Microsoft System Center 2012 R2

Operations Guide for System Center 2012 – Operations Manager

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

About This Document 11

Operations Guide for System Center 2012 - Operations Manager 11
- Quick Reference to Operations Manager Tasks 13
- Initial Monitoring After Operations Manager Is Installed 16
  - Managing Discovery and Agents 17
    - Operations Manager Agent Installation Methods 18
    - Install Agent on Windows Using the Discovery Wizard 19
    - Install Agent on UNIX and Linux Using the Discovery Wizard 22
    - Install Agent Using the MOMAgent.msi Setup Wizard 24
    - Install Agent Using the Command Line 26
    - Install Agent and Certificate on UNIX and Linux Computers Using the Command Line 29
    - Managing Certificates for UNIX and Linux Computers 33
    - Process Manual Agent Installations 34
    - Applying Overrides to Object Discoveries 37
    - Configuring Agents 38
    - Examples of Using MOMAgent Command to Manage Agents 41
    - Upgrading and Uninstalling Agents on UNIX and Linux Computers 42
    - Upgrading Agents on UNIX and Linux Computers Using the Command Line 44
    - Manually Uninstalling Agents from UNIX and Linux Computers 47
    - Uninstall Agent from Windows-based Computers 49
  - Using Management Packs 50
    - What Is in an Operations Manager Management Pack? 51
    - Management Packs Installed with Operations Manager 55
    - Management Pack Life Cycle 58
    - How to Import an Operations Manager Management Pack 62
    - How to Remove an Operations Manager Management Pack 66
    - Creating a Management Pack for Overrides 67
    - How to Export an Operations Manager Management Pack 70
    - How to Add Knowledge to a Management Pack 71
  - Tuning Monitoring by Using Targeting and Overrides 72
    - Using Classes and Groups for Overrides in Operations Manager 74
    - How to Override a Rule or Monitor 76
    - How to Enable or Disable a Rule or Monitor 77
    - Using the Enforced Attribute in Overrides 78
    - How to Enable Recovery and Diagnostic Tasks 79
- Managing Access in Operations Manager 81
  - Operations Manager Accounts 82
  - Implementing User Roles 84

Choose a Profile 86
Define a Scope Using Operations Manager Groups 89
Assign Tasks and Views 89
How to Assign Members to User Roles 90
Operations Associated with User Role Profiles 92
How to Create a New Action Account in Operations Manager 97
How to Manage the Report Server Unattended Execution Account in Operations Manager 98
Control Access by Using the Health Service Lockdown Tool in Operations Manager 99
Accessing UNIX and Linux Computers in Operations Manager 100
Credentials You Must Have to Access UNIX and Linux Computers 102
How to Set Credentials for Accessing UNIX and Linux Computers 105
How to Configure sudo Elevation and SSH Keys 111
Required Capabilities for UNIX and Linux Accounts 114
Configuring SSL Ciphers 117
Administering and Configuring the UNIX/Linux Agent 118
Managing Run As Accounts and Profiles 122
Distribution and Targeting for Run As Accounts and Profiles 123
How to Create a Run As Account 125
How to Associate a Run As Account to a Run As Profile 127
How to Create a New Run As Account for Accessing the Operations Manager Database 129
How to Configure Run As Accounts and Profiles for UNIX and Linux Access 130
Operations Manager Monitoring Scenarios 133
Agentless Monitoring in Operations Manager 133
How to Configure a Computer for Agentless Management 135
How to Configure a Proxy for Agentless Monitoring 137
Monitoring Across Untrusted Boundaries in Operations Manager 139
About Gateway Servers in Operations Manager 139
Determining the Health of Gateway Servers 140
Using Multiple Gateway Servers 142
How to Configure Agent Failover to Multiple Gateway Servers 142
How to Configure a Gateway Server to Failover Between Multiple Management Servers 143
Certificate Renewal for Gateway Servers and Management Servers 144
Client Monitoring Using Agentless Exception Monitoring in Operations Manager 145
How to Configure a Management Server for Client Monitoring 146
How to Configure Clients for Client Monitoring 149
How to Customize Client Monitoring Data Collection and Solution Response URLs for Error Groups 149
How to Configure Error Transmission Settings for Client Monitoring in Operations Manager 150
Forwarding Client Error Reports (Client Monitoring) 152
Monitoring Clusters by Using Operations Manager 153
Monitoring Networks by Using Operations Manager 154

