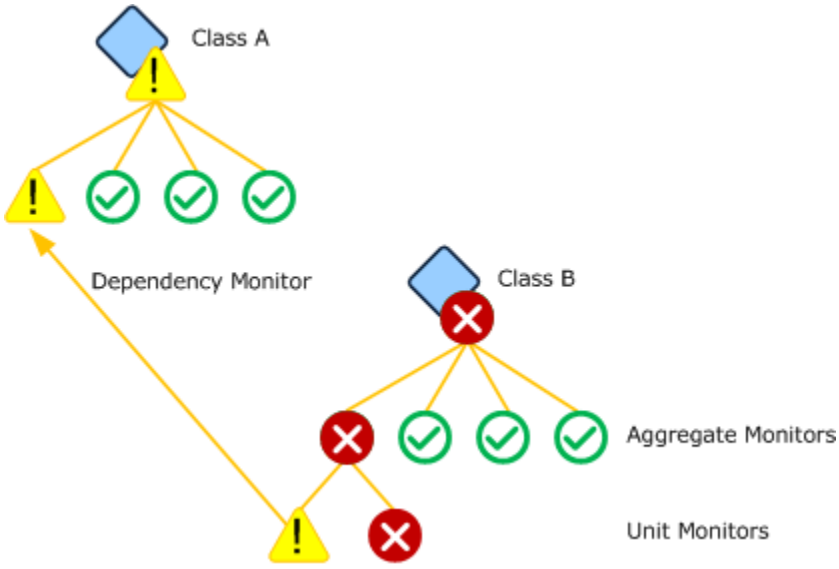
Dependency Monitors

Dependency monitors let the health of one object be affected by the health of another object. This allows for health rollup between specific related instances of different classes.

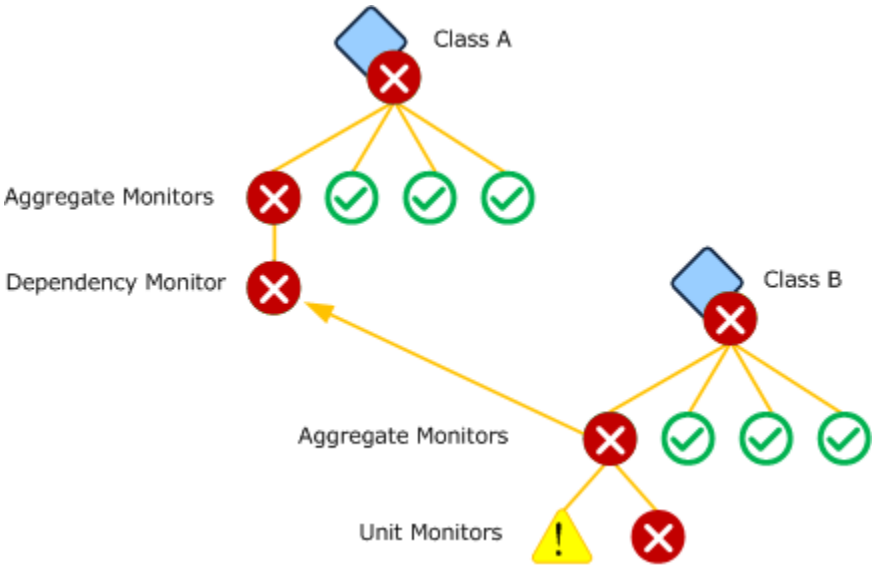
Each dependency monitor is based on a specific hosting or containment relationship. Just creating a relationship between two objects does not alone provide rollup between their health states. A dependency monitor must be associated with the relationship for rollup of health to be performed.

The source and target class for a dependency monitor are defined by the relationship that the monitor is based on. The monitor must additionally specify a specific unit monitor or aggregate monitor on the target class and an aggregate monitor on the source class. Only the health of the target monitor is considered when calculating the health of the dependency monitor, and it only affects the health of the specified aggregate monitor on the target object.

Dependency monitor based on unit monitor

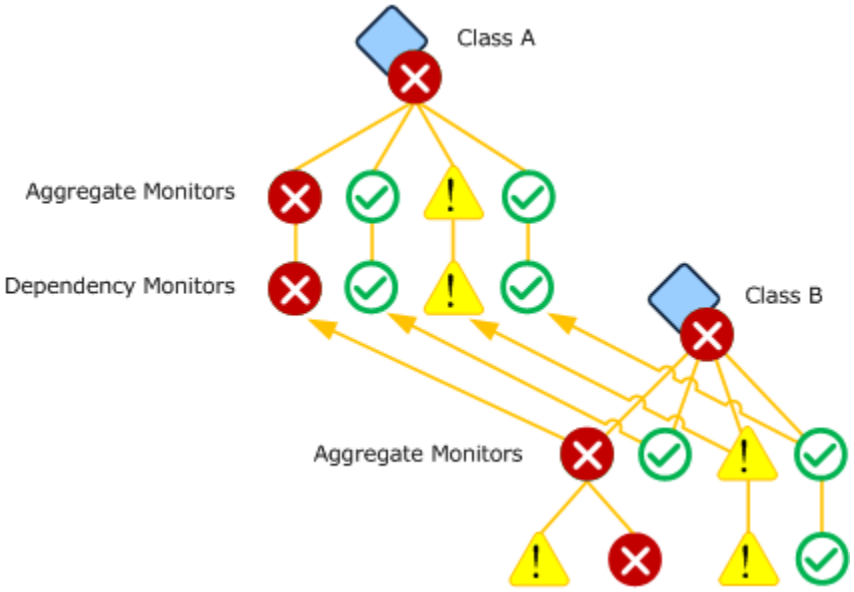


Dependency monitor based on aggregate monitor



Multiple dependency monitors can be created on a single relationship if the health of the source class should be affected by multiple unit or aggregate monitors on the target class. For example, a dependency monitor might be created for each standard aggregate monitor as shown in the following image.

Multiple dependency monitors for a single class



Health Rollup Policy

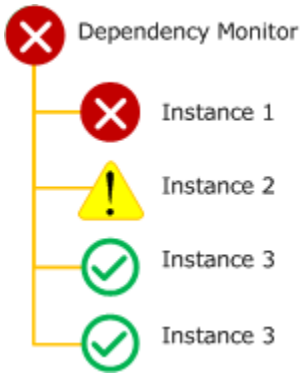
There may be multiple instances of the target class, each with a different health state. Each dependency monitor must define a health rollup policy to define the logic that is used to

determine the health of the dependency monitor based on the health of the instances of its target monitor. The possible health rollup policies for a dependency monitor are as follows:

Worst state policy

The source object matches the state of the target object that has the worst health state. This is used when the source object should only be healthy if all the target objects are healthy. This is the most common policy used by dependency monitors.

Worst state health policy

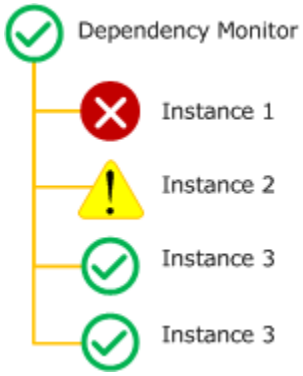


Best state policy

The source object matches the state of the target object that has the best health state. This policy is used when only one of the source objects has to be healthy for the target object to be healthy.

For example, the **Microsoft Windows Hyper-V 2008 Monitoring** management pack has a dependency monitor on the hosting relationship from **Microsoft.Windows.HyperV.ServerRole** to **Microsoft.Windows.HyperV.VirtualNetwork** that uses a best state policy. This is because the server running Hyper-V is functional as long as it has one functional virtual network. The logic defined by this management pack is that the server class should show an error state if no virtual networks are available.

Best state health policy

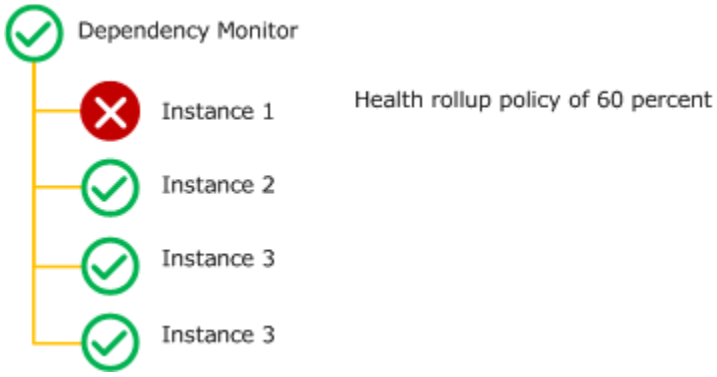


Percentage policy

The source object matches the worst state of a single member of a specified percentage of target objects in the best state. This policy is used when a certain percentage of target objects must be healthy for the target object to be considered healthy.

For example an application might run on a web farm that includes multiple Web servers. Because of the redundancy offered in this kind of deployment, the application might be considered healthy if a particular percentage of servers is available. The farm itself could be represented in the management pack by a health rollup class based on System.ApplicationComponent with a containment relationship to the Web servers. A dependency monitor could be created on this containment relationship with a health rollup policy specifying a percentage. Even if one or more Web servers had a problem, as long as the specified percentage were in a healthy state then the class representing the web farm would also be healthy.

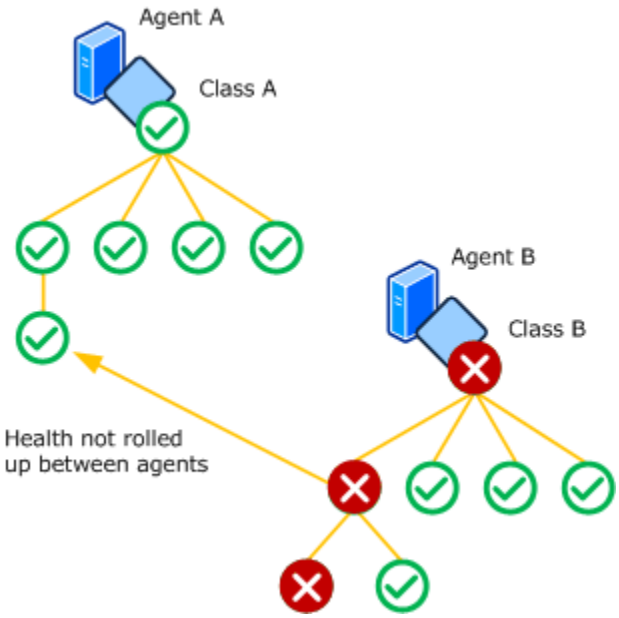
Percentage health policy



Health rollup between agents

Health state can only be rolled up between objects managed by the same agent unless the source object is managed by the Root Management Server. Groups and classes used for health rollup are typically unhosted. This means that they are managed by the RMS so that they can roll up health from objects managed by different agents. A relationship can be discovered between objects managed by different agents, but any dependency monitor associated with that relationship will not work as expected.

Health rollup between agents



Aggregate Monitors

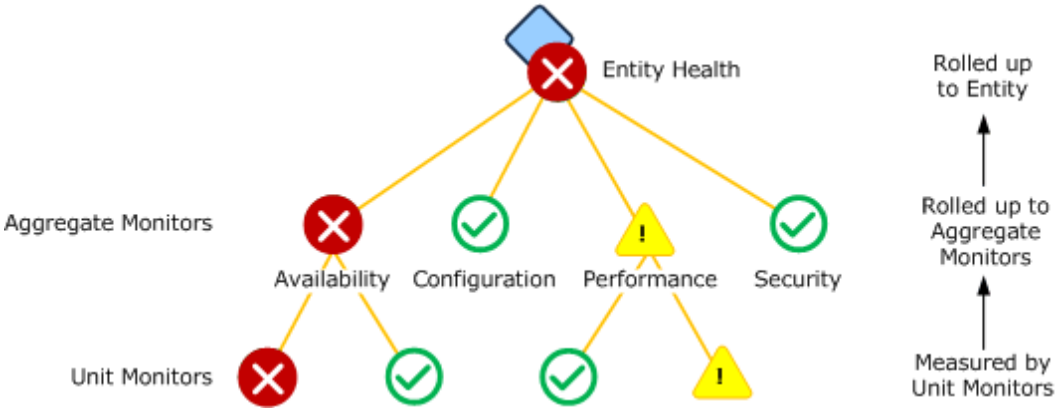
Aggregate monitors group multiple monitors to provide a single health aggregated health state. This provides an organization to all of the monitors targeted at a particular class and provides a consolidated health state for specific categories of operation.

Standard Aggregate Monitors

Every class has four standard aggregate monitors: Availability, Configuration, Performance, and Security. These are in the System.Health.Library management pack and targeted at the **Entity** class. Because all classes inherit from the **Entity** class, all classes inherit these standard monitors. The standard set of aggregate monitors will be sufficient for most classes.

Most monitors will fall into one of the four categories represented by the standard aggregate monitors. Because of this, custom aggregate monitors will typically use one of the standard aggregate monitors as their parent instead of being positioned alongside them directly under the entity health. Unit monitors and dependency monitors will similarly use either a custom aggregate monitor or one of the standard aggregate monitors as their parent.

Standard aggregate monitors



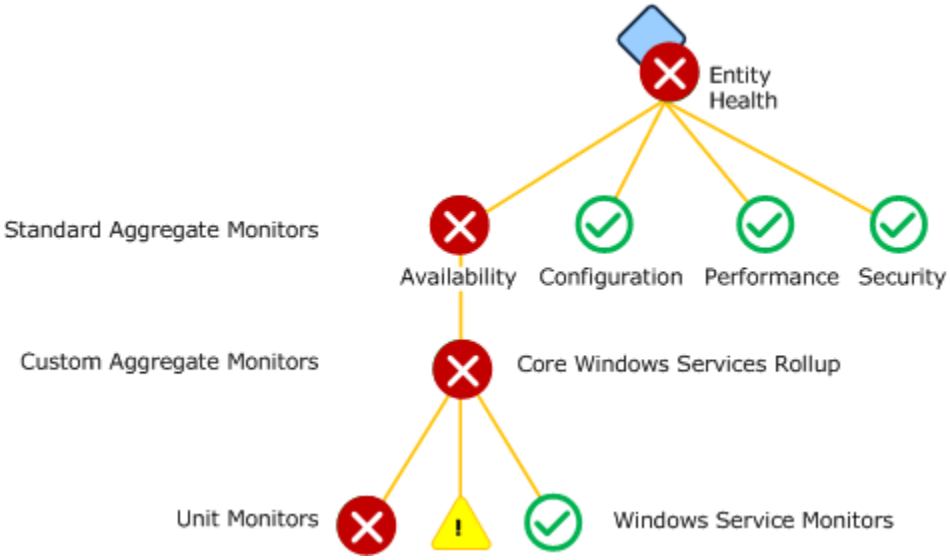
Custom Aggregate Monitors

Management packs can include custom aggregate monitors specific to the requirements of classes in a particular application. These monitors may use another aggregate monitor for their parent or the top level Entity State similar to the standard aggregate monitors use. Custom aggregate monitors can be configured underneath another aggregate monitor or attached directly to the entity state.

For example, the Windows Server 2008 Operating System (Monitoring) management pack includes an aggregate monitor called Microsoft.Windows.Server.2008.OperatingSystem.CoreServicesRollup that is used to combine the health of the different services that are monitored by this management pack. There are nine services that the management pack considers critical to the operation of a computer running Windows Server 2008. Instead of positioning these directly under the Availability aggregate monitor alongside other unit monitors, the aggregate monitor provides a combined health measurement for all the related services.

This aggregate monitor is illustrated in the following diagram.

Core Windows Services Rollup aggregate monitor



Health Rollup Policy

Each aggregate monitor must define a health rollup policy which is the logic that is used to determine the health of the aggregate monitor based on the health of the monitors under it. The possible health rollup policies for an aggregate monitor are as follows:

Worst state

The state of the aggregate monitor matches the state of the child monitor with the worst health state. This is the most common policy used by aggregate monitors.

Worst state health policy

Best state

The state of the aggregate monitor matches the state of the child monitor with the best health state.

Best state health policy

Alerting on Aggregate Monitors

You can configure alerts on aggregate monitors just like with unit monitors, and you can leverage this feature to reduce noise by limiting the number of redundant alerts you receive. To implement this strategy, group together a common set of unit monitors underneath an aggregate monitor. Configure the aggregate monitor to send an alert, but configure unit monitors to not send an alert. When one of the unit monitors goes to a critical or warning state (depending on the configuration of your aggregate monitor), it will cause the aggregate monitor to change to the same state and cause an alert to be sent. If another unit monitor under the same aggregate goes to a warning or critical state, another alert won't be sent since the aggregate monitor will already be in the negative state.

This strategy should only be used if the unit monitors measure a particular feature of the application. The assumption it relies on is that a problem with one of the monitors will alert support staff to a problem in the application. They can inspect the Health Explorer for further information including the other monitors that may be unhealthy. Additional alerts for a similar problem would not be of value but only create excess noise.

If the unit monitors measure different features of the application such that alerts should be received separately from each, then either multiple aggregate monitors should be created or this strategy should not be used.

Diagnostics and Recoveries

Diagnostics and *recoveries* run when a monitor changes state. Diagnostics collect additional information about the detected problem. Recoveries try to resolve the problem. Each will typically run a command or script that outputs information displayed in the Health Explorer in the Operations Console.

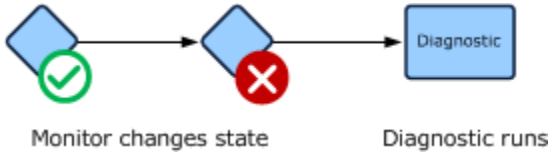
Diagnostics

Diagnostics run after a monitor changes state and try to collect additional information about the issue. This information is provided to the user with the state change history in the properties of the monitor. If the **Run diagnostic automatically** property of the diagnostic is set to true, then it is run automatically when the monitor changes state. If the **Run diagnostic automatically**

property of the diagnostic is set to false, then a link is provided to the user in the Operations console that they can click to run the diagnostic.

Diagnostics are not intended to make any changes to the application or system that they are running on. Because they are running a script or command, however, there is no way for Operations Manager to make sure that these changes are not being made. It is the responsibility of the management pack author to make sure that no such changes are being made. If changes to the application or system are required, then a recovery should be used.

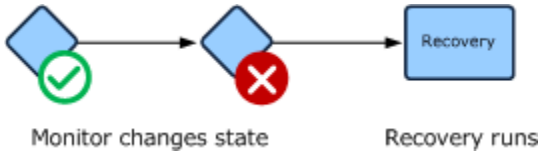
Diagnostic



Recoveries

Recoveries are workflows that run after a monitor changes state. Recoveries try to correct the issue, and return the monitor to a healthy state. Any output from the recovery is provided to the user with the state change history in the properties of the monitor that the diagnostic is associated with. If the **Run diagnostic automatically** property of the recovery is set to true, then the recovery is run automatically when the monitor changes state. If the **Run diagnostic automatically** property of the recovery is set to false, then a link is provided to the user in the Operations console that they can click to run the recovery.

Recovery



Recalculating State

If a recovery is successful, then the monitor should return to a healthy state the next time that the monitor detects the required information. If the monitor runs a scheduled script for example, then the monitor will return to healthy the next time that the script runs and the monitors detects the criteria for a healthy state. If the monitor relies on an event for its healthy state, the application is expected to create the required event in response to the recovery successfully correcting the problem. If a monitor is configured to use a manual reset though, then the user will still be required to manually set it to a healthy state.

A recovery can be configured to recalculate the state of the monitor immediately after it runs. This option has the same effect as the user selecting **Recalculate Health** for the monitor in the

Operations console. Recalculating state only has an effect on monitors that run on a schedule such as a script and that have on demand detection defined. If the monitor does not have on demand detection defined, then the option has no effect. The advantage of configuring a monitor to recalculate state is that it can return the monitor to a healthy state immediately instead of waiting for the schedule.

Diagnostic and Recovery Wizard Options

When you run the Diagnostic or Recovery wizard, you will need to provide values for options in the following tables. Each table represents a single page in the wizard.

Diagnostic or Recovery Task Type

The **Diagnostic Task Type** or **Recovery Task Type** page allows you to specify the type of diagnostic or recovery to create and the management pack file to store it in.

Option	Description
Select the type of diagnostic task to create Select the type of recovery task to create	Specifies if the diagnostic or recovery will run a command or a script.
Management Pack	Management pack file to store the diagnostic or recovery. If the monitor is in an unsealed management pack file, then the diagnostic or recovery must be stored in the same one. For more information on management packs, see Selecting a Management Pack File.

General

The **General** page includes general settings for the diagnostic or wizard including its name, category, target, and the management pack file to store it in.

Option	Description
Diagnostic Name Recovery Name	The name used for the diagnostic or recovery. For a rule, the name appears in the **Rules** view in the **Authoring** pane. When you create a view or report, you can select this name to use the data collected by it. For a monitor, the name appears in the Health Explorer of any target objects.
Description	Optional description of the diagnostic or

Option	Description
	recovery.
Management Pack	Management pack to store the rule. For more information on management packs, see Selecting a Management Pack File.
Select the health state for which this diagnostic will run Select the health state for which this recovery will run	Specifies the health state that the diagnostic or recovery will run in response to. When the monitor changes to the specified state from another state, the diagnostic or recovery will run.
Run diagnostic automatically Run recovery automatically	If selected, the diagnostic or recovery will automatically run when the monitor changes to the specified state. If not selected, the diagnostic or recovery will be displayed as a link in the Health Explorer that the user can click to run.
Recalculate monitor state after recovery finishes (Recoveries only)	Specifies whether the recovery should initiate a recalculation of the monitor health state after completing. This is described in Recalculating State.

Command Line

The **Command Line** page is only available for **Run Command** diagnostics and recoveries. It includes details about the command to run.

Option	Description
Full path to file	The path and name of the executable to run.
Parameters	Any command line parameters that you would include after the executable if you were running it from a command line. You can include variables that refer to values from properties of the target object of the monitor.
Working directory	The default directory to set while the command runs if the executable requires one.
Timeout (in seconds)	The number of seconds that the command can run before the agent stops it. This prevents problem scripts from running continuously and

Option	Description
	putting excess overhead on the agent computer. The timeout value assigned to a script should allow enough time for the script to run under ordinary conditions, but should be less than the interval that the script is scheduled to run. If a script is configured to have a timeout value greater than its duration, then possibly multiple copies of the script could be running concurrently.

Script

The **Script** page is only available for **Run Script** diagnostics and recoveries. It contains the body of the script itself and its parameters. You can type the script directly into the dialog box, but you will usually write it using another text editor and then copy the text of the script and paste it. This allows you to use a more functional editing tool and test the script on a command line before including it in the management pack.

Option	Description
File Name	Name of the script. Must have either a .vbs or .js extension depending on its language. There is no requirement to make this name unique because each script is provided its own temporary directory on the agent.
Timeout	The number of seconds that the script can run before the agent stops it. This prevents problem scripts from running continuously and putting excess overhead on the agent computer. The timeout value assigned to a script should allow enough time for the script to run under ordinary conditions, but should be less than the interval that the script is scheduled to run. If a script is configured to have a timeout value greater than its duration, then possibly multiple copies of the script could be running concurrently.
Script	The body of the script.

Option	Description
Parameters	Click to provide values for any arguments in the script. For more information, see Script Arguments.

Creating Diagnostics and Recoveries

Use the following procedure to create a diagnostic in Operations Manager with the following details:

- Collects a list of the processes running on the agent computer.

To create a diagnostic that runs a command

1. Create a monitor using a procedure from one of the topics in Monitors and Rules.

   In the Operations console, select the **Authoring** workspace, and then select **Monitors**.
2. In the **Monitors** pane, expand the monitor you created in the first step.
3. Right-click the monitor and select **Properties**.
4. Select the **Diagnostic and Recovery** tab.
5. Click **Add** and then **Diagnostic for a warning health state** or **Diagnostic for a critical health state**. The options available in this step will depend on the health states of the monitor.
6. On the **Diagnostic Task** Type page, do the following:
   a. In the **Select the type of diagnostic task to create** box, select **Run Command**.
   b. Click **Next**.
7. On the **General** tab, do the following:
   a. In the **Diagnostic Name** box, type **Check Running Processes**.
   b. In the **Select the health state for which this diagnostic will run** dropdown, select either **Warning** or **Critical**. The diagnostic will run when the monitor changes from a healthy state to the specified state.
   c. Ensure that **Run diagnostic automatically** is selected.
   d. Click **Next**.
8. On the **Command Line** tab, do the following:
   a. In the **Full path to file** box, type **%windir%\system32\tasklist.exe**.
   b. Click **Create**.
   c. Click **OK**.

Tasks

Tasks in System Center 2012 – Operations Manager are actions that can be run on demand by the user. Depending on the kind of task, the action may run either on the user's local workstation or on one or more specified agents.

In This Section

Console Tasks

Tasks that run on the user's workstation using the current user's credentials.

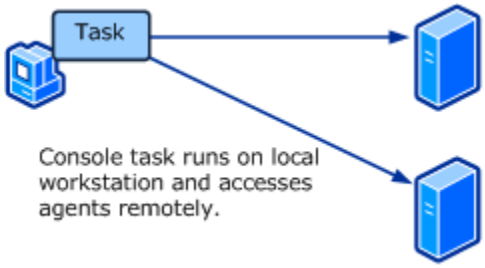
Agent Tasks

Tasks that run on the agent computer using the credentials of the specified user profile.

Console Tasks

Console tasks in System Center 2012 – Operations Manager run on the workstation where the Operations Console is running and uses the same credentials as the logged on user. The application that is run by the task must be installed on the workstation.

Console task



Console tasks are useful for running administration consoles or other tools that remotely access application components. These will usually be executable programs that run outside the Operations console. You can also run a command line utility and have the output displayed in a **Console Task Output** window.

For example, an administration console might require the name of the server that is running the application. The target for the task could be a class based on **Windows Computer Role** representing the application installation on the server. The task would only be available when an instance of the target class is selected. Because the class is hosted by **Windows Computer**, the PrincipalName property could be provided on the command line.

Create Console Task Wizard Options

When you run the **Create Console Task** wizard, you have to provide values for the options in the following tables. Each table represents a single page in the wizard.

General Properties

The following options are available on the **General Options** page of the wizard.

Option	Description
Task Name	The name used for the task. This name is displayed in the **Actions** pane in the Operations console.
Description	Optional description of the task.
Task target	Target class of the task. The task will be displayed in the **Actions** pane when an instance of the target class is selected. Properties from the target object are available to use in the parameter of the task You do not specify a target for Alert and Event command line tasks. They are available to all alerts and events regardless of the class that created them.

Command Line

The following options are available on the **Command Line** page of the wizard.

Option	Description
Application	Path and name of the application to run.
Parameters	Parameters to add to the command line. This can be a combination of static text and variables for the properties of the target class or one of its parent classes. If a variable used for a parameter could resolve to text containing a space, you should enclose the variable in quotations (""). If there are no quotations and the text includes a space, then it will be seen as multiple parameters.

Option	Description
Working directory	The default directory to use when the application is run.
Display output when this task is run	If selected, a **Console Task Output** window is opened when the task is run to display command line output. Make sure this option is selected if the application for the task is a utility that you would normally run from a command prompt.

Command Line Tasks

Command line tasks run a command line application or batch file using a target class. They are listed in the **Actions** pane of the Operations console when an instance of the target class is selected. You can specify the path to the application and the working directory. You can also use $Target variables from the target class or one of its parents to be included on the command line.

The following procedure creates a console task to run the **nslookup** utility to resolve the name of a computer to an IP address on the local computer. In this example, you will pass the principle name of the target computer to the command line.

To create a command line task

1. Select the **Authoring** workspace.
2. In the Authoring pane, expand **Management Pack Objects**.
3. Right click **Tasks** and select **Create a New Task** to open the **Create Task Wizard**.
4. On the **Task Type** page, do the following:
   a. Under **Console Tasks**, select **Command line**.
   b. In the **Select destination management pack** dropdown, select the management pack file to store the task. For more information about management packs, see Selecting a Management Pack File.
   c. Click **Next**.
5. On the **General Properties** page, do the following:
   a. Under **Task Name**, type **NSLookup**. This is the text that will be displayed in the **Actions** pane.
   b. Click the Select button to open the **Select Items to Target** dialog box.
   c. Select **Windows Computer** and click **OK**.
   d. Click **Next**.
6. On the **Command Line** page, do the following:
   e. .a. In the **Application** box, type **%windir%\system32\nslookup.exe**.

b. Click the button to the right of the **Parameters** box and select **Principal Name**.
c. Ensure that the **Display output when this task is run** checkbox is selected. This option causes the **Console Task Output** window to be opened when the task is run.
d. Click **Create**.

To test the command line task

1. Select the **Monitoring** workspace.
2. Select the **Windows Computers** view.
3. Select a computer listed in the **Windows Computers** pane.
4. In the **Windows Computer Tasks** section of the **Tasks** pane, click **NSLookup**.
5. When you have inspected the results of the lookup, click **Close**.

Alert Command Line Tasks

Alert command line tasks run a command line application or batch file based on an alert. They are listed in the **Actions** pane of the Operations console when an alert is selected. You can specify the path to the application and the working directory. You can also use properties from the selected alert on the command line.

The following procedure creates a command line task to run a custom application forwarding an alert to an external ticketing system. It runs a custom program that accepts the Ticket ID, Managed Object Name, and Owner as command line parameters. In this example, it is expected that the managed object name and owner would possibly include spaces, so they are enclosed in quotations.

To create an alert command line task

1. Select the **Authoring** workspace.
2. In the Authoring pane, expand **Management Pack Objects**.
3. Right click **Tasks** and select **Create a New Task** to open the **Create Task Wizard**.
4. On the **Task Type** page, do the following:
   a. Under **Console Tasks**, select **Alert command line**.
   b. In the **Select destination management pack** dropdown, select the management pack file to store the task. For more information about management packs, see Selecting a Management Pack File.
   c. Click **Next**.
5. On the **General Properties** page, do the following:
   a. Under **Task Name**, type **Forward Alert**. This is the text that will be displayed in the **Actions** pane.
   b. Click **Next**.
6. On the **Command Line** page, do the following:
   a. In the **Application** box, type **c:\ticketing\CreateTicket.exe**.

b. Click the button to the right of the **Parameters** box and select **Ticket ID**.
c. Type a space after **$Ticket ID$**.
d. Click the button to the right of the **Parameters** box and select **Managed Object Name**.
e. Type quotations ("") around **$Managed Object Name$** and a space after the second quotation.
f. Click the button to the right of the **Parameters** box and select **Owner**.
g. Type quotations ("") around **$Owner$**.
h. Verify that the final **Parameters** box looks like the following:

$Ticket ID$ "$Managed Object Name$" "$Owner$"

i. Ensure that the **Display output when this task is run** checkbox is not selected.
j. Click **Create**.

Event Command Line Tasks

Event command line tasks run a command line application or batch file based on an event. They are listed in the **Actions** pane of the Operations console when an event is selected. You can specify the path to the application and the working directory. You can also use properties from the selected event on the command line.

The following procedure creates a command line task to run a custom application creating a ticket in an external ticketing system based on the selected event. It runs a custom program that accepts the Event Number, Managed Object Name, and Description as command line parameters. In this example, it is expected that the managed object name and description would possibly include spaces, so they are enclosed in quotations.

To create an event command line task

1. Select the **Authoring** workspace.
2. In the Authoring pane, expand **Management Pack Objects**.
3. Right click **Tasks** and select **Create a New Task** to open the **Create Task Wizard**.
4. On the **Task Type** page, do the following:
   a. Under **Console Tasks**, select **Event command line**.
   b. In the **Select destination management pack** dropdown, select the management pack file to store the task. For more information about management packs, see Selecting a Management Pack File.
   c. Click **Next**.
5. On the **General Properties** page, do the following:
   a. Under **Task Name**, type **Create Ticket**. This is the text that will be displayed in the **Actions** pane.
   b. Click **Next**.
6. On the **Command Line** page, do the following:

a. In the **Application** box, type **c:\ticketing\CreateTicket.exe**.
b. Click the button to the right of the **Parameters** box and select **Number**.
c. Type a space after **$Number$**.
d. Click the button to the right of the **Parameters** box and select **Managed Object Name**.
e. Type quotations ("") around **$Managed Object Name$** and a space after the second quotation.
f. Click the button to the right of the **Parameters** box and select **Description**.
g. Type quotations ("") around **$Description$**.
h. Verify that the final **Parameters** box looks like the following:

   $Ticket ID$ "$Managed Object Name$" "$Description$"
i. Ensure that the **Display output when this task is run** checkbox is not selected.
j. Click **Create**.

See Also

Tasks

Agent Tasks

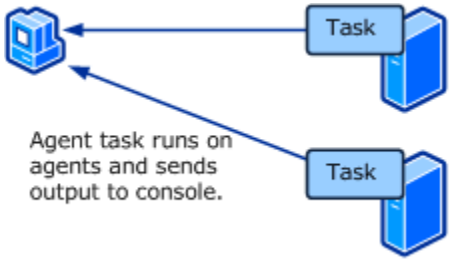
Agent Tasks

Agent tasks in System Center 2012 – Operations Manager are run on the agent computer where the target object is managed. An agent task can be a script or an executable program run from a command line. If an executable program is used, the application must be installed on the agent computer.

Agent tasks are useful for performing actions on the agent computer or for retrieving information for the user. They provide the following capabilities:

- Run a script or command locally on the agent computer without logging on to the computer interactively.
- Run a script or command on multiple agents with a single action.
- Run a script or command by using local user credentials with permissions not available to the user.

Agent Task



Credentials

Tasks run under the credentials of the Default Action Account on the agent computer. This account typically has sufficient privileges for accessing most application components, even if the user running the task does not have these user rights. If the task is required to perform an action requiring other credentials, such as accessing an external data source, then you can specify credentials when you run the task.

Output

Any output sent to the standard out stream (StdOut) from the script or command is provided to the user as Task Output in the Operations Console. Command line programs will typically output information to this stream. Scripts should output information by using commands such as WScript.Echo to provide this information.

Create Agent Task Wizard Options

When you run the **Create Agent Task** wizard, you have to provide values for the options in the following tables. Each table represents a single page in the wizard.

General Properties

The following options are available on the **General Options** page of the wizard.

Option	Description
Task Name	The name used for the task. This name is displayed in the **Actions** pane in the Operations console.
Description	Optional description of the task.
Task target	Target class of the task. The task will be displayed in the **Actions** pane when an instance of the target class is selected. Properties from the target object are available to use in the parameter of the task You do not specify a target for Alert and Event command line tasks. They are available to all alerts and events regardless of the class that created them.

Command Line

The following options are available on the **Command Line** page of the wizard. This page is only available for a command line agent task.

Option	Description
Application	Path and name of the application to run.
Parameters	Parameters to add to the command line. This can be a combination of static text and variables for the properties of the target class or one of its parent classes. If a variable used for a parameter could resolve to text containing a space, you should enclose the variable in quotations (""). If there are no quotations and the text includes a space, then it will be seen as multiple parameters.
Working directory	The default directory to use when the application is run.
Timeout	The number of seconds that the application is allowed to run. If it has not completed within this time, the application will be ended and an error returned.

UNIX/Linux Shell Command

The following options are available on the Shell Command Details page of the wizard. This page is only available for an **UNIX/Linux Shell Command** agent task.

Option	Description
Command	The shell command to execute. This can be the full path to a program or script, a command, or a one-line sequence of multiple commands (using pipeline operators).
Run As Profile	Either the **UNIX/Linux Action Account** or **UNIX/Linux Privileged Account** profile. Select the profile that associates the required account credentials with the task target. The associated account will be used to execute the command.
Timeout (seconds)	The number of seconds that the command can

Option	Description
	run before the agent stops it. This prevents problem commands from running continuously and putting excess overhead on the agent computer.

Script

The following options are available on the **Script** page of the wizard. This page is only available for a script agent task.

Option	Description
File Name	Name of the script. Must end in a .vbs or .js extension depending on whether your script is written in VBScript or JScript.
Timeout	The number of seconds that the script can run before the agent stops it. This prevents problem scripts from running continuously and putting excess overhead on the agent computer.
Script	The body of the script.
Parameters	Click to provide values for any arguments in the script. For more information, see Script Arguments.

Creating Agent Tasks

Command Line Agent Tasks

Command line agent tasks run a command line application or batch file using a target class. They are listed in the **Actions** pane of the Operations console when an instance of the target class is selected. You can specify the path to the application and the working directory. This application must be installed on the agent computer when the task is run. You can also use $Target variables from the target class or one of its parents to be included on the command line. Any output from the application sent to the console are delivered back to the user in the **Task Status** dialog box in the Operations console when the task is run.

The following procedure creates a console task to run the **netstat** utility to list the ports that the agent computer is listening on.

To create a command line agent task

1. Select the **Authoring** workspace.
2. In the Authoring pane, expand **Management Pack Objects**.
3. Right click **Tasks** and select **Create a New Task** to open the **Create Task Wizard**.
4. On the **Task Type** page, do the following:
   a. Under **Agent Tasks**, select **Command line**.
   b. In the **Select destination management pack** dropdown, select the management pack file to store the task. For more information about management packs, see Selecting a Management Pack File.
   c. Click **Next**.
5. On the **General Properties** page, do the following:
   a. Under **Task Name**, type **Netstat**. This is the text that will be displayed in the **Actions** pane.
   b. Click the Select button to open the **Select Items to Target** dialog box.
   c. Select **Windows Computer** and click **OK**.
   d. Click **Next**.
6. On the **Command Line** page, do the following:
   a. In the **Application** box, type **%windir%\system32\netstat.exe**.
   b. Click **Create**.

UNIX/Linux Shell Command Agent Tasks

UNIX/Linux Shell Command tasks run a command line application or script using a target class. They are listed in the **Actions** pane of the Operations console when an instance of the target class is selected. You can specify the path to a script or command, a command to run, or a one-line sequence of multiple commands (using pipeline operators). Any output from the application sent to the console are delivered back to the user in the **Task Status** dialog box in the Operations console when the task is run.

The following procedure creates a console task to run the **netstat** utility to list the ports that the agent computer is listening on.

To create an UNIX/Linux Shell Command agent task

1. Select the **Authoring** workspace.
2. In the Authoring pane, expand **Management Pack Objects**.
3. Right click **Tasks** and select **Create a New Task** to open the **Create Task Wizard**.
4. On the **Task Type** page, do the following:
   a. Under **Agent Tasks**, select **Run an UNIX/Linux Shell Command**.
   b. In the **Select destination management pack** dropdown, select the management pack file to store the task. For more information about management packs, see

Selecting a Management Pack File.

c. Click **Next**.

5. On the **General Properties** page, do the following:
   a. Under **Task Name**, type **Netstat**. This is the text that will be displayed in the **Actions** pane.
   b. Click the Select button to open the **Select Items to Target** dialog box.
   c. Select **UNIX/Linux Computer** and click **OK**.
   d. Click **Next**.
6. On the **Shell Command Details** page, do the following:
   a. In the **Command** box, type **netstat**.
   b. Select the **Run As profile** to use.
   c. Input the task timeout in seconds.
   d. Click **Create**.