How to Discover Network Devices in Operations Manager 158
Network Device Discovery Settings 165
Run As Accounts for Network Monitoring in Operations Manager 171
How to Delete or Restore a Network Device in Operations Manager 172
Tuning Network Monitoring 174
Viewing Network Devices and Data in Operations Manager 194
Security for Servers Performing Network Discovery 198
Network Devices Supported for Discovery by Operations Manager 198
Reports for Network Monitoring in Operations Manager 199
Monitoring Service Level Objectives by Using Operations Manager 200
Defining a Service Level Objective Against an Application 201
Defining a Service Level Objective Against a Group 203
Running a Service Level Tracking Report 204
Creating a Service Level Dashboard 205
Monitoring .NET Applications 207
Viewing and Investigating Alerts for .NET Applications (Server-side Perspective) 208
Working with the Application Diagnostics Console 217
Working with Events by Using Application Diagnostics 222
Prioritizing Alerts by Using Application Advisor 226
User Roles for Application Performance Monitoring 229
How to Configure Grooming Settings for .NET Application Performance Monitoring Events 230
Working with Sensitive Data for .NET Applications 235
Notes for AVIcode 5.7 Customers 236
Monitoring Java Applications 239
How to Configure Monitoring for Java Applications 240
How to Monitor Java Applications 243
Strategies for Monitoring a New Java Application 245
Fabric Monitoring 246
Getting Started with the Fabric Health Dashboard 247
Scoping the Fabric Health Dashboard to a Specific Cloud and Investigating Details 249
The Fabric Monitoring Diagram View: Displaying Health States of Cloud Environments 250
Using System Center Advisor to Proactively Monitor Cloud Fabric 251
Monitoring UNIX and Linux Computers by Using Operations Manager 252
Supported UNIX and Linux Operating System Versions 252
Using Templates for Additional Monitoring of UNIX and Linux 260
Troubleshooting UNIX and Linux Monitoring 261
Certificate Issues 261
Management Pack Issues 263
Operating System Issues 265
Logging and Debugging 266
Monitoring Linux Computers in Windows Azure by Using Operations Manager 268
Collecting Security Events Using Audit Collection Services in Operations Manager 273

Audit Collection Services Security ... 277
Audit Collection Services Capacity Planning ... 278
Audit Collection Services Performance Counters ... 283
How to Enable Audit Collection Services (ACS) Forwarders ... 286
How to Enable Event Logging and ACS Rules on Solaris and AIX Computers ... 287
How to Filter ACS Events for UNIX and Linux Computers ... 289
How to Configure Certficates for ACS Collector and Forwarder ... 290
Monitoring Audit Collection Services Performance ... 293
How to Remove Audit Collection Services (ACS) ... 296
Audit Collection Services Administration (AdtAdmin.exe) ... 297
AdtAdmin.exe /AddGroup ... 300
AdtAdmin.exe /DelGroup ... 301
AdtAdmin.exe /Disconnect ... 302
AdtAdmin.exe /GetDBAuth ... 304
AdtAdmin.exe /GetQuery ... 305
AdtAdmin.exe /ListForwarders ... 305
AdtAdmin.exe /ListGroups ... 307
AdtAdmin.exe /SetDBAuth ... 309
AdtAdmin.exe /SetQuery ... 310
AdtAdmin.exe /Stats ... 311
AdtAdmin.exe /UpdForwarder ... 314
AdtAdmin.exe /UpdGroup ... 316
Connecting Operations Manager With Other Management Systems ... 317
How to Configure a Product Connector Subscription ... 318
Monitoring Operations Manager from a Second Management Group ... 319
Integrating Active Directory and Operations Manager ... 320
Using Active Directory Domain Services to Assign Computers to Operations Manager Management Groups ... 320
How to Create an Active Directory Domain Services Container for a Management Group ... 322
How to Use Active Directory Domain Services to Assign Computers to Management Servers ... 323
Changing the Active Directory Integration Setting for an Agent ... 326
Viewing System Center Advisor Alerts ... 326
Getting Information from Operations Manager ... 328
Using the Operations Manager Consoles ... 330
Comparing the Operations Console and Web Console in Operations Manager ... 330
How to Connect to the Operations Console ... 332
How to Connect to the Web Console ... 333
Using the Monitoring Workspace in Operations Manager ... 334
Using Health Explorer in Operations Manager ... 336
Using My Workspace in Operations Manager ... 337
Using the Administration Workspace in Operations Manager ... 340

Using the Reporting Workspace in Operations Manager ... 345
Using the Authoring Workspace in Operations Manager ... 346
Finding Data and Objects in the Operations Manager Consoles ... 350
Using Advanced Search ... 354
Examples of Using Advanced Search in Operations Manager ... 357
Using Views in Operations Manager ... 358
View Types in Operations Manager ... 358
Standard Views in Operations Manager ... 366
Creating Views in Operations Manager ... 371
How to Personalize a View in Operations Manager ... 381
Guidance for Scoping and Targeting Views ... 381
Using SharePoint to View Operations Manager Data ... 382
Subscribing to Alert Notifications ... 390
How to Create and Configure the Notification Action Account ... 391
How to Enable an Email Notification Channel ... 392
How to Enable an Instant Message Notification Channel ... 394
How to Enable a Text Message (SMS) Notification Channel