Script Agent Tasks

Script agent tasks run a Windows script using a target class. They are listed in the **Actions** pane of the Operations console when an instance of the target class is selected. The script can perform some action or it can collect information that is delivered back to the user in the **Task Status** dialog box. To return information to the user, you can use any script command that will display information on the command line. For VBScript, this will typically be the **WScript.Echo** command.

The following procedure creates an agent script task to reboot the target computer. It accepts two parameters. The first is the name of the computer that it retrieves from the **Principal Name** property of the target. The second is a flag that specifies that the reboot should be performed. This value defaults to **false**, and the user must change it to **true** when they run the task or the reboot will not be performed. This provides an additional safety to the task to prevent an operator from accidentally performing a reboot.

To create a command line agent task

1. Select the **Authoring** workspace.
2. In the Authoring pane, expand **Management Pack Objects**.
3. Right click **Tasks** and select **Create a New Task** to open the **Create Task Wizard**.
4. On the **Task Type** page, do the following:
   a. Under **Agent Tasks**, select **Run a script**.
   b. In the **Select destination management pack** dropdown, select the management pack file to store the task. For more information about management packs, see Selecting a Management Pack File.
   c. Click **Next**.
5. On the **General Properties** page, do the following:
   a. Under **Task Name**, type **Reboot Computer**. This is the text that will be displayed in

the **Actions** pane.

b. Click the Select button to open the **Select Items to Target** dialog box.

c. Select **Windows Computer** and click **OK**.

d. Click **Next**.

6. On the **Script** page, do the following:

a. In the **File Name** box, type **RebootComputer.vbs**.

b. Leave the default of 1 minute for the **Timeout**.

c. Copy the following script and past into the **Script** box.

```
sComputer = WScript.Arguments(0)
bConfirmFlag = cbool(WScript.Arguments(1))

Set colOS =
GetObject("winmgmts:{impersonationLevel=impersonate,(Shutdown)
}//" & sComputer).ExecQuery("select * from
Win32_OperatingSystem where Primary=true")

If bConfirmFlag Then
    For each objOS in colOS
objOS.Reboot()
    Next
Else
WScript.Echo "Confirm flag set to false. Computer will not be
rebooted."
End If
```

d. Click **Parameters** to open the **Parameters** dialog box.

e. Click Target and then select **Principal Name**.

f. Type a space after the computer name variable and then type **false**. The final parameter line should look similar to the following:

$Target/Property[Type="MicrosoftWindowsLibrary7585000!Microsoft.Windows.Computer"]/PrincipalName$ false

g. Click **OK**.

h. Click **Create**.

See Also

Tasks

Distributed Applications

A *Distributed Application* in Operations Manager is an application that is comprised of multiple objects. These objects may be defined by different management packs and may be managed on the same agent or on different agents. The purpose of the distributed application is to provide an overall health for an application that is comprised of different objects.

Distributed applications do not provide any additional monitoring for the objects in an application. Instead, they include objects that are already being monitored. The value of the distributed application is to provide a relationship between the health of objects that are part of a single application.

You can create distributed applications using the **Distributed Applications Designer** in the Operations console.

Distributed Application Designer

The *Distributed Application Designer* provides you with the ability to create a distributed application in a graphical environment with minimal knowledge of the underlying management pack elements that are created. There are some limitations to the tool though as follows:

- The component groups can only have explicit members, which means that you cannot populate them dynamically. For example, you may have a distributed application with a set of web sites. You install an additional web server with a site that should be included. You would have to edit the distributed application and manually add the new site.
- You cannot create multiple levels of health rollup. The health of the application will be the worst health of any of the component groups regardless of the relationships that have been created for them.

You can create a distributed application without these limitations by using the Visual Management Pack Designer.

Contents of Distributed Applications

Objects

A distributed application must include one or more objects in order to be useful. Any object discovered by different management packs installed in the management group can be used in a distributed application. This might come from a management pack installed from the catalog or one that you have created on your own. These can be objects created by different monitoring wizards as discussed in Management Pack Templates.

Component Groups

A component group can contain any number of objects, and any object added to the distributed application must be contained in a component group. When you create the component group, you specify one or more classes that the group can contain. Only objects that are instances of these classes may be added to the particular group. If you specify **All Objects** then any objects in the management group can be included in the component group.

If you want to limit the objects that can be included in the component group, then you should select the **Object(s) if the following type(s)** and then select one or more classes from the class tree. The tree will contain all of the classes in the management group which are provided by all the management packs currently installed.

The dialog box arranges classes in a tree according to their base classes. You can read more about base classes at Base Classes. If you select a class, then each of its base classes will also be selected. This allows you to select a single class such as **Computer Role** that is often used as a base class and automatically select all of its base classes.

Relationships

Relationships can be drawn between component groups to represent some relation between different kinds of objects. Health is not rolled up between the component groups, but the relationship is indicated by lines between the groups.

Distributed Application Templates

Templates allow you to start a new distributed application with a predefined set of component groups. You need to add objects to these component groups and can modify the component groups and add additional component groups as you require. You can save time in creating a distributed application by selecting a template that most closely resembles your requirements. If you want to create an empty distributed application and manually add all your own component groups, then select the **Blank** template.

The following table lists the available templates:

Template	Description	Container Groups	Contained Classes
.NET 3-Tier Application	Brings together objects and monitoring data from synthetic transactions with data from Application Performance Monitoring	• [Application name] Client Perspective • [Application name] Presentation Tier • [Application name] Business Tier • [Application name] Data Tier	• Perspective • ASP.NET application • .NET application component • Database
Line of Business	Component groups	• Web Sites	• Web Site

Template	Description	Container Groups	Contained Classes
Web Application	common to a web application	• Databases	• Database
Messaging	Component groups common to messaging services	• Messaging Clients • Storage • Messaging Components • Directory Services • Network Services • Physical Network	• Perspective • • Logical Hardware Component • Computer Role • Computer Role • Network Device
Blank	Empty distributed application with no component groups	None	None

Viewing Distributed Applications

Each distributed application will be listed in the **Distributed Application** state view in the **Monitoring** pane of the Operations console. The state of the distributed application will be the worst state of any of the objects that it contains. You can launch any of the other kinds of the view by right-clicking on the distributed application and selecting the view that you want. Each view will include data for all of the objects contained in the distributed application.

Creating and Modifying Distributed Applications

To create a distributed application

1. If you don't have a management pack for the application that you are monitoring, create one using the process in Selecting a Management Pack File.
2. In the Operations console, select the **Authoring** workspace.
3. Right-click **Distributed Applications** and select **Create a new distributed application**.
4. In the **Name** box, type a name for the distributed application. This name will appear in the **Monitoring** workspace of the Operations console.
5. In the **Template** box, select the template for the starting point of the distributed application. See Distributed Application Templates for information on the available templates.
6. Select the management pack that you created in step 1.
7. Click **OK**.

To edit an existing distributed application

1. In the Operations console, select the **Authoring** workspace.
2. Select **Distributed Applications**.
3. In the **Distributed Applications** pane, right-click the distributed application you want to edit and select **Edit**.

To create a component group

1. With the distributed application open, click **Add Component**.

   Note
   The first time that you create a component group since opening the Operations console, it may take several seconds to open the **Create a New Component Group** dialog box since the list of classes must be cached. The amount of time that this takes will depend on the number of classes in your management group.
2. In the **Name your component group** text box, provide a name for the component group. This is the name that will appear in the diagram view and the Health Explorer for the distributed application.
3. If the component group should be able to contain any type of object, then select **All Objects**. If you want to specify one or more types that the component group should be able to contain, then select **Objects of the following type**.
4. Select one or more classes to allow objects of that type to be included in the management group.
5. Click **OK** when you have selected the classes.

   Note
   You may receive a message saying that the allowed limit was reached while making a new object type button visible. This means that no more object selection panes can be added to left side of the Distributed Application Designer. Either select **Leave the new object type not visible** to not create a new object selection panel for the current component group or select **Replace the selected visible Object Type button with a new one** and select one of the object types in the list to close. You can reopen the selection pane by selecting it in the **Organize Object Types** pane.

To add an object to the distributed application

1. Ensure that a component group is created that allows the type of object that you want to add.
2. If a selection pane is not open for the type of object you want to add, click **Organize Object Types** and then select the type of object you want to add.
3. Select the type of object you want to add in the Object Picker. This should display a list of all objects of the selected type.

4. Click and drag one or more of the objects into a component group. Note that you will only be able to add the objects to a component group that will accept objects of that type.

See Also

Understanding Classes and Objects

360 .NET Application Monitoring Dashboards in System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

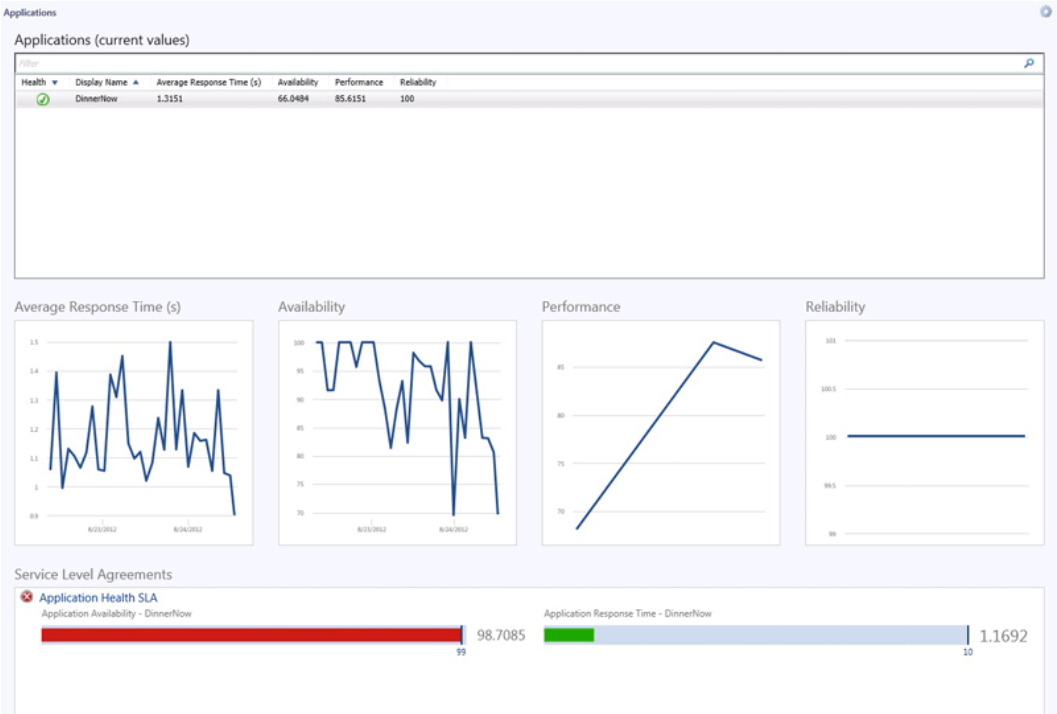
System Center 2012 – Operations Manager can show you different perspectives of application health in one place—360 .NET Application Monitoring Dashboards. The 360 .NET Application Monitoring Dashboards display information from Global Service Monitor, .NET Application Performance Monitoring, and Web Application Availability Monitoring to provide a summary of health and key metrics for 3-tier applications in a single view. The 360 .NET Application Monitoring Dashboards show where an application is unhealthy and provide a launch point for Application Summary Dashboards that highlight component-level issues, which are helpful when troubleshooting.

The 360 .NET Application Monitoring Dashboards display data from powerful monitoring tools. .NET Application Performance Monitoring looks deep into the application to get details that can help you pinpoint solutions from server- and client-side perspectives. Web Application Availability monitoring in Operations Manager monitors internal synthetic transactions. Global Service Monitor monitors the availability of applications from an outside location, measuring availability from where the user is.

The Applications Dashboard

The Applications Dashboard gives you a holistic view of all applications modeled through a Distributed Application (DA) and help answer these questions:

- Are my applications healthy? This is provided by the state view that shows the DA health as measured by availability from Global Service Monitor.
- Do the high-level metrics indicate a problem? Four metric scores provide this information, showing Average response time (Global Service Monitor), Availability (Global Service Monitor), Performance Exceptions (.NET Application Performance Monitoring), and Reliability (exception events from .NET Application Performance Monitoring.)
- Is the application meeting SLAs? Once you select a DA, the lower part of the dashboard retrieves all SLAs defined for that DA, and show a state for that SLA.



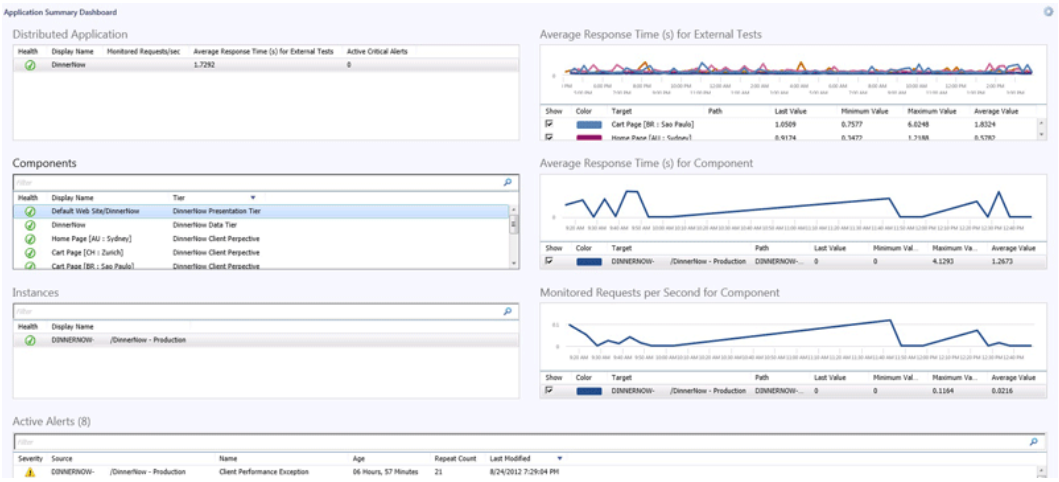
The Applications Dashboard highlights the following:

Key application metric or action	Type of monitoring used
Availability	Web Application Availability Monitoring and Global Service Monitor
Reliability	.NET Application Performance Monitoring
Performance	.NET Application Performance Monitoring and Global Service Monitor

The Application Summary Dashboard

The Application Summary Dashboard shows components and instances of applications, performance data, and active alerts. The data are not aggregated, so the Application Summary Dashboard is a useful tool for troubleshooting.

When you select an application in the Applications Dashboard, **Application Summary Dashboard** appears in the right rail. To open it, click **Application Summary Dashboard**.



The Applications Summary Dashboard highlights the following:

Key application metric or action	Type of monitoring used
Distributed Application	The distributed application that you selected on the Applications Dashboard
Components	Components discovered by .NET Application Performance Monitoring and Global Service Monitor that are part of the selected distributed application. When you select a component, the related data displays in the Average Response Time (s) for Component and Monitored Requests per Second for Component charts. **Note** Not all components have the associated data in these two charts—only the components discovered by .NET Application Performance Monitoring.
Instances	The instances of each component. For example, you might have several instances of a website running on several computers.
Active Alerts	Active alerts for the selected distributed application
Average Response Time (s) for External Tests	Average response time in seconds for the monitoring tests that you have configured in Global Service Monitor for the selected

Key application metric or action	Type of monitoring used
	distributed application
Average Response Time (s) for Component	Average response time in seconds for the selected component as configured by .NET Application Performance Monitoring
Monitored Requests per Second for Component	Monitored requests per second for the selected component as configured by .NET Application Performance Monitoring

See Also

Before You Begin Using 360 .NET Application Monitoring Dashboards in System Center 2012 SP1

How to Configure 360 .NET Application Monitoring Dashboards in System Center 2012 SP1

How to Use the 360 .NET Application Monitoring Dashboards in System Center 2012 SP1

Before You Begin Using 360 .NET Application Monitoring Dashboards in System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

Before you begin using 360 .NET Application Monitoring Dashboards, you must configure application monitoring for the applications you want to monitor.

Configure Application Monitoring

Before you begin using 360 .NET Application Monitoring Dashboards, you must configure .NET Application Performance Monitoring, Web Application Availability Monitoring, and Global Service Monitor for the applications you want to monitor. For more information, see:

- .NET Application Performance Monitoring Template
- Web Application Availability Monitoring Template
- Global Service Monitor documentation is on Connect. To get the documentation and get started, go to http://connect.microsoft.com and download **Global Service Monitor Installer** (Windows Installer).

Important

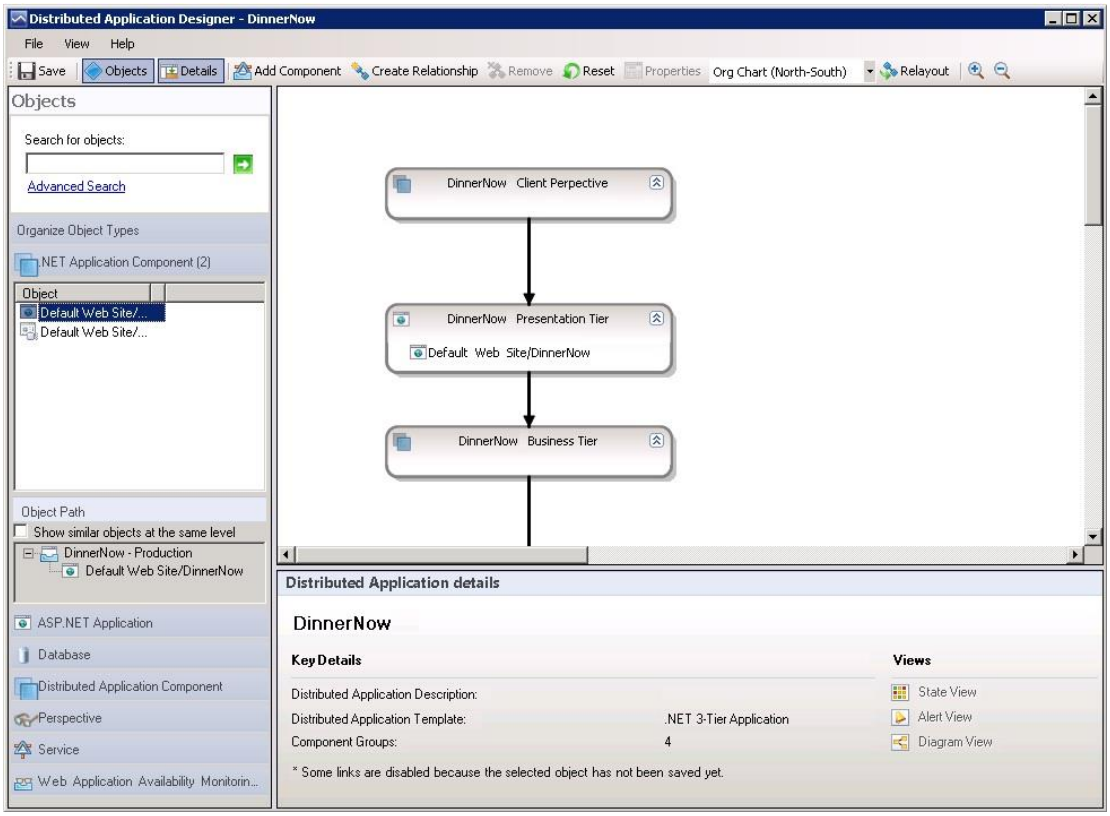
Before configuring the 360 .NET Application Monitoring Dashboards, make sure to allow enough time for all of the applications you want to monitor to be discovered.

How to Configure 360 .NET Application Monitoring Dashboards in System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

To configure 360 .NET Application Monitoring Dashboards

1. In Operations Manager, click the **Authoring** button.
2. Right-click **Distributed Applications** and select **Create a new distributed application**. The **Distributed Application Designer** opens.
3. In the **Distributed Application Designer**, choose a name for your distributed application and enter a description (optional). In the **Choose Distributed Application Template**, select the **.NET 3 Tier Application** template. In the **Save to a Management Pack** section, select an existing management pack or create a new management pack where your distributed application and its components will be saved. Click **OK**.
4. In the **Distributed Application Designer**, you can drag and drop the discovered application instances and components you want to monitor and view on the Application Summary Dashboard. Headings in the **Objects** pane map to the boxes. The items you drag in should be in the context of what you previously configured for.NET Application Performance Monitoring, Web Application Availability, and Global Service Monitor.



To select components and instances of the distributed application that you want to view in the Application Summary Dashboard, in **Object Types**, click an object type, select the instances you want display in the Application Summary Dashboard, and then drag them to the matching component group in the main flow.

Note

If you configured applications to monitor using 360 .NET Application Monitoring Dashboards, but do not see them in the Distributed Application Designer, you might need to allow more time for all of the applications you want to monitor to be discovered.

5. For more information about distributed applications and the Distributed Application Designer, see Distributed Applications.

To change thresholds for SLAs

1. To change thresholds for SLAs, in Operations Manager click the **Authoring** button, click **Management Pack Objects**, click **Service Level Tracking**, and then double-click **Application Health SLA**.
2. In the **Service Level Tracking** wizard, on the **Service Level Objectives** page, you can add, edit, or remove service level objectives, which define the performance thresholds or the states that you want to track for the selected targeted class, objects, or group. When you are done, click **Finish**.

Note

You can also add SLAs and SLOs and they will display in the Application Dashboard automatically.

To set the time range for data displayed in the dashboards

1. To set a time range for the data displayed in the Applications Dashboard, click the round icon in the upper right corner and click **Personalize**. Set the time range for data collections and then click **Finish**.
2. To set a time range for the data displayed in the Applications Summary Dashboard, click the round icon in the upper right corner and click **Personalize**. Set the time range for data collections and then click **Finish**.

To personalize the Application Summary Dashboard

1. To personalize the Application Summary Dashboard, hover over the section you want to modify, click the round icon above its upper right corner, and then click **Personalize**.

   Note

   You can personalize the **Average Response Time(s) for Externals Tests**, **Average Response Time(s) for Component**, **Monitored Requests per Second for Component**, and the **Active Alerts** sections. The **Distributed Application**, **Components**, and **Instances** sections cannot be personalized.
2. Select the display or chart preferences for the information you want the dashboard to display, and then click **Finish**.

To select locations to display on the Average Response Time(s) for External Tests dashboard

1. On the **Application Summary Dashboard**, in the **Average Response Time(s) for External Tests** section, the application components and locations you have configured to monitor from are listed and displayed on the chart. To change which application component and locations are displayed on the chart, select only the application component locations you want to see.
2. The chart will update automatically.

To synchronize active alerts in the Application Summary Dashboard with Team Foundation Server (TFS) work items

1. Import the Team Foundation Server (TFS) Work Item Management Pack into Operations Manager. This management pack synchronizes Operations Manager alerts with TFS work items so alerts from Operations Manager can be sent directly to development where they can view and track it in Visual Studio and remain synchronized with the alert you see in Operations Manager.
2. When the management pack is imported, assign an alert to engineering and this will synchronize the alert with TFS automatically.

How to Use the 360 .NET Application Monitoring Dashboards in System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

To open and use the Application Dashboard

1. In Operations Manager, click the **Monitoring** button, click **Application Monitoring**, and then click **Applications**.
2. To open the Application Dashboard, click the application you want to see details about.

   The 360 .NET Application Monitoring Dashboards show:

   - A list of all applications configured to appear in the 360 .NET Application Monitoring Dashboards
   - The current state of each 360 distributed application
   - Aggregated Average Transaction Response Time (in seconds) Performance Data from Global Service Monitor
   - Availability percentage for the last 24 hours represented as a score
   - Aggregated % Performance events for the last 24 hours represented as a score. (100 is a perfect score with no performance exceptions. This will be reduced as the % performance events are increased.)
   - Aggregated % Exception events represented as a score. (100 is a perfect score with no exception events. This number will be reduced as the % exception events are increased.)
   - The history of these counters, each in a performance graph, for the selected interval
   - SLA information. The default SLA thresholds can be changed. You can also add your own SLAs as long as they are targeted at the distributed application. These SLAs will also appear in the dashboard.

   You can also change the interval shown in the dashboard by clicking **Personalize**. The default is 24 hours.

   Note

   Information, such as average response, availability, performance, and reliability in the Applications Dashboard is aggregated. Aggregate performance counters provide value since the application owner typically wants to know how their website is performing, not how the individual instances of the website are performing. Instance-level detail is not required until troubleshooting begins.

To open and use the Application Summary Dashboard

1. The Application Summary Dashboard shows components and instances of applications, performance data, and active alerts. The data are not aggregated, so the Application Summary Dashboard is a useful tool for troubleshooting.

   To view an Application Summary Dashboard, click an application in the Applications Dashboard. **Application Summary Dashboard** appears in the right pane.
2. To open the Application Summary Dashboard, click **Application Summary Dashboard**.

Report Authoring for System Center 2012 - Operations Manager

The knowledge and procedures that you need for authoring custom reports in Operations Manager for System Center 2012 has not changed from System Center Operations Manager 2007 R2. For guidance, see the Operations Manager 2007 Report Authoring Guide.

Related Resources

- TechNet Library main page for Operations Manager
- What's New in Operations Manager for System Center 2012
- Operations Manager for System Center 2012 Release Notes
- Operations Guide for Operations Manager for System Center 2012
- Deployment Guide for Operations Manager for System Center 2012
- Operations Manager for System Center 2012 Supported Configurations

Cmdlets in System Center 2012 - Operations Manager

This section contains cmdlet reference information for System Center 2012 – Operations Manager cmdlets and Operations Manager cmdlets for UNIX and Linux.

For more information on using Windows PowerShell Cmdlets in System Center 2012 Operations Manager, see System Center 2012 Integration Guide - Operations Manager.

Topic	Description
Operations Manager Cmdlet Reference	This section contains cmdlet help topics for the System Center 2012 – Operations Manager cmdlets.
Operations Manager Cmdlets for UNIX and Linux	This section contains cmdlet help topics for the Operations Manager cmdlets for UNIX and Linux.

Operations Manager Cmdlet Reference

This section contains help topics for the System Center 2012 – Operations Manager cmdlets and about topics.

Topic	Description
Operations Manager Cmdlet Help Topics	Contains the cmdlet help topics for each of the Operations Manager cmdlets.
Operations Manager Cmdlet About Help Topics	Contains the about topics for the Operations Manager cmdlets.

Operations Manager Cmdlet About Help Topics

This section contains the conceptual ("about") help topics for the System Center 2012 – Operations Manager cmdlets.

Topic	Description
about_OpsMgr_Cmdlet_Names	Maps Operations Manager 2007 cmdlets to System Center 2012 – Operations Manager cmdlets.

Topic	Description
about_OpsMgr_Connections	Describes management group connection types that you can create in the Operations Manager shell.
about_OpsMgr_RunAsAccount	Describes how to create and associate Run As accounts in Operations Manager.
about_OpsMgr_WhatsNew	Describes new features in the System Center 2012 – Operations Manager cmdlets.

about_OpsMgr_Cmdlet_Names

about_OpsMgr_Cmdlet_Names

```
TOPIC
    about_OpsMgr_Cmdlet_Names


SHORT DESCRIPTION
    Maps the System Center Operations Manager 2007 cmdlets to the
    System Center 2012 - Operations Manager cmdlets.



LONG DESCRIPTION
    All cmdlets in System Center 2012 - Operations Manager have new names, and can
    be identified by the "SCOM" or "SC" preceding the noun name. In some cases, the
    verb associated with the cmdlet has also been updated.

    This topic outlines which cmdlets are new to System Center 2012 - Operations
    Manager, which Operations Manager 2007 cmdlets have an equivalent System Center -
    2012 Operations Manager cmdlet ("renamed" cmdlets), and Operations Manager 2007
    cmdlets that have no System Center 2012 - Operations Manager equivalent ("deprecated"
    cmdlets).

    ----------------------------------------------------------------------
```

```
SYSTEM CENTER 2012 - OPERATIONS MANAGER MODULE NAME
-------------------------------------------------------------------------


Operations Manager 2007 snap-in
    Microsoft.EnterpriseManagement.OperationsManager.Client


System Center 2012 - Operations Manager module
    OperationsManager


-------------------------------------------------------------------------
NEW SYSTEM CENTER 2012 - OPERATIONS MANAGER CMDLETS
-------------------------------------------------------------------------
Add-SCOMADAgentAssignment
Add-SCOMAlertResolutionState
Add-SCOMConnector
Add-SCOMNotificationChannel
Add-SCOMNotificationSubscriber
Add-SCOMNotificationSubscription
Add-SCOMRunAsAccount
Add-SCOMRunAsProfile
Add-SCOMSubscriberSchedule
Add-SCOMUserRole
Clear-SCOMSubscriberSchedule
Disable-SCOMAgentProxy
Disable-SCOMDiscovery
Disable-SCOMMonitor
Disable-SCOMOperationalDataReporting
Enable-SCOMAgentProxy
Enable-SCOMDiscovery
Enable-SCOMMonitor
Enable-SCOMOperationalDataReporting
Exit-SCOMCEIP
Export-SCOMEffectiveMonitoringConfiguration
Get-SCOMAccessLicense
```

Get-SCOMADAgentAssignment

Get-SCOMAgentApprovalSetting

Get-SCOMAlertResolutionSetting

Get-SCOMAlertResolutionState

Get-SCOMDatabaseGroomingSetting

Get-SCOMDataWarehouseSetting

Get-SCOMErrorReportingSetting

Get-SCOMHeartbeatSetting

Get-SCOMLicense

Get-SCOMLocation

Get-SCOMManagementGroup

Get-SCOMReportingSetting

Get-SCOMResourcePool

Get-SCOMRMSEmulator

Get-SCOMRunAsDistribution

Get-SCOMRunAsProfile

Get-SCOMWebAddressSetting

Join-SCOMCEIP

New-SCOMLocation

New-SCOMResourcePool

Remove-SCOMADAgentAssignment

Remove-SCOMAlertResolutionState

Remove-SCOMConnector

Remove-SCOMLocation

Remove-SCOMNotificationChannel

Remove-SCOMNotificationSubscriber

Remove-SCOMNotificationSubscription

Remove-SCOMResourcePool

Remove-SCOMRMSEmulator

Remove-SCOMRunAsAccount

Remove-SCOMRunAsProfile

Remove-SCOMSubscriberSchedule

Repair-SCOMAgent

Set-SCOMAgentApprovalSetting

Set-SCOMAlertResolutionSetting

Set-SCOMDatabaseGroomingSetting

Set-SCOMDataWarehouseSetting

Set-SCOMErrorReportingSetting

Set-SCOMHeartbeatSetting

Set-SCOMLicense

Set-SCOMLocation

Set-SCOMMaintenanceMode

Set-SCOMReportingSetting

Set-SCOMResourcePool

Set-SCOMRMSEmulator

Set-SCOMRunAsDistribution

Set-SCOMRunAsProfile

Set-SCOMWebAddressSetting

Test-SCOMCEIP

Test-SCOMOperationalDataReporting

Update-SCOMADAgentAssignment

Update-SCOMLocation

Update-SCOMRunAsAccount

Write-SCOMCommand

RENAMED CMDLETS

Operations Manager 2007 Name	System Center 2012 - Operations Manager Name
Add-ConnectorToTier	Add-SCOMTierConnector
Add-RemotelyManagedComputer	Add-SCOMAgentlessManagedComputer
Add-UserToUserRole	Set-SCOMUserRole
Approve-AgentPendingAction	Approve-SCOMPendingManagement
Disable-NotificationSubscription	Disable-SCOMNotificationSubscription
Disable-Rule	Disable-SCOMRule
Enable-NotificationSubscription	Enable-SCOMNotificationSubscription

Enable-Rule	Enable-SCOMRule
Export-ManagementPack	Export-SCOMManagementPack
Get-Agent	Get-SCOMAgent
Get-AgentPendingAction	Get-SCOMPendingManagement
Get-Alert	Get-SCOMAlert
Get-AlertHistory	Get-SCOMAlertHistory
Get-Connector	Get-SCOMConnector
Get-DefaultSetting	Get-SCOM<SettingName>Setting
Get-Diagnostic	Get-SCOMDiagnostic
Get-Discovery	Get-SCOMDiscovery
Get-Event	Get-SCOMEvent
Get-FailoverManagementServer	Get-SCOMParentManagementServer
Get-GatewayManagementServer	Get-SCOMGatewayManagementServer
Get-MaintenanceWindow	Get-SCOMMaintenanceMode
Get-ManagementGroupConnection	Get-SCOMManagementGroupConnection
Get-ManagementPack	Get-SCOMManagementPack
Get-ManagementServer	Get-SCOMManagementServer
Get-Monitor	Get-SCOMMonitor
Get-MonitorHierarchy	Get-SCOMMonitor
Get-MonitoringClass	Get-SCOMClass
Get-MonitoringObject	Get-SCOMClassInstance
Get-MonitoringObjectGroup	Get-SCOMGroup
Get-NotificationAction	Get-SCOMNotificationChannel
Get-NotificationEndpoint	Get-SCOMNotificationChannel
Get-NotificationRecipient	Get-SCOMNotificationSubscriber
Get-NotificationSubscription	Get-SCOMNotificationSubscription
Get-Override	Get-SCOMOverride
Get-OperationsManagerCommand	Get-SCOMCommand
Get-PrimaryManagementServer	Get-SCOMParentManagementServer
Get-Recovery	Get-SCOMRecovery
Get-RelationshipClass	Get-SCOMRelationship
Get-RelationshipObject	Get-SCOMRelationshipInstance
Get-RemotelyManagedComputer	Get-SCOMAgentlessManagedComputer
Get-ResultantCategoryOverride	Get-SCOMOverrideResult

Get-ResultantRuleOverride	Get-SCOMOverrideResult
Get-ResultantUnitMonitorOverride	Get-SCOMOverrideResult
Get-RootManagementServer	Get-SCOMRMSEmulator
Get-Rule	Get-SCOMRule
Get-RunAsAccount	Get-SCOMRunAsAccount
Get-Task	Get-SCOMTask
Get-TaskResult	Get-SCOMTaskResult
Get-UserRole	Get-SCOMUserRole
Install-Agent	Install-SCOMAgent
Install-AgentByName	Install-SCOMAgent
Install-ManagementPack	Import-SCOMManagementPack
New-LdapQueryDiscoveryCriteria	Install-SCOMAgent
New-MaintenanceWindow	Start-SCOMMaintenanceMode
New-ManagementGroupConnection	New-SCOMManagementGroupConnection
New-Tier	Add-SCOMTieredManagementGroup
New-WindowsDiscoveryConfiguration	Install-SCOMAgent
Reject-AgentPendingAction	Deny-SCOMPendingManagement
Remove-ConnectorFromTier	Remove-SCOMTierConnector
Remove-DisabledMonitoringObject	Remove-SCOMDisabledClassInstance
Remove-ManagementGroupConnection	Remove-SCOMManagementGroupConnection
Remove-RemotelyManagedComputer	Remove-SCOMAgentlessManagedComputer
Remove-Tier	Remove-SCOMTieredManagementGroup
Resolve-Alert	Set-SCOMAlert
Set-AlertDestination	Set-SCOMAlert
Set-DefaultSetting	Set-SCOM<SettingName>Setting
Set-ManagementServer	Set-SCOMParentManagementServer
Set-ProxyAgent	Set-SCOMAgentlessManagedComputer
Start-Discovery	Install-SCOMAgent
Start-Task	Start-SCOMTask
Uninstall-Agent	Uninstall-SCOMAgent
Uninstall-ManagementPack	Remove-SCOMManagementPack

DEPRECATED OPERATIONS MANAGER 2007 CMDLETS

Get-AlertDestination

New-CustomMonitoringObject

New-DeviceDiscoveryConfiguration

Get-MonitoringClassProperty

Get-MonitoringObjectPath

Get-MonitoringObjectProperty

New-MonitoringPropertyValuePair

Get-PerformanceCounter

Get-PerformanceCounterValue

Add-RemotelyManagedDevice

Get-RemotelyManagedDevice

Remove-RemotelyManagedDevice

Get-State

SEE ALSO

about_OpsMgr_WhatsNew

about_OpsMgr_Connections

about_OpsMgr_Connections

TOPIC

about_OpsMgr_Connections

SHORT DESCRIPTION

Describes the types of management group connections that you can create when using the Operations Manager Shell.

LONG DESCRIPTION

To use the System Center Operations Manager 2012 cmdlets, you need to establish a connection to an Operations Manager management group. There are two types of connections that you can establish: persistent and temporary.

If you have not previously used the Operations Console, the first time you use the command shell you will be prompted for the name of a management server to connect to. If you have used either the Operations Console or the command shell before, the command shell will attempt to connect to the last management server to which it had successfully connected.

PERSISTENT CONNECTIONS

To create a persistent management group connection, use the New-SCOMManagementGroupConnection cmdlet. You can establish multiple management group connections, but only one can be active at a time.

To set an active connection, use the Set-SCOMManagementGroupConnection cmdlet. You can also use Set-SCOMManagementGroupConnection to change which management group connection is the active connection. After you have set an active connection, all cmdlets that you run will use this connection by default.

To see which connection is the active connection, use the Get-SCOMManagementGroupConnection cmdlet. This cmdlet lists all established management group connections and identifies the active connection.

TEMPORARY CONNECTIONS

You can create a temporary connection to a management group that is not the active management group connection by using the ComputerName and Credential parameters for a cmdlet. If you do not specify credentials, the user's security context is used.

OPENING THE OPERATIONS MANAGER SHELL FROM THE OPERATIONS CONSOLE

You can open the Operations Manager Shell from the Operations Console by using the following method: right-click an object in the user interface, click Open, and then click Operations Manager Shell.

When you use this method to open the command shell, the user interface passes the object's instance ID to the command shell as an argument. After the command shell opens, it establishes a connection to the management server, and then and runs the following command:

```
Get-SCOMClassInstance -ID [Id of the selected object]
```

You will see the command written to the console before it is run. The instance returned from this cmdlet is stored in a variable named $context. You can use the $context variable within that PowerShell session to take actions on the object.

SEE ALSO

New-SCOMManagementGroupConnection

Get-SCOMManagementGroupConnection

set-SCOMManagementGroupConnection

Remove-SCOMManagementGroupConnection

about_OpsMgr_WhatsNew

about_OpsMgr_RunAsAccount

---

about_OpsMgr_RunAsAccount

TOPIC

about_OpsMgr_RunAsAccount

SHORT DESCRIPTION

Describes how to create and associate a new Run As account.

LONG DESCRIPTION

A Run As account is a named set of credentials that is presented by a Run As profile for authentication when monitors, rules, or tasks are run. A Run As account may be used by one or more Run As profiles.

You can get existing Run As accounts by using the Get-SCOMRunAsAccount cmdlet. To create a Run As account, use the Add-SCOMRunAsAccount cmdlet. You can manage the secure distribution of Run As accounts by using the Get-SCOMRunAsDistribution and Set-SCOMRunAsDistribution cmdlets.

There are many types of Run As accounts, each of which uses a unique set of parameters to create. For examples of how to create each type of Run As account, type: "Get-Help Add-SCOMRunAsAccount -examples".

EXAMPLES

The following example script creates a Windows Run As account object, and sets it for approved secure distribution to all Agents and Management Servers.

```
# Get credentials for the Run As account. The user name should be
# entered in the format "domain\user".
$Creds = Get-Credential

# Create the Run As account object.
$RunAsAccount = Add-SCOMRunAsAccount -Windows `
                                     -Name "My New Run As Account" `
                                     -RunAsCredential $creds
```

```
        # Creates an array consisting of all Agent and Management Server objects
        # present in the Management Group.
        $distribution = ( Get-SCOMAgent ) +
                        ( Get-SCOMManagementServer )

        # Approves the new account for secure distribution to all Agents
        # and Management Servers.
        Set-SCOMRunAsDistribution -RunAsAccount $runAsAccount `
                                  -MoreSecure `
                                  -SecureDistribution $distribution
```

After you have created your Run As account, you must associate the Run As account with a Run As profile to use the account. The following commands get the Run As profile with which to associate the Run As account, the Run As account, and the class instance. Then, the last command uses the Set-SCOMRunAsProfile cmdlet to add the Run As account to the Run As profile.

```
        $Profile = Get-SCOMRunAsProfile -DisplayName "My Run As Profile"
        $Account = Get-SCOMRunAsAccount -Name "My New Run As Account"
        $Instance = Get-SCOMClassInstance -DisplayName "Contoso financial SQL Servers"
        Set-SCOMRunAsProfile -Action "Add" -Profile $Profile -Account $Account -Instance
$Instance
```

SEE ALSO

Add-SCOMRunAsAccount

Get-SCOMRunAsAccount

Get-SCOMRunAsDistribution

Set-SCOMRunAsDistribution

Get-SCOMRunAsProfile

Set-SCOMRunAsProfile

about_OpsMgr_WhatsNew

about_OpsMgr_WhatsNew

TOPIC

about_OpsMgr_WhatsNew

SHORT DESCRIPTION

Describes the new features that are included with the System Center Operations Manager 2012 cmdlets.

LONG DESCRIPTION

The Operations Manager 2012 cmdlets are provided in a module that is imported into the Operations Manager Shell. To start the Operations Manager Shell from the Windows user interface, click Start, All Programs, System Center Operations Manager 2012, and then Operations Manager Shell. To manually import the OM10 module into a Windows PowerShell session, type "Import-Module OperationsManager" at the command prompt.

After you have opened an Operations Manager Shell session or manually imported the module, you can run the individual cmdlets alone or combine them into scripts to automate tasks.

The cmdlets in this module are only compatible with Operations Manager 2012. You can recognize the Operations Manager 2012 cmdlets by the "SCOM" preceding the noun name.

To work with the Operations Manager 2007 cmdlets, see "Using the Deprecated Operations Manager 2007 Cmdlets" later in this topic.

WINDOWS POWERSHELL 2.0 SUPPORT

Operations Manager 2012 adds support for Windows PowerShell 2.0, which includes new cmdlets, parameters, and features, including the following:

Remoting

You can run commands on one or several remote computers by using a single command. You can run individual commands, or create a session in which you can run a series of commands.

Background Jobs

Background jobs are commands that run asynchronously, returning the command prompt immediately, even if the command is still running. You can use background jobs to run commands in the background so that you can continue to use your session for other work while the command runs. You can run a background job on a remote computer by using the Invoke-Command cmdlet.

Script Debugger

You can use the cmdlet-based debugger to help you debug functions and scripts. The debugger cmdlets allow you to set and manage breakpoints, and let you display the call stack.

For more information about PowerShell 2.0, see about_Windows_PowerShell_2.0.

CONNECTIONS

To use the Operations Manager 2012 cmdlets, you need to establish a connection to an Operations Manager management group. There are two types of connections that you can establish: persistent and temporary. To establish a new, persistent, management group connection, use the New-SCOMManagementGroupConnection cmdlet. To establish a temporary connection, use the ComputerName and Credential parameters for the cmdlet.

For more information about connections in Operations Manager 2012, see about_OpsMgr_Connections.

NEW CMDLETS

Operations Manager 2012 provides a full set of new cmdlets. For information about how the Operations Manager 2007 cmdlets map to the Operations Manager 2012 cmdlets, see about_OpsMgr_Cmdlet_Names.

Following are some common tasks you might want to perform in Operations Manager with their associated cmdlets.

AGENTS

Task	Cmdlets
Get a list of agents	Get-SCOMAgent
Install or uninstall an agent	Install-SCOMAgent Uninstall-SCOMAgent Get-SCOMPendingManagement Approve-SCOMPendingManagement Deny-SCOMPendingManagement

ALERTS

Task	Cmdlets
Get a list of alerts	Get-SCOMAlert
Update or close multiple alerts	Set-SCOMAlert
Put a resource into or remove it from maintenance mode	Get-SCOMMaintenanceMode Start-SCOMMaintenanceMode

	Set-SCOMMaintenanceMode

MANAGEMENT PACKS

Task	Cmdlets
Get a list of management packs	Get-SCOMManagementPack
Backup and remove management packs	Get-SCOMManagementPack -Recurse |` Export-SCOMManagementPack |` Remove-SCOMManagementPack -Confirm
Get objects in a management pack	Get-SCOMDiscovery Get-SCOMRule Get-SCOMMonitor Get-SCOMGroup Get-SCOMClass Get-SCOMClassInstance Get-SCOMRunAsProfile Get-SCOMRunAsAccount
Enable or disable a workflow	Enable-SCOMDiscovery Disable-SCOMDiscovery Enable-SCOMMonitor Disable-SCOMMonitor Enable-SCOMRule Disable-SCOMRule

WORKING WITH THE MANAGEMENT GROUP OBJECT

Most objects returned by cmdlets in this module include properties and

methods from the Operations Manager Software Development Kit (SDK)
(http://go.microsoft.com/fwlink/?LinkId=194656). To see what methods
and properties are available on the objects returned by the cmdlets,
use the Get-Member cmdlet. For example:

```
Get-SCOMAlert | Get-Member
```

For more information about Get-Member, type "Get-Help Get-Member".

In the following example, the first command gets an agent object, and the
second command returns the management group object for the agent object:

```
C:\PS> $Agent = Get-SCOMAgent -Name Server01
C:\PS> $Agent.ManagementGroup
```

NOTE: The "ManagementGroup" property for an object provides programmatic
access to the management group that the object was retrieved from, using
the Operations Manager SDK. The Get-SCOMManagementGroup cmdlet can also
be used to obtain a management group object.

USING THE DEPRECATED OPERATIONS MANAGER 2007 CMDLETS

The Operations Manager 2007 cmdlets are deprecated in Operations Manager
2012 and will be removed in a future release. However, they are still
available for use while migrating from Operations Manager 2007. To use
the deprecated cmdlets, you must open a PowerShell session, load the
snap-in, and then run the startup script:

```
C:\PS>Add-PSSnapIn Microsoft.EnterpriseManagement.OperationsManager.Client
C:\PS>cd "$env:Program Files\System Center Operations Manager 2012\Console"
c:\PS>.\Microsoft.EnterpriseManagement.OperationsManager.ClientShell.Startup.ps1
```

SEE ALSO

about_OpsMgr_Cmdlet_Names

```
about_OpsMgr_Connections

about_OpsMgr_RunAsAccount
```

Operations Manager Cmdlets for UNIX and Linux

Insert introduction here.

Section Heading

Insert section body here.

Subsection Heading

Insert subsection body here.

Glossary for System Center 2012 - Operations Manager

Term	Definition
action account	The Windows account that is used by the MonitoringHost.exe processes to gather data from providers and to run actions, such as scripts and command-line batch files, on monitored devices.
agent	The feature that is installed on a Windows-based computer that performs management. The agent collects data, compares sampled data to predefined values, creates alerts, and runs responses.
Agentless Exception Monitoring	A feature in Operations Manager that allows the collection of client application crash data to a single location on a management server,

Term	Definition
	resulting in data that can then be analyzed by your company for patterns.
agentless managed computer	A computer without an agent that is monitored by a management server or a proxy agent.
agent-managed computer	A computer that has an agent installed on it and that reports to a management group.
alert	An indication of a significant event requiring attention. Alerts are created by rules and monitors.
alert severity	The property of an alert indicating the seriousness of the condition it communicates, such as, Service Unavailable, Security Issue, Critical Error, Error, Warning, Information, and Success.
Alert view	A view in the Operations console that displays the alerts that the console user has the rights to see about a specific object.
Audit Collection Services	A service, required by Operations Manager, that collects and forwards all security events from monitored computers to a central database.
class	A definition of an item that can be discovered and managed. A class can be targeted by monitors, rules, discoveries, and tasks.
company knowledge	An editable field of a rule or monitor in which you can capture any relevant information about the required steps to resolve an alert that was raised by the rule or monitor.
data warehouse server	The server that hosts the OperationsManagerDW database.
discovery	An element in a management pack that defines logic for locating monitored objects and their properties and relationships between different objects.
Event view	A view in the Operations console that displays specified events in the management group that

Term	Definition
	the console user has the rights to see.
Favorite view	A view available from the My Workspace area of the Operations console where you can save views that you regularly use, similar to how you save a webpage to your Favorites list in Internet Explorer.
gateway server	A server role in Operations Manager that enables the monitoring of computers that lie outside of the Kerberos trust boundaries (Kerberos realm) of the management group.
heartbeat	A message generated by an agent that tells its management server that the agent is functioning. It also informs Operations Manager about the current rules that are evaluated by the agent, and if it is necessary, it requests updates.
management group	The basic functional unit of an Operations Manager implementation that can perform monitoring. It must contain a SQL Server 2008 database server, one or more management servers, one or more Operations consoles, and one or more agents. In addition, it can also contain a reporting server, a gateway server, and an Audit Collection Services server.
management pack	A set of files that you install for use with Operations Manager and that allow you to monitor applications and add functionality to Operations Manager.
management server	The component of an Operations Manager management group that is responsible for communication with agents, databases, and the root management server.
model	In Operations Manager, a software representation of hardware, software, services and other logical components that are in your environment. The model captures the nature of those components and the relationships between them.

Term	Definition
monitor	In Operations Manager, an element in a management pack that defines logic for determining the health state of an object. A monitor can set health state.
Operations console	The Operations Manager interface that you use to perform monitoring, administration, authoring, and reporting functions.
Operations Manager Connector Framework	An interface to the System Center Data Access Service that allows applications to synchronously communicate with a management server.
Operations Manager Health Explorer	A feature of Operations Manager that allows you to view and then take action on alerts, state changes, and other significant issues generated by monitoring objects on your network.
Operations Manager reporting server	The server role that is responsible for building and presenting reports.
Operations Manager Shell	A customized instance of Windows PowerShell that provides a collection of Operations Manager-specific cmdlets.
override	A mechanism by which the default behavior of a rule, monitor, or discovery can be changed for a specific target, group, or object.
Performance view	The Operations console pane that displays specified performance information.
product connector	A software component that is used to synchronize data between Operations Manager and other management systems.
product knowledge	Content, embedded in rules and monitors, that contains information from the management pack author about the causes of an alert and suggestions on how to fix the issue that caused an alert to be raised.
reporting data warehouse	An Operations Manager feature that manages the OperationsManagerDW database and that can be independently installed.

Term	Definition
resolution state	The state of an alert in relation to its status in the resolution cycle. The default resolution states include New, Acknowledged, and Resolved.
resource pool	A collection of management servers that automatically distributes Operations Manager workflows between the management servers in that collection. If one or more management servers become unavailable, the workflows are automatically redistributed.
rule	In Operations Manager, an element in a management pack that defines the events and performance data to collect from computers, and what to do with the information after it is collected. A rule cannot set a health state.
Run As account	A Windows account that can be associated with a Run As profile, and that can use the Windows Authentication, NTLM, Basic, or Digest methods of authentication.
synthetic transaction	A method that can be used to test the availability or performance of a specific service or application from the perspective of an end user. In Operations Manager, these are initiated by rules and monitors.
System Center Data Access service	A Windows service that runs on the management servers in each management group, and that allows client applications to access Operations Manager data and functionality.
task	In Operations Manager, an element in a management pack that is manually initiated by an operator to run a predefined command or script against a monitored object.
user role	A combination of a profile and a scope. A profile defines actions that a user is allowed to perform. A scope defines the objects on which the actions can be performed.

Term	Definition
view	In the Operations console, a display of a filtered set of data from the OperationsManagerDB database.
web console	The browser-based interface that allows you to access the monitoring and reporting workspaces according to your user role.

Privacy Statement for System Center 2012 - Operations Manager

At Microsoft, we're working hard to protect your privacy, while delivering products that bring you the performance, power and convenience you desire in your personal computing. This privacy statement explains many of the data collection and use practices of Microsoft System Center 2012 – Operations Manager. This privacy statement focuses on features that communicate with the Internet and is not intended to be an exhaustive list. It does not apply to other online or offline Microsoft sites, products or services.

Collection and Use of your Personal Information

When we need information that personally identifies you or allows us to contact you, we will explicitly ask you for it. The personal information we collect from you will be used by Microsoft and its controlled subsidiaries and affiliates to provide the service(s) or carry out the transaction(s) you have requested or authorized, and may also be used to request additional information on feedback that you provide about the product or service that you are using; to provide critical updates and notifications regarding the software; to improve the product or service, for example bug and survey form inquiries, or to provide you with advance notice of events or to tell you about new product releases.

Except as described in this statement, personal information you provide will not be transferred to third parties without your consent. We occasionally hire other companies to provide limited services on our behalf, such as performing statistical analysis of our services. We will only provide those companies the personal information they need to deliver the service, and they are prohibited from using that information for any other purpose.

Information that is collected by or sent to Microsoft may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries or agents maintain

facilities, and by using a Microsoft site or service, you consent to any such transfer of information outside of your country. Microsoft abides by the safe harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of data from the European Union. Microsoft may disclose personal information about you if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on Microsoft or the site; (b) protect and defend the rights or property of Microsoft (including enforcing our agreements), or (c) act in urgent circumstances to protect the personal safety of Microsoft employees, users of Microsoft products or services, or members of the public.

Collection and Use of Information about Your Computer

Operations Manager contains Internet enabled features that can collect certain standard information from your computer ("standard computer information") along with information needed for a specific feature and send it to Microsoft. Standard computer information includes information such as your IP address, operating system version, a code that identifies the manufacturer of your computer, and your regional and language settings. This computer information is generally not personally identifiable.

Security of Your Information

Microsoft is committed to protecting the security of your personal information. We use a variety of security technologies and procedures to help protect your personal information from unauthorized access, use, or disclosure. For example, we store the information you provide on computer servers with limited access that are located in controlled facilities.

Changes to the Privacy Statement

We may occasionally update this privacy statement. When we do, we will revise the "last updated" date at the top of the privacy statement. We encourage you to periodically review this privacy statement to be informed of how Microsoft is protecting your information.

For More Information

Microsoft welcomes your comments regarding this privacy statement. If you believe that Microsoft has not adhered to this privacy statement, please contact us by e-mail at OMPrivacy@microsoft.com.

Microsoft Privacy

Microsoft Corporation

One Microsoft Way

Redmond, Washington 98052 USA

Specific Features:

The following features describe the functionality and controls in Operations Manager:

Customer Experience Improvement Program

What This Feature Does:

If you choose to participate, the Customer Experience Improvement Program (CEIP) feature will collect information about how all users of the Operations Console use Operations Manager so that we can identify trends and usage patterns. This information helps improve the quality, reliability, and performance of Microsoft software and services.

Information Collected, Processed, or Transmitted:

The information CEIP collects includes software and hardware performance, as well as basic software and hardware configuration such as RAM, processor type, and screen resolution. We do not collect names, addresses or other contact information. For more information about CEIP, see the Microsoft Customer Experience Improvement Program.

Use of Information:

The information collected is used to help improve Microsoft's products and services. Microsoft employees, contractors and vendors who have a business need to use the data are provided access as necessary.

Choice/Control:

The first time you install the Operations Manager Database server, during setup you'll be asked whether you would like to participate in CEIP.

To turn CEIP on or off later:

1. Start the Operations console, and in the navigation pane, select **Administration**.
2. In the **Administration** workspace under **Device Management**, select **Settings**.
3. In the **Settings** view, under **Type: General**, double-click **Privacy** to launch the **Global Management Group Setting-Privacy** property page.
4. Select the **CEIP** tab.
5. To turn CEIP off, select **I don’t want to join this program at this time**.

   To turn CEIP on, select **Join the Customer Experience Improvement Program (Recommended)**.
6. Click **OK**.

Important Information:

The Operations Manager administrator or other administrator with sufficient privileges may construct Group Policy to opt in or out of CEIP by setting a registry-based policy. The relevant registry key and settings are as follows:

Key = HKEY_LOCAL_MACHINE\Software\Microsoft\SQMClient\SCOM

RegEntry name = CEIPEnable

Entry type REG_DWORD (Hexadecimal):

0 is off

1 is on

Operational Data Reporting

What This Feature Does:

Operational Data Reports summarize how Operations Manager is being used in your management group. If you consent to sending operational data reports to Microsoft, each week, SQL Server 2005 Reporting Services reports will be generated from the operational data in your Operations Manager Data Warehouse and sent to Microsoft.

Information Collected, Processed, or Transmitted:

Operational Data Reports are XML files with data about your system configuration and the Microsoft-authored management packs that you are using. The reports include information about the operational environment of a management group, such as the number of agents controlled by Operations Manager, the most common alerts, and which management packs you are running.

Sample Operational Data Reports can be viewed at the Operations Manager web site along with descriptions of the data collected. If you have consented to sending these reports, you may view the reports that will be sent to Microsoft by navigating to the %windir%\temp\OpsMgr 2012 Operational Data Reports folder on the management server running the ODR workflows. Note: You can determine this by running the Show Running Workflows task against each of the management servers in the management group.

You can also view your Management Group, Management Pack, and Most Common Alerts Operational Data Reports by going to the Operations Console and in the Reporting View running these reports in the Microsoft ODR Report Library folder.

Use of Information:

Microsoft uses the data in Operational Data Reports to better understand how the Operations Manager product works as deployed in customers' environments. These reports will help improve future software and services.

Choice/Control:

The first time you install the Operations Manager Data Warehouse server, you'll be asked whether you would like to send Operations Data Reports to Microsoft.

To turn Operational Data Reporting on or off after install:

1. Start the Operations console, in the navigation pane select **Administration**.
2. In the **Administration** workspace, under **Device Management**, select **Settings**.
3. In the **Settings** View, under **Type: General**, right-click **Privacy** and choose **Properties** from the context menu.
4. Select the **Operational Data Reports** tab.
5. To turn Operational Data Reports off, select **No, don't send operational data reports to Microsoft**.

   To turn Operational Data Reports on, select **Yes, send operational data reports to Microsoft (recommended)**.
6. Click **OK**.

Important Information:

Operational Data Reporting cannot be configured using Group Policy.

Operations Manager Error Reporting

What This Feature Does:

Operations Manager Error Reporting asks users to send error report data to Microsoft via the Internet. This feature allows you to report problems you may be having with Operations Manager Management Servers, Gateway Servers, and Agents components. Please note that this feature does not control error reporting for other Operations Manager components such as Operations Console, Web Console, and Reporting Server. The Operations Manager Database and Data Warehouse error reporting behavior is defined by what settings SQL Server 2005 is using.

Choice/Control:

The first time you install the Operations Manager Database server, you'll be asked whether you would like to send Operations Manager Error Reports to Microsoft. You can choose automatic reporting in which case reports will be sent without prompting you. Alternatively, you can choose to be prompted for approval each time an error report is generated, which lets you review the information in a report before it is sent.

To turn Operations Manager Error Reporting on or off for the agents:

1. Start the Operations console, in the navigation pane select "Administration".
2. In the **Administration** workspace, under **Device Management**, select **Settings**.

3. In the **Settings** view, under **General**, right-click **Privacy** and choose **Properties** from the context menu.
4. Select the **Error Reporting** tab.
5. To turn Operations Manager Error Reporting off, click **Don't generate error reports**.

   To turn Operations Manager Error Reporting on and automatically send error reports, click **Automatically send error reports about this product to Microsoft without prompting the user (recommended)**.

   To turn Operations Manager Error Reporting on and queue error reports, click **Prompt the user for approval before sending error reports to Microsoft**.
6. Click **OK**.
7. In the navigation pane, under **Device Management**, click **Agent Managed**.
8. Select one or more agents in the middle result pane.
9. Right-click the agent and choose **Repair** in the context menu.
10. If your Management Servers Action Account does not have the right permissions on the agents, in the **Repair Agents** dialog box, choose the **Other user account** option, and type in the credentials of an account that has access to the agents.
11. Click **Repair**.
12. Click **Close** when completed.

To turn Operations Manager Error Reporting on or off for the management servers and gateway servers:

1. Log on to a server where the management server or gateway server is installed.
2. Click **Start**, and then click **Run**.
3. In the **Run** box, type **regedit** and click **OK**.
4. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HealthService\Parameters\.
5. Double-click the **Error Reports Enabled** DWORD value and set the value data **1** to turn on Error Reporting or **0** to turn off Error Reporting.

   Optionally, if you have enabled Error Reporting but would like to queue error reports before sending to Microsoft, you can edit the **Queue Error Reports** DWORD value and set the value data to **1** which will queue error reports to prompt for approval or **0** to directly send error reports to Microsoft.
6. Click **OK** when completed and the change will take effect

Important Information:

Error Reporting for Operations Manager Management Servers, Gateway Servers, and Agents cannot be configured using Group Policy.

Agentless Exception Monitoring (AEM) Error Forwarding

What This Feature Does:

Operations Manager can be configured to collect error reports generated due to application and operating system problems from all the computers in an enterprise running Windows operating systems and managed by Operations Manager. Additionally, Operations Manager can also be configured to forward the error reports to the Microsoft Error Reporting service.

Information Collected, Processed, or Transmitted:

The forwarded error reports to Microsoft can be either in Basic or Detailed format. In Basic format, the error report forwarded contains only the signature of the error used to uniquely identify an error without specific information about the environment in which it was generated. In Detailed format, the error report can consist of a detailed memory dump, registry settings, results of a Windows Management Instrumentation (WMI) query, and additional files along with the error signature from the computer on which the error report was generated.

Reports might unintentionally contain personal information, but this information is not used to identify or contact you or your organization. For example, a report that contains a snapshot of memory might include a name, part of a document the user was working on, or data the user recently submitted to a website.

Choice/Control:

This feature is off by default. During the process of configuring client monitoring, you can specify the policy for Error Forwarding to Microsoft.

1. Start the Operations console, in the navigation pane select **Administration**.
2. In the **Administration** workspace, under **Device Management**, select **Management Servers**.
3. In the **Management Servers** view, select any management server that has Client Monitoring Mode disabled, and right-click the management server.
4. Click **Configure Client Monitoring** to open the Configure Client Monitoring wizard.
5. On the **Error Forwarding** page, select **Forward all collected errors to Microsoft (Recommended)** to enable Error Forwarding to Microsoft.

   If you do not want to enable Error Forwarding to Microsoft, leave the option unselected.
6. After completing the wizard successfully, if you chose to enable Error Forwarding, a group policy template is created that can be used by an administrator with sufficient privileges to configure the managed computers in the enterprise to send error reports to the Management Server. Until the policy is active on the managed computers, these computers will not send error reports to the management server.

To enable or disable Error Forwarding after a management server has Client Monitoring Mode enabled:

1. Start the Operations console, in the navigation pane select **Administration**.
2. In the **Administration** workspace, under **Device Management**, select **Management Servers**.
3. In the **Management Servers** view, select any management server that has Client Monitoring Mode enabled, and right-click the management server.
4. Click **Properties**.
5. In **Properties**, click the **Error Forwarding** tab.
6. On the **Error Forwarding** page, select **Forward all collected errors to Microsoft (Recommended)** to enable Error Forwarding to Microsoft.

   If you do not want to enable Error Forwarding to Microsoft, leave the option unselected.
7. After clicking **OK**, Error Forwarding will be enabled if the option was selected in the previous step.

To selectively control the error reports forwarded to Microsoft after Client Monitoring mode has been enabled:

1. Start the Operations console, in the navigation pane select **Administration**.
2. In the **Administration** workspace, under **Settings**, double-click **Privacy**.
3. In **Properties**, select the **Error Transmission** tab.
4. On the **Error Transmission** tab, you can set the filter(s) to exclude error reports forwarded to Microsoft based on user name, computer name, application name, module, and application error type. Click **Filter** to set the exclusion filter criteria.
5. If you want to include additional diagnostic data requested by Microsoft from the managed computers in the error reports forwarded to Microsoft, you can select **Upload the diagnostic data collection requests**. If this diagnostic data should include files, registry settings, WMI queries and memory dumps, select the corresponding boxes on the tab.
6. After you click **OK** or **Apply**, the selected inclusion and exclusion policies defined in the steps above will be applied to all management servers that have Error Forwarding enabled.

To disable Error Forwarding and Client Monitoring mode:

1. Start the Operations console, in the navigation pane select **Administration**.
2. In the **Administration** workspace, under **Device Management**, select **Management Servers**.
3. In the **Management Servers** view, select any management server that has Client Monitoring Mode enabled, right-click the management server, and click **Disable Client Monitoring**.
4. Select **Yes** in the **Confirm Disable Client Monitoring** dialog box.

Please note that by disabling Error Forwarding in this manner, the management server will also stop forwarding centrally collected CEIP data to Microsoft. Managed computers may individually continue to send error reports and CEIP data if so configured.

In order to disable error forwarding from the managed computers, an administrator with sufficient privileges will have to undo the group policy that was applied during the process of configuring client monitoring.

For more information on how to further configure AEM, please review Client Monitoring Using Agentless Exception Monitoring in Operations Manager in the Operations Manager Operations Guide on TechNet.

Agentless Exception Monitoring CEIP Forwarding

What This Feature Does:

Operations Manager can be set up to forward Customer Experience Improvement Program reports collected from the computers managed by Operations Manager to Microsoft. These CEIP reports are forwarded as is without any modifications or filtering. For more information about CEIP, see the Microsoft Customer Experience Improvement Program.

Choice/Control:

This feature is off by default. When users run the Configure Client Monitoring Wizard they can configure whether they would like to collect CEIP reports and create a Group Policy template used to configure the managed computers.

During the process of configuring client monitoring, you can specify the policy for CEIP Forwarding:

1. Start the Operations console, in the navigation pane select **Administration**.
2. In the **Administration** workspace, under **Device Management**, select **Management Servers**.
3. In the **Management Servers** view, select any management server that has Client Monitoring Mode disabled, and right-click the management server.
4. Click **Configure Client Monitoring** to open the Configure Client Monitoring wizard.
5. On the **CEIP Forwarding** page, if you want to enable CEIP forwarding, for **Do you want to centrally collect CEIP data and forward to Microsoft?**, select **Yes, use the selected Management Server to collect and forward CEIP data to Microsoft**.

   If you do not want to enable CEIP forwarding to Microsoft, select **No, please continue to send data directly to Microsoft**.
6. After completing the wizard successfully, if you chose to enable CEIP Forwarding, a group policy template is created that can be used by an administrator with sufficient privileges to configure the managed computers in the enterprise to send CEIP data to the management server. Until the policy is active on the managed computers, these computers will not send CEIP data to the management server.

To disable CEIP Forwarding:

1. Start the Operations console, in the navigation pane select **Administration**.
2. In the **Administration** workspace, under **Device Management**, select **Management Servers**.
3. In the **Management Servers** view, select any management server that has Client Monitoring Mode enabled, right-click the management server, and click **Disable Client Monitoring**.

4. Select **Yes** in the **Confirm Disable Client Monitoring** dialog box.

Please note that by disabling CEIP Forwarding in this manner, the management server will also stop forwarding centrally collected error reports to Microsoft. Managed computers may individually continue to send CEIP data if so configured.

In order to disable CEIP Forwarding from the managed computers, an administrator with sufficient privileges will have to undo the group policy that was applied during the process of configuring Client Monitoring.

Microsoft Update

What This Feature Does:

Microsoft update is a service that provides Windows updates as well as updates for other Microsoft software, including Operations Manager. For details about what information is collected, how it is used, and how to change your settings, see the Update Services Privacy Statement at http://go.microsoft.com/fwlink/?linkid=50142.

Choice/Control:

If you are running any Operations Manager feature on a Windows server operating system, this feature is controlled by your Windows server settings. You can turn this feature on or off in **Windows Update** by clicking **Change settings**.

If you are running the Operations console or an Operations Manager agent on a Windows client operating system, see the Update Services Privacy Statement at http://go.microsoft.com/fwlink/?LinkID=115475 for details about controlling this feature.

Application Performance Monitoring (APM)

What This Feature Does:

Allows monitoring of ASP.NET applications, Windows Communications Foundation web services from server- and client-side perspectives, and Windows Services to get details about application availability and performance that can help pinpoint solutions. Allows administrators to specify settings, the types of events to collect, the performance goals to measure, and which servers to monitor. Operations Manager .NET Application Performance Monitoring provides insight into how .NET applications are running. Administrators can see how frequently a problem is occurring, how a server was performing when a problem occurred, and the chain of events related to the slow request or method that is unreliable. This is the information needed to partner with software developers and database administrators to help ensure that application availability and performance are at optimal levels. Application Performance Monitoring for server- and client-side perspectives might collect sensitive data and retain it in your database.

Sensitive data collection and retention:

- Application Performance Monitoring for server- and client-side perspectives might collect sensitive data and retain it in your database. Review your compliance policies before enabling application monitoring.
- Client-side monitoring might additionally collect, transmit, and retain information from Internet browsers. This information for public-facing Internet applications might be collected from countries and regions other than where your database is located.
- Enabling exception stack and global variables data collection sends page data to the monitored server. You should not collect exception stack and global variables for data-sensitive applications unless all pages are secured with https protocol.
- Application Monitoring Operators, system administrators, and potentially others with elevated permissions will have access to this data.
- No data is sent outside of the enterprise.

Choice/Control:

Client-side monitoring is disabled by default. Administrators should review their compliance policies before enabling application monitoring. For instructions on enabling client-side monitoring, see “Enabling Client-Side Monitoring” and “Client-Side Modifying Settings” in .NET Application Performance Monitoring Template

Integration with Team Foundation Server (TFS)

What This Feature Does:

This feature is implemented in the form of a management pack and synchronizes System Center 2012 - Operations Manager alerts and Team Foundation Server (TFS) work items. After importing this management pack, operators can assign alerts to the engineering team. Assigning an alert to engineering creates a new work item in TFS. The management pack workflow tracks and synchronizes changes made to TFS work items and changes made to associated Operations Manager alerts.

Sensitive data collection and retention:

- Although the feature does not retain data, it does make Operations Manager data visible throughout TFS and Visual Studio software. This data might include the sensitive data collected by Application Performance Monitoring (APM) and other data available in Operations Manager alerts. Review your compliance policies before enabling application monitoring.
- Similarly, data (such as work item assignment history and comments) in TFS work items is made visible to Operations Manager users.
- No data is sent outside of the enterprise.

Choice/Control:

The Team Foundation Server Work Item Synchronization management pack is optional to install. When the management pack is installed, you can configure whether to send all or only selected alerts to TFS manually or automatically.

Global Service Monitor (GSM)

What This Feature Does:

Allows monitoring of end-points of public-facing applications to get details about application availability, reliability and performance. Externally facing end-points can be, for example, web sites, web services, or ports. Monitoring can be performed from multiple geo-locations. GSM allows administrators to specify alert settings, the performance goals to measure, and which end-points to monitor. Global Service Monitor provides insights into how public-facing applications are running from the geo-distributed point of view. Administrators can see performance characteristics of each end-point (such as response time), whether response received is valid, and whether the end point is available externally. If there is a problem, administrators can see how frequently a problem is occurring, and from which geographical location the problem was observed. This is the information needed to partner with software developers and database administrators to help ensure that application availability and performance are at optimal levels. Global Service Monitor might collect sensitive data and retain it in your database.

Sensitive data collection and retention:

- Global Service Monitor might collect sensitive data and retain it in your database. Review your compliance policies before enabling application monitoring.
- Performance, reliability and availability information for public-facing Internet applications might be collected from countries and regions other than where your database is located.
- Enabling Global Service Monitor will collect the data about your application performance, availability and reliability. This data is stored temporarily on the servers in Microsoft datacenters, and eventually it is sent to the management servers in the enterprise.
- The data can contain sensitive information, such as web response, if your public-facing application is password protected and you choose to use authentication while running Global Service Monitor tests.
- Application Monitoring Operators, system administrators, and potentially others with elevated permissions will have access to this data.

Choice/Control:

Global Service Monitor is not installed by default. Administrators should review their compliance policies before installing Global Service Monitor and configuring the monitoring tests.

Release Notes for System Center 2012 - Operations Manager

These release notes apply to the appropriate version of Operations Manager in System Center 2012 and contain known issues that you might experience.

There are three versions of release notes:

1. Release Notes for System Center 2012 - Operations Manager
2. Release Notes for Operations Manager in System Center 2012 SP1
3. Release Notes for Operations Manager in System Center 2012 R2

Release Notes for Operations Manager in System Center 2012 R2

Before you install and use Operations Manager in System Center 2012 R2, read these release notes.

Advisor Monitoring Server group reserved for Advisor Connector use only

Description: The Microsoft System Center Advisor Monitoring Server group is reserved for the control of agents that are included into the Advisor Connector. This group should not be modified or added to the Advisor Managed list.

Workaround: This is by design.

.NET Framework required for enabling Advisor Connector on agents

Description: To enable the Advisor Connector on Operations Manager agent computers, Microsoft .NET Framework must first be installed.

Workaround: For agents running Windows Server 2008 R2 and earlier, install .Net Framework 3.5 SP1. For agents running Windows Server 2012 and newer, install .Net Framework 4.0 or higher.

ASP.NET Web API data producers not installed if Microsoft .NET Framework 4.x not installed first

Description: If you install an Operations Manager for System Center 2012 R2 agent on a computer that does not have Microsoft .NET Framework 4.x previously installed, some data

producers for the ASP.NET Web API will not be installed. If you later install the Microsoft .NET Framework 4.x on the computer and try to monitor an application that uses the ASP.NET Web API with the application monitoring feature, the applicable data producers will still be missing, and monitoring for that application will not work.

Workaround: This is by design. To restore the missing data producers, the agent should be re-installed after Microsoft .NET Framework 4.x has been installed on the computer.

You must import management packs in order to use Application Performance Monitoring with Windows Server 2012 R2

Description: You must import the Windows Server 2012 R2 and IIS 8 management packs in order to use Application Performance Monitoring (APM) with Windows Server 2012 R2.

Workaround: System Center 2012 R2 Operations Manager includes APM support for Windows Server 2012 R2 and IIS8 (Internet Information Services 8). However, In order for this feature to work you must import the following set of monitoring packs:

- Microsoft.Windows.Server.2012.R2.Discovery.mp
- Microsoft.Windows.Server.Library version 6.0.6989.0 or newer
- Microsoft.Windows.Server.2012.Discovery version 6.0.6989.0 or newer
- Microsoft.Windows.InternetInformationServices.CommonLibrary version 7.0.8862.0 or newer
- Microsoft.Windows.InternetInformationServices.2012 version 7.0.8862.0 or newer

  This is a new version of the IIS8 management pack. Do NOT use the Microsoft.Windows.InternetInformationServices.6.2 management pack, which was part of the "Windows 8 beta management pack release". Remove the Microsoft.Windows.InternetInformationServices.6.2 management pack if you had previously imported it.
- Microsoft.SystemCenter.Apm.Web.IIS8

  This is in the /ManagementPacks folder of the System Center 2012 – Operations Manager media, and is the equivalent of the Microsoft.SystemCenter.Apm.Web.IIS7 management pack which was previously (and still is) used for IIS7.

WCFServerAsyncBeginProducer cannot be found on agent after upgrade

Description: During upgrade from System Center 2012 to System Center 2012 R2, a new System Center 2012 R2 agent which is configured for APM monitoring will still receive OLD configuration settings from a management group which has not yet been upgraded, and might log an 'information' event (ID 1295) in the event log with the following message:

Cannot find producer "Microsoft.EnterpriseManagement.OperationsManager.Apm.Instrumentation.InstrumentationClas

s.WCFServerAsyncBeginProducer of assembly Microsoft.EnterpriseManagement.OperationsManager.Apm.Instrumentation, Version=7.0.5000.0, Culture=Neutral, PublicKeyToken=9396306c2be7fcc4, processorArchitecture=MSIL" in assembly Microsoft.EnterpriseManagement.OperationsManager.Apm.Instrumentation, Version=7.0.5000.0, Culture=Neutral, PublicKeyToken=9396306c2be7fcc4, processorArchitecture=MSIL, producer is inaccessible due to access level or producer has an incorrect signature. Please see documentation for details.

Workaround: None. This event is by design. Everything else in APM works normally, and this event message can be safely ignored.

After upgrade the web console does not work due to IIS becoming corrupt

Description: While upgrading to System Center 2012 R2, Operations Manager, if the upgrade breaks the web console, you can encounter a Runtime Error: **Server Error in '/OperationsManager' Application**. In the application log on the web console server, you will see an event with an exception message: **Could not load type 'System.ServiceModel.Activation.HttpModule'**.

For example, as part of the upgrade process you are prompted to add "HTTP Activation" to the role services of the Operating System. This leaves IIS in a semi-broken state, and requires a re-registration of ASP.NET in IIS to correct. This can occur anytime you add any IIS components after ASP.NET.

Workaround: Re-register ASP.NET in IIS.

- On Windows Server 2008 R2 SP1, run the following in an elevated CMD: `C:\Windows\Microsoft.NET\Framework64\v4.0.30319>aspnet_regiis.exe -i -enable`
- On Windows Server 2012, run the following in an elevated CMD: `C:\Windows\Microsoft.NET\Framework64\v4.0.30319>aspnet_regiis.exe -r`

Using sudo elevation with Solaris operating systems requires a configuration change if sudo executable is not in an expected path

Description: If you want to use sudo elevation on a computer running Solaris, and the sudo executable is not in an expected path, you need to create a link to the correct path. Operations Manager will look for the sudo executable in the path /opt/sfw/bin, and then in the path /usr/bin. If sudo is not installed in one of these paths, a link is required.

Workaround: The UNIX and Linux agent installation script creates the symbolic `link /etc/opt/microsoft/scx/conf/sudodir` to the folder expected to contain sudo. The agent uses this symbolic link to access sudo. The installation script automatically creates the symbolic link, so no action is needed for standard UNIX and Linux configurations. However, if sudo is installed in a non-standard location, you should change the symbolic link to point to the folder where sudo is

installed. If you change the symbolic link, its value is maintained for uninstall, re-install, and upgrade operations with the agent.

See Also

Release Notes for System Center 2012 - Operations Manager

Release Notes for Operations Manager in System Center 2012 SP1

Important
Before you install and use System Center 2012 Service Pack 1 (SP1), read these release notes about Operations Manager.

Critical and non-critical connectivity exceptions are both shown as “non-critical” for MVC applications

Description: When monitoring an ASP.NET MVC application with Application Performance Monitoring (.NET application performance monitoring), if the setting to monitor "All Exceptions" is selected (as opposed to only "Critical Exceptions"), all connectivity exceptions will report as "critical".

Workaround: Select only the "Critical Exception" option for monitoring for MVC applications, as opposed to "All Exceptions".

.NET Application Performance Monitoring will not work correctly when Operations Manager agents and management servers are on different Operations Manager release versions

Description: Discovery of WCF endpoints, monitoring of Windows Services and other Application Performance Monitoring (.NET application performance monitoring) related functionality is not supported across Operations Manager versions. For example, a 2012 SP1 agent reporting to a System Center 2012 – Operations Manager server (or vice versa, an System Center 2012 – Operations Manager agent reporting to a 2012 SP1 management group) will not work correctly.

Workaround: Install both agents and management servers with the same Operations Manager release.

No parameters are collected for RecordError when monitoring an ASP.NET MVC application

Description: When monitoring an ASP.NET MVC application with Application Performance Monitoring (.NET application performance monitoring), exception events do not have parameters collected.

Workaround: None. We are working on this to issue to be resolved in a future release.

You must import Windows 8 management packs in order to use Application Performance Monitoring with Windows Server 2012

Description: You must import the Windows Server 2012 and IIS 8 management packs in order to use APM (.NET application performance monitoring) with Windows Server 2012.

Workaround: System Center 2012 Service Pack 1 (SP1), Operations Manager includes APM support for Windows Server 2012 and IIS8 (Internet Information Services 8). However, In order for this feature to work you must import the following set of monitoring packs:

- Microsoft.Windows.Server.Library version 6.0.6989.0 or newer
- Microsoft.Windows.Server.2012.Discovery version 6.0.6989.0 or newer
- Microsoft.Windows.InternetInformationServices.CommonLibrary version 7.0.8862.0 or newer
- Microsoft.Windows.InternetInformationServices.2012 version 7.0.8862.0 or newer

  This is a new version of the IIS8 management pack. Do NOT use the Microsoft.Windows.InternetInformationServices.6.2 management pack, which was part of the "Windows 8 beta management pack release". Remove the Microsoft.Windows.InternetInformationServices.6.2 management pack if you had previously imported it.
- Microsoft.SystemCenter.Apm.Web.IIS8

  This is in the /ManagementPacks folder of the System Center 2012 – Operations Manager media, and is the equivalent of the Microsoft.SystemCenter.Apm.Web.IIS7 management pack which was previously (and still is) used for IIS7.

WCFServerAsyncBeginProducer cannot be found on agent after upgrade

Description: During some changes made to the agent for Beta, we removed a class from the code.Result: During upgrade, a new SP1 agent which is configured for APM monitoring will still receive OLD configuration settings from a management group which has not yet been upgraded, and might log an 'information' event (ID 1295) in the event log with the following message:

Cannot find producer "Microsoft.EnterpriseManagement.OperationsManager.Apm.Instrumentation.InstrumentationClas

s.WCFServerAsyncBeginProducer of assembly Microsoft.EnterpriseManagement.OperationsManager.Apm.Instrumentation, Version=7.0.5000.0, Culture=Neutral, PublicKeyToken=9396306c2be7fcc4, processorArchitecture=MSIL" in assembly Microsoft.EnterpriseManagement.OperationsManager.Apm.Instrumentation, Version=7.0.5000.0, Culture=Neutral, PublicKeyToken=9396306c2be7fcc4, processorArchitecture=MSIL, producer is inaccessible due to access level or producer has an incorrect signature. Please see documentation for details.

Workaround: None. This event is by design. Everything else in APM works normally, and this event message can be safely ignored.

Web Recorder functionality does not work with IE10 on Windows 8

Description: Web Recorder functionality does not work with Internet Explorer 10 on Windows 8.

Workaround: None.

The Network Summary Dashboard cannot load data on the OM12SP1 UI when connecting to an OM12 Management Group

Description: When using the Network Summary Dashboard in System Center 2012 Service Pack 1 (SP1), Operations Manager, customers cannot load data when connecting to a System Center 2012 – Operations Manager management group.

Workaround: Use the System Center 2012 – Operations Manager User Interface to connect to a System Center 2012 – Operations Manager management group, or upgrade the management group to SP1.

On upgrade from a licensed install customers will see an Evaluation EULA even though product is licensed

Description: During upgrade from a licensed installation of Operations Manager, customers will see an Evaluation EULA even though product is licensed.

Workaround: Run `Get-ScomLicense` in PowerShell to see the actual license agreement.

File names for the Data Warehouse database and log are .mdf and .ldf

Description: The file name for the Operations Manager Data Warehouse SQL Database is always ".mdf", and the log file name ".ldf" instead of the database name.

Workaround: Use the SQL process to rename the files to match the database name. See How to consolidate physical files and rename the logical file name in SQL Server 2000 and in SQL Server 2005.

The Microsoft System Center Application Monitoring 360 SLA Management Pack is not imported by default during setup

Description: The applications dashboard under Monitoring\Application Monitoring in the Monitoring section of the Operations Manager console contains a section for Service Level Agreements (SLAs). By default, this section is empty for any application. There is a management pack containing default SLAs for these applications on the SP1 CD that you can import, that will make the SLAs appear. You can also create and modify your own SLAs for the applications.

Workaround: There are two processes to populate SLAs in the applications dashboard:

1. Create your own SLAs for the applications. For more information, see How to Configure 360 .NET Application Monitoring Dashboards in System Center 2012 SP1.
2. Import the "Microsoft System Center Application Monitoring 360 SLA" management pack, **Microsoft.SystemCenter.ApplicationMonitoring.360.SLA.XML**, from the SP1 media, which contains default SLAs.

Do not install a System Center 2012 SP1, Operations Manager Management Group pointing to a System Center 2012 Data Warehouse

Description: Do not install a System Center 2012 Service Pack 1 (SP1), Operations Manager versioned management group pointing to a System Center 2012 – Operations Manager versioned data warehouse. The data warehouse will not function.

Workaround: None. Ensure both the management group and the data warehouse pointed to are running the SP1 version of System Center 2012 – Operations Manager.

After upgrade to SP1 the web console does not work due to IIS becoming corrupt

Description: While upgrading to System Center 2012 Service Pack 1 (SP1), Operations Manager, if the upgrade breaks the web console, you can encounter a Runtime Error: **Server Error in '/OperationsManager' Application**. In the application log on the web console server, you will see an event with an exception message: **Could not load type 'System.ServiceModel.Activation.HttpModule'**.

For example, as part of the upgrade process you are prompted to add "HTTP Activation" to the role services of the Operating System. This leaves IIS in a semi-broken state, and requires a re-

registration of ASP.NET in IIS to correct. This can occur anytime you add any IIS components after ASP.NET.

Workaround: Re-register ASP.NET in IIS.

- On Windows Server 2008 R2 SP1, run the following in an elevated CMD: `C:\Windows\Microsoft.NET\Framework64\v4.0.30319>aspnet_regiis.exe -i -enable`
- On Windows Server 2012, run the following in an elevated CMD: `C:\Windows\Microsoft.NET\Framework64\v4.0.30319>aspnet_regiis.exe -r`

Using sudo elevation with Solaris operating systems requires a configuration change if sudo executable is not in an expected path

Description: If you want to use sudo elevation on a computer running Solaris, and the sudo executable is not in an expected path, you need to create a link to the correct path. Operations Manager will look for the sudo executable in the path /opt/sfw/bin, and then in the path /usr/bin. If sudo is not installed in one of these paths, a link is required.

Workaround: The UNIX and Linux agent installation script creates the symbolic link `/etc/opt/microsoft/scx/conf/sudodir` to the folder expected to contain sudo. The agent uses this symbolic link to access sudo. The installation script automatically creates the symbolic link, so no action is needed for standard UNIX and Linux configurations. However, if sudo is installed in a non-standard location, you should change the symbolic link to point to the folder where sudo is installed. If you change the symbolic link, its value is maintained for uninstall, re-install, and upgrade operations with the agent.

Release Notes for System Center 2012 - Operations Manager

These release notes apply to System Center 2012 – Operations Manager and contain known issues that you might experience.

The release notes contain the following sections:

- Installation
- Management Servers
- Dashboard Views
- Network Monitoring
- UNIX and Linux
- Alerts
- Operations
- Performance

- Management Packs
- Application Performance Monitoring
- Management Pack Authoring
- Product Connectors

Installation

You might see the following issues when you install Operations Manager.

Cannot install using an existing database

Description: In Operations Manager, you can only install the first management server in a management group by using the option to create a new database, or install subsequent management servers to a management group by using an existing database. The option to install by using an existing empty operational database is not available for Operations Manager.

Workaround: There is no workaround.

Leading spaces in the installation folder path are removed

Description: In Setup, when you designate the installation directory on the "Installation Location" page, if a folder has any leading spaces, the spaces will be removed. For example, "D:\ Test" will be changed to "D:\Test".

Workaround: There is no workaround.

Unicode characters in domain or computer name are not supported

Description: Installation of Operations Manager fails if the domain name or computer name contains Unicode characters. The event log for the installation will not contain an error message that explicitly states that the failure was due to Unicode characters.

Workaround: There is no workaround.

Install hotfix before installing the Operations console

Description: Before you install the Operations console, install the hotfix from article 976898 (http://go.microsoft.com/fwlink/?LinkID=194637) in the Microsoft Knowledge Base. You have to contact Microsoft Customer Support Services to request the hotfix download. This hotfix helps prevent performance problems with the Operations console. After you install the hotfix, you must restart the computer.

This hotfix might not be required for all servers. The Operations console prerequisite checker checks for this prerequisite and alerts the user if it is not there. The hotfix has to be installed if the prerequisite checker finds that the hotfix is missing.

Uninstall might result in unhandled exceptions in log

Description: When you uninstall Operations Manager, some exceptions might be logged in the OpsMgrSetupWizard.log file. These exceptions do not affect the functionality of uninstalling the program. You can ignore them.

Workaround: There is no workaround.

Server-side tracing on a Web console server might require additional installation steps

Description: Web console server side tracing cannot be performed on a Web console server without the Operations Manager agent or Operations console installed.

Workaround: Either install the Operations Manager agent or Operations console on the Web console server.

Installing Web console might cause ASP.NET or internal server errors

Description: After you install the Web console, you might experience ASP.NET or internal server (50x.x) errors, such as HTTP Error 500.19.

Workaround: Perform the following steps.

1. At an elevated command prompt, reregister Internet Information Services (IIS) to use ASP.NET 4.0 by running the following command:

   %WINDIR%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -r
2. Change the Webconsole IIS Application pool “OperationsManagerMonitoringView” ASP.NET framework integration from ASP.NET 4.0 to ASP.NET 2.0.
3. Run IISreset.

Web console can fail to open

Description: After you install the Web console, the console fails to open and you see the following error message:

```
Could not write to output file 'c:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\operationsmanager\857ec549\f35afedc\App_global.asax.tyqhcqzi.dll'
```

Workaround: Change the Identity of the OperationsManager application pool to run as LocalSystem by performing the following steps:

1. Open IIS Manager.
2. In the **Connections** pane, expand the server node and click **Application Pools**.
3. On the **Application Pools** page, select the OperationsManager application pool, and then click **Advanced Settings** in the **Actions** pane.
4. For the **Identity** property, click the **...** button to open the **Application Pool Identity** dialog box.
5. Select **LocalSystem** in the **Built-in account** menu.

6. Click **OK**.

.NET Framework 4 is required on gateway servers to support network monitoring

Description: In Operations Manager, if you are using the networking monitoring feature in a management group where the devices being managed are behind gateway servers, these gateway servers must have .NET Framework 4 installed. The prerequisite checker does not check for .NET Framework 4 when you install a gateway server. If .NET Framework 4 is not installed, certain workflows such as network discovery will fail. The event log will only show that workflows have failed and been unloaded, but will not indicate that .NET Framework 4 is required.

Workaround: Install .NET Framework 4 on gateway servers. You can download the .NET Framework 4 redistributable package at http://go.microsoft.com/fwlink/?LinkId=201924.

Specifying an action account during agent upgrade can cause the agent to stop communicating

Description: If you specify an action account during the upgrade process for the agent, the agent can stop communicating with its management server, and the agent will appear in an unmonitored (gray) state in the Operations console. The following events will be logged on the computer that is running the agent.

- 7022 - The Health Service has downloaded secure configuration for management group Management Group 1, and processing the configuration failed with error code 0x80FF003F(0x80FF003F)
- 20070 - The OpsMgr Connector connected to ManagementServer1, but the connection was closed immediately after authentication occurred. The most likely cause of this error is that the agent is not authorized to communicate with the server, or the server has not received configuration. Check the event log on the server for the presence of 20000 events, indicating that agents which are not approved are attempting to connect.

Workaround: In the Operations console, in the **Administration** workspace, expand **Run As Configuration**, expand **Accounts**, right-click **Local System Action Account**, and then click **Properties**. In the **Properties** dialog box, on the **Credentials** tab, re-enter the password to the action account. Next, restart the Health service to restore communication to the management server.

If the upgrade of an agent fails, it may not rollback to the previous configuration

Description: If you are upgrading an agent from Operations Manager 2007 to System Center 2012 – Operations Manager and that upgrade process fails, the agent may be removed completely. This is because the upgrade process has moved beyond the point where a rollback is possible.

Workaround: Reinstall the agent.

Installation fails if the model database in SQL is larger than the size of the database being created

Description: SQL Server has a model database that is used as a template for creating new databases. If the size of this database is larger than the initial size that you specify for either the operational or data warehouse databases, then installation will fail.

Workaround: Specify a database size larger than the size of the model database.

You will be opted out of the Customer Experience Improvement Program if you upgrade to Operations Manager

Description: If you opted into the Customer Experience Improvement Program in Operations Manager 2007 R2 and then upgrade to System Center 2012 – Operations Manager, you will be automatically opted out.

Workaround Option 1: Perform the upgrade using the command line with the /SendCEIPReports:1 option. This will opt into the CEIP regardless of the previous setting.

Workaround Option 2: After the upgrade is completed, reset the CEIP settings to opt-in. The steps on how to perform this are in the privacy statement.

Management Servers

You might see the following issues related to management servers in Operations Manager .

Instances can take a few minutes to load after a management server failover

Description: When the management server workloads are transferred to another management server on a failover, there is an intentional delay of one minute for the configuration manager to reload managed instances. This can result in managed objects being inactive for one to two minutes after the failover occurs.

Workaround: There is no workaround.

A management server may experience an error if it runs out of ESE storage

Description: If a management server runs out of Extensible Storage Engine (ESE) storage, it will create an error event in the **Operations Manager** event log with an ID of 623. This will leave the Health Service on the management server in an unworkable state.

Workaround:

1. Stop the service **System Center Management Health Service**.
2. Delete the health state directory and its contents. By default this is **C:\Program Files\System Center Operations Manager 2012\Server\Health Service State**. The path is stored in

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\HealthService\Parameters\State Directory.

3. Start the service **System Center Management Health Service**.

Dashboard Views

You might see the following dashboard issues when you use Operations Manager.

Find and Scope do not work in dashboard views

Description: In new dashboard views, **Find** and **Scope** on the toolbar do not work.

Workaround: There is no workaround.

Must change views to refresh network and application monitoring dashboard views

Description: To refresh the information displayed in the network or application monitoring dashboard views, you must navigate to another view and then navigate back to the network or application monitoring dashboard view. The **Refresh** task on the **View** menu and **F5** do not work. If the dashboard view opens in a separate window, such as the Network Node dashboard view or the Network Vicinity dashboard view, you must close the window and then reopen it to refresh the information.

Workaround: There is no workaround.

Must restart console after importing a management pack that contains a binary for dashboards

Description: When you import a management pack mpb file, you must restart the Operations console before you can view the new dashboard view.

Note

This does not apply to new dashboard views for Operations Manager which are installed during setup, nor to new management packs that use installed components. It only applies to .mpb files that install new or updated visual components.

Workaround: After you import a new version of a management pack that contains a binary used for dashboards, restart the Operations console.

Agent State view in Administration workspace is not available

Description: If you right-click an agent in the Agent Managed node in the Administration workspace and select to open a state view, the view will fail to open.

Workaround: In the Monitoring workspace, use the Agent Details views or create a custom state view.

Changing a 1-column dashboard view from grid layout to flow layout results in an empty dashboard view

Description: When you create a 1-column dashboard view by using the following steps, the dashboard view will display as a blank screen, with no option to add a widget.

1. In the Monitoring workspace, right-click in the navigation tree, point to **New**, and then click **Dashboard View**.
2. On the **Template** page, click **Grid Layout**, and then click **Next**.
3. On the **General Properties** page, enter a name for the dashboard view.
4. Click **Previous**.
5. On the **Template** page, click **Flow Layout** and then click **Next**.
6. On the **General Properties** page, click **Next**.
7. On the **Select Layout** page, leave the Column Count value as “1” and click **Next**.
8. On the **Summary** page, click **Create**.
9. On the **Completion** page, click **Close**.

Workaround: To correct the empty dashboard view, perform the following steps.

1. In the dashboard view, click the **Configure** button in the top right corner.
2. Click **Next** to open the **Select Layout** page.
3. In the **Column Count** field, overwrite the existing value “1” with “1”.
4. Click **Finish**.

User may not be able to use dashboards in My Workspace if they have a User Role with limited Group Scope

Description: If a user has a User Role that does not include all groups in the Group Scope, then the user will not be able to view, create, save, or delete dashboards in the My Workspace pane. This is a known issue in Operations Manager 2012.

Workaround: There is no workaround.

User with limited Group Scope may not be able to make personalization changes to widgets and dashboards

Description: If a user has a User Role that does not include all groups in the Group Scope, then the user may not be able to make personalization changes to dashboards and widgets, even if they are within the user’s scope. This is a known issue in Operations Manager.

Workaround: Have a user with administrative role make the required changes.

Author may not see a dashboard they create in the Monitoring pane

Description: If a user with an Author user profile creates a dashboard in the Monitoring pane, they will not see it until an Administrator updates the user role, even if the user role has been

configured for all dashboards. This is because the dashboard is not automatically added to the scope of the profile when it is created. This is a known issue with Operations Manager.

Workaround: An Administrator must edit the user profile and provide access to the new dashboard.

Configuration changes to existing views may be unpredictable

Description: Changes that you make to custom views may not work properly. This is due to a known bug in Operations Manager.

Workaround: Restart the Operations console and attempt the configuration change again. If this is unsuccessful, delete the view and create it again.

Operations console may crash if you scroll a view with a table to the right

Description: When you scroll a view with a table, such as an alert view or state view, to the right, the Operations console may crash. This is due to a known problem in Windows Presentation Foundation.

Workaround: Install hotfix described in http://support.microsoft.com/kb/2484832.

Management Group Health dashboard may temporarily calculate unavailable agents incorrectly

Description: When an agent is first discovered, there is a short interval when it may not have a health service watcher. If the agent is registered as **not monitored** and does not yet have a health service watcher when the **Management Group Health** dashboard does its calculation, the agent will incorrectly be counted as **unavailable**.

Workaround: This issue is temporary, and will automatically correct itself, once the health service watcher is discovered.

Personalization settings for Dashboard Widgets will be lost when upgrading to Operations Manager Release Candidate

Description: If you are upgrading from Operations Manager Beta to Operations Manager Release Candidate, you will lose any personalization settings on dashboard widgets.

Workaround: There is no workaround for this issue, you must manually recreate the settings.

Can’t create a dashboard in the web console if the Web Console is installed on a localized operating system

Description: You can create dashboards and add widgets to it using the web console. This is not supported in the Operations Manager though if the web console is installed on a localized version

of Windows Server. This feature works if the web console is installed on the US-EN version of Windows Server.

Workaround: Use the Operations console to create the dashboards.

The Objects by Performance widget will display no data if (All) instance is used

Description: The Objects by Performance widget displays the top specified number of objects sorted by a particular performance counter. This widget will display no data if you use (All) for the Instance.

Workaround: Select a specific instance instead of selecting (All).

A Read-Only Operator may not be able to open a diagram view

Description: When a Read-Only Operator attempts to open a diagram view in the Web Console, they may receive an error saying that they do not have sufficient privileges. They may get this error even though they have appropriate permissions to the view. This problem is caused by permissions on a temp folder that are configured incorrectly.

Workaround: To correct the problem, perform the following steps on the server running in the web console.

1. Open Windows Explorer and navigate to **C:\Program Files\System Center 2012\Operations Manager\WebConsole\MonitoringView** .
2. Right-click the **TempImages** folder and select **Properties**.
3. Select the **Security** tab and click **Advanced**.
4. Click **Change Permissions**.
5. Select **Include inheritable permissions from this object's parent.**
6. In the **Permissions entries** box, select the entry for **SYSTEM** and click **Remove**.
7. In the **Permissions entries** box, select the entry for **Administrators** and click **Remove**.
8. Click **OK** for each open dialog box.

Operations Manager dashboards hosted in SharePoint may not display properly if the web console requires HTTPS

Description: If the Operations Manager web console was installed with the option to require SSL, dashboards hosted in SharePoint may not display properly. This is an unsupported scenario in System Center 2012 - Operations Manager RTM.

Workaround: Change the configuration of the OperationsManager web site hosting the web console to not require SSL.

Network Monitoring

You might see the following issues when you use Operations Manager for network monitoring.

SNMP Traps do not work if the SNMP Trap service is running on the agent computer

Description: If the Windows SNMP Trap service is running on an agent computer, that agent cannot receive SNMP traps from network devices. Ensure that this service is not running on any agent that is receiving SNMP traps that should be analyzed by Operations Manager.

Workaround: There is no workaround.

Deleting a large number of devices can take a long time

Description: Deleting more than 20 devices at one time can take considerably longer to run.

Workaround: We recommend that you delete network devices in batches no larger than 20 at a time to get the best performance.

Only one effective Run As account can be used for a network device

Description: If the same network device is discovered by two or more management servers that are using different Run As accounts, only the first account is used to manage the device. If this account was not distributed to the other management servers, they will log errors about being unable to resolve the account.

Workaround: There is no workaround.

Gateway Pool topology does not work for network topologies at scale

Description: If you use a gateway pool to monitor a large number of network devices, there will be high latency of performance counters and health state changes. This is due to a known performance impact from the method used to deliver data to the pool in Operations Manager.

Workaround: Reduce the number of network devices being monitored.

UNIX and Linux

You might see the following issues related to UNIX and Linux computers in Operations Manager .

Using sudo elevation with Solaris operating systems requires a configuration change if sudo executable is not in an expected path

Description: If you want to use sudo elevation on a computer running Solaris, and the sudo executable is not in an expected path, you need to create a link to the correct path. Operations Manager will look for the sudo executable in the path /opt/sfw/bin, and then in the path /usr/bin. If sudo is not installed in one of these paths, a link is required.

Workaround: The UNIX and Linux agent installation script creates the symbolic link `/etc/opt/microsoft/scx/conf/sudodir` to the folder expected to contain sudo. The agent uses this symbolic link to access sudo. The installation script automatically creates the symbolic link, so no action is needed for standard UNIX and Linux configurations. However, if sudo is installed in a non-standard location, you should change the symbolic link to point to the folder where sudo is installed. If you change the symbolic link, its value is maintained for uninstall, re-install, and upgrade operations with the agent.

Alerts

You might see the following issues related to alerts in Operations Manager .

All Management Servers Resource Pool Unavailable alert remains active

Description: The All Management Servers Resource Pool Unavailable alert can remain active after all management servers have recovered from an unavailable state. This can occur when more than one management server in the server pool reports as unavailable within the same second, which generates multiple alerts. When the availability issue is resolved, only one alert is resolved.

Workaround: Verify that all management servers have network connectivity, are not in maintenance mode, and that the Health service is generating a heartbeat, and then resolve the alert manually in the Operations console. Do not resolve the alert manually if the majority of management servers are unavailable.

Product knowledge for alerts incorrect or missing

Some alerts in Operations Manager have incorrect or missing product knowledge. Refer to the following product knowledge articles for the following alerts:

- **Resource Pool Heartbeat Failure Alert**

Resource Pool Heartbeat Failure Alert

Alert Name: Health Service Heartbeat Failure

Alert Description: The Health Service on <mgmt server name> failed to heartbeat.

Summary

The Health Service has stopped on a computer.

This alert is generated by the System Center Data Access Service on the agent's management server when it has determined one of the members of the resource pool has not sent a heartbeat. The purpose of this alert is to inform the administrator that the host computer is unhealthy and will not perform monitoring as expected.

Error Alert: The System Center Data Access Service has failed multiple consecutive times to determine the availability of the server.

Causes

The following conditions can cause this alert:

- The agent computer is not running.
- The agent computer has lost network connection.
- The Health service on the agent computer is placed into Maintenance Mode.
- The Health service on the agent computer has been set to Manual/Disabled and the computer was restarted.
- The Health service on the agent computer failed to start correctly.
- The Health service on the agent computer has been stopped.

Resolutions

You can enable a recovery to automatically restart the agent if it fails.

In the event that the recovery is disabled or was not successful, you can navigate to the **State Change Events** tab and run the recovery from the details pane. To open the **State Change Events** tab, right-click the alert, select **Open**, and then click **Health Explorer**. In the Health Explorer, select the alert that is in a critical state, and then in the right-hand pane, click the **State Change Events** tab. In the details pane, click the recovery task to run the recovery.

Note

A diagnostic task for this monitor runs ping to determine if the computer can be contacted from the management server. The default firewall settings for computers running Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 prevent the computers from providing a ping response. To configure these computers to allow incoming ICMP traffic, see "Create an Inbound ICMP Rule on Windows 7, Windows Vista, Windows Server 2008, or Windows Server 2008 R2" (http://go.microsoft.com/fwlink/?LinkId=161045).

Additional Information

The below table explains the reason codes in the alert description:

Reason Code	Description
17	The Health Service is paused.
25	The Health Service Action Account is configured incorrectly or has invalid credentials.
41	The Health Service failed to parse the new configuration.
42	The Health Service failed to load the new configuration.
43	A System Rule failed to load.
49	Collection of Object State Change Events is

Reason Code	Description
	stalled.
50	Collection of Monitor State Change Events is stalled.
51	Collection of Alerts is stalled.
97	The Health Service is unable to register with the Event Log Service. The Health Service cannot log additional Heartbeat and Connector events.
98	The Health Service is unable to parse configuration XML.

Alert resolution state can be incorrect in Operations console

When you select multiple alerts and then resolve the alerts by using Alert Status in the Properties dialog box, the resolution state for each alert will be updated in the operational database but might not update correctly in the Operations console. The resolution state for all alerts will update in the Operations console when you navigate to another view and then return to the alert view or when a new alert is generated.

Workaround: Navigate to another view and then return to the alert view to update alert resolution state.

Operations

You might see the following issues when you use Operations Manager.

Operations console might have a memory leak

Description: The Operations console might experience a memory leak over a period of time. This issue will be fixed in a future release of Operations Manager.

If the Operations console appears to be running slowly, perform the following steps to determine if a memory leak is the cause:

1. Open Task Manager.
2. Locate the console process Microsoft.EnterpriseManagement.Monitoring.Console.exe.
3. Inspect the memory (Private Working Set) is using.

   If the console memory usage is higher than 700 MB, there is a memory leak.

Workaround: Close the console and then reopen the console.

My Subscriber Information and My Subscriptions not working

Description: When you open the Operations console in a role other than administrator, **My Subscriber Information** and **My Subscriptions** options are available in the **Tools** menu, but do not work.

Workaround: There is no workaround.

Print Preview does not work in diagram views

Description: Print Preview does not work in diagram views. If you try to open **Print Preview**, the Operations console crashes.

Workaround: There is no workaround.

Cannot create a new channel from the Tasks menu on the toolbar

Description: In the Operations console, in the **Administration** workspace, the **New Channel** task on the **Tasks** menu of the toolbar does not work.

Workaround: To create a new channel, in the navigation pane, right-click **Channels** point to **New channel**, and then click the type of channel that you want to create.

Time filter does not work for event views

Description: In an event view, the **Show at least** time filter does not work.

Workaround: There is no workaround.

Order of sections in Tasks pane might change

Description: In the Operations console, the order of the sections in the **Tasks** pane might change when you open a view.

Workaround: There is no workaround.

Override options on toolbar are unavailable

Description: In the **Active Alerts** view, the options on the **Override** menu on the toolbar are unavailable.

Workaround: Select an alert, right-click, and point to **Overrides**. The **Disable** and **Override** options are available on this menu.

Additional elements visible in views

Description: If you create a state view showing all types of entities, some additional elements are visible with names starting such as "<Identifier Schema=...", which will appear as "Not Monitored".

Workaround: Create views targeted to specific types or limited to specific groups, rather than an entity. If you create a view showing all entities, these entities may be ignored.

Workflows might crash on Itanium-based systems

Description: Workflows that use managed modules such as Windows PowerShell and Windows Workflow Foundation (WF) might crash when running on monitored Itanium-based systems.

Workaround: If the workflow was started manually, such as running a task, rerun the workflow. Scheduled workflows are likely to succeed the next time that they are scheduled to run.

Cannot change target for Discovered Inventory

Description: In Operations Manager, the Change Target Type task in the **State Actions** section of the **Tasks** pane does not work for the Discovered Inventory view.

Workaround: There is no workaround.

Do not close Operations console when a secondary console windows is open

Description: Health Explorer and some dashboard views open a secondary console window. If you close the Operations console when the secondary console window is open, the secondary console window loses navigation functionality and might crash.

Workaround: Close all instances of the console and start over.

The Online parameter for the Get-Help cmdlet directs you to Operations Manager TechCenter

Description: In the Operations Manager , when you use the *Online* parameter with the **Get-Help** cmdlet for cmdlets included in the new Windows PowerShell v2 module, the Operations Manager TechCenter is displayed, rather than Help content specific to the cmdlet.

Workaround: Workaround: There is no workaround.

Properties for Run As account can be slow to open

Description: When you open Properties for a Run As account, it may take several minutes for the Properties dialog box to open if the credentials for the Run As account have been distributed to more than 1000 computers.

Workaround: There is no workaround.

Some tasks might have inconsistent or inaccurate results

Description: If you run a task that targets a hosted entity that is managed by a resource pool, the task might generate inconsistent or inaccurate results. This is due to a change in how task

workflows are handled with the addition of resource pools to the Operations Manager infrastructure.

Workaround: There is no workaround.

Azure application may not work properly on an agent reporting to both management groups with different Operations Manager versions

Description: If an agent is configured in both an Operations Manager 2007 R2 and Operations Manager management group, and that agent is used as the proxy for monitoring an application with the Windows Azure Application Monitoring Management Pack, the application monitoring may not work properly.

Submenu does not appear in web console context menu

Description: If you have Silverlight 5 installed, when you right click an item in a view in the web console, the context menu is displayed but submenus are not. There is no workaround for this issue in Operations Manager.

Workaround: There is no workaround.

Nodes in the Monitoring pane in both the Operations and web console may be duplicated

Description: Certain folder nodes in the Monitoring pane in both the Operations console and web console may be duplicated. This is a known issue in Operations Manager.

Workaround: There is no workaround required since both nodes are functional.

Help file may open to error page

Description: In some wizards and dialog boxes, when you click a Help link or press F1, the Help file may open with an error page that states "This program cannot display the webpage". These links will be fixed in the next release.

Workaround: In the Help file, use the Contents tab or Search tab to locate the documentation you need.

Performance

You may experience degraded performance under the following conditions.

Opening a state view with many objects

Description: It may take a long time to open a state view in the web console that lists thousands of objects.

Workaround: Workaround: Create a dashboard with a single state widget targeting the same object type but using a filter to only include objects with a particular health state. You can also modify a user role to limit the scope of objects that are included in the state view.

Opening the health explorer for an object containing many other objects

Description: It may take a long time to open the health explorer for an object with a deep monitoring hierarchy. This includes a group that contains many other objects that themselves contain other objects.

Workaround: Open the health explorer for an object lower in the monitoring hierarchy.

Opening a performance view that includes many objects each with many performance counters

Description: It may take a long time to open a performance view that includes many objects with each of those objects containing many performance counters.

Workaround: Open the performance view for a single object.

Operations Manager 2007 R2 command shell may have performance problems

Description: When you use the Operations Manager 2007 R2 command shell or type or script certain commands that make use of the provider, you might experience slow performance. This is due to changes to the underlying instance space and SDK which allow many more instances in the database. The Operations Manager 2007 R2 command shell was not designed to deal with this many instances.

Workaround: Use the Operations Manager command shell.

Management Packs

You might see the following issues related to Management Packs when you use System Center 2012 – Operations Manager.

Some third party management packs may not work in Operations Manager

Description: Most existing management packs written for Operations Manager 2007 SP1 or Operations Manager 2007 R2 are compatible with System Center 2012 – Operations Manager. If a management pack has any of the following features, it may not work properly in System Center 2012 – Operations Manager.

- Management packs that require new modules on the agent, management pack templates, or new view types. The APIs for Operations Manager have changed which may break these features.
- Management packs that attempt to create or update other management packs or management pack elements.
- Management packs that leverage SNMP modules and SNMP network devices discovered by Operations Manager 2007. These management packs will continue to work after an upgrade, but they will be unable to target network devices discovered through the Operations Manager discovery wizard.

Workaround: You should report any incompatibilities that you identify to the vendor of the management pack so that they can make appropriate corrections. You should also report the issue to the Feedback Center on Microsoft Connect (https://connect.microsoft.com/OpsMgr/Feedback)

SharePoint 2010 Management Pack configuration task fails in Operations Manager

Description: The task in the SharePoint 2010 MP to configure the SharePoint servers to be monitored fails in Operations Manager. The task runs a Windows PowerShell script that is leveraging SDK calls that are not supported in Operations Manager. This occurs in both new and upgraded installations. If the task is run in Operations Manager 2007 R2 before upgrading to System Center 2012 – Operations Manager, the SharePoint Servers will continue to be monitored. This issue only occurs if the servers to be monitored are changed or configured for the first time.

Workaround: Import the SharePoint Management Pack from Connect and run the **Configure SharePoint Management Pack (SCOM 2012)** task.

Microsoft Exchange 2007 Template management pack will not install from catalog

Description: An error message will be displayed if the Microsoft Exchange 2007 Template management pack is installed from the catalog in Operations Manager.

Workaround: Download the management pack to disk and then import into the management group.

Cannot export and then import a management pack that contains resources

Description: If you use the Operations console to export a management pack which contains resources such as icons, the management pack cannot be subsequently imported in Operations Manager .

Workaround: There is no workaround.

Application Performance Monitoring

You might see the following issues related to Application Performance Monitoring when you use System Center 2012 – Operations Manager.

Links in Application Monitoring events in alert descriptions may not work

Description: If you are using a dashboard that includes an alert widget and you view an alert raised by APM, you will not be able to use the link embedded in the alert description to launch the APM event details in Application Diagnostics.

Workaround: Open the alert in an alert view.

Workaround: Install the web console in the management group.

You may receive an alert after configuring client-side monitoring for the first time

Description: After you configure client-side monitoring on a server for the first time, you may receive an event with ID 1108 saying that an account specified in the Run As profile Microsoft.SystemCenter.Apm.Csm.EncryptionProfile cannot be resolved. This will create an alert in Operations Manager that does not automatically resolve.

This event occurs because the rules used to collect data for client-side monitoring may start running before the Run As account is sent to the health service. The Run As account will be downloaded, at which point client-side monitoring will be fully functional.

Workaround: There is no workaround required. You can safely ignore the event and resolve the alert.

Microsoft.EnterpriseManagement.Modules.Apm.WebLibraryConfigManager may fail to load after upgrade

Description: After upgrading to Operations Manager you may see a series of error events with ID 4508 and 4509 in the event log on agent managed computers. This is because some of the assemblies required by the APM modules have either not yet been downloaded through dependency download or are not being loaded due to a problem with the health service cache.

Workaround: Restart the health service on the agent to clear the cache and ensure that the proper assemblies are loaded.

.NET Application Performance Monitoring templates created in Beta will not work in RTM

Description: If you used the .NET Application Performance Monitoring template in the Beta version of Operations Manager to monitor applications, those templates need to be deleted and

recreated in the release version of Operations Manager. Any templates created in the Release Candidate will work in RTM.

Workaround: Delete and recreate the templates.

Processes configured by appending the PID to the name will not group properly in Application Advisor

Description: In an environment where the application process is configured to be named <process>_<PID> in System Performance Monitor, performance counters and other data will not be aggregated across all instances of the application. Instead each process will show up as a discreet application.

Workaround: Do not use the PID in the name if require grouping by process name.

Creating very long application environment tags will cause the configuration to fail for the application

Description: If you create a new environment tag with longer than 255 characters, you will get configuration failures on the agent side when the agent tries to configure monitoring for the application.

Workaround: Reduce the size of the environment tag.

You may receive a warning that secondary properties could not be discovered when monitoring WCF services

Description: With some WCF services the IIS API is unable to detect the version of .NET being used by the application pool. In these cases, the API will default to using the .NET 2.0 configuration files. If this happens, discovery will not be able to pull secondary endpoint properties from the application and will raise a warning.

Workaround: There is no workaround available.

Users may lose access to the Application Diagnostics and Advisor consoles

Description: Valid users may on rare occasion lose access to the Application Diagnostics and Advisor consoles. Connections to SQL Server are closed as “un-authorized access”.

Workaround: Restart the SQL Server hosting the Operations Manager database.

Management Pack Authoring

You might see the following issues related to management pack authoring when you use Operations Manager.

Searching for instance in the group dialog box can be slow

Description: When creating or modifying a group, it can take a long time to search for an instance if a large number of items are returned.

Workaround: Either wait for the instances to be returned or change the search to return fewer instances.

Cannot edit System Center 2012 – Operations Manager management pack in Operations Manager 2007 R2 Authoring Console

Description: Management packs that are exported from Operations Manager cannot be opened in the Operations Manager 2007 R2 Authoring Console. Management packs created by the Operations Manager R2 Authoring Console and any management packs created in Operations Manager 2007 R2 can be imported into System Center 2012 – Operations Manager.

Workaround: Edit the management pack in Operations Manager 2007 R2 or export from an existing Operations Manager 2007 R2 management group into the Authoring console. Once you have completed your edits, then import the management pack into Operations Manager.

Product Connectors

You might see the following issues related to product connectors when you use System Center 2012 – Operations Manager.

Operations Manager 2007 R2 Connectors may not work in System Center 2012 – Operations Manager

Description: The following connectors are not supported and may not work in System Center 2012 – Operations Manager.

- Microsoft System Center Operations Manager 2007 R2 Connector for IBM Tivoli Enterprise Console
- Microsoft System Center Operations Manager 2007 R2 Connector for HP OpenView Operations for Unix
- Microsoft System Center Operations Manager 2007 R2 Connector for HP OpenView Operations for Windows
- Microsoft System Center Operations Manager 2007 R2 Connector for BMC Remedy ARS
- Microsoft System Center Operations Manager 2007 R2 Universal Connector

If you have any of these connectors installed and open the **Interop Connectors** node in the Operations console, you may receive an error message.

Workaround: Interoperability between Operations Manager and other products is through System Center Orchestrator 2012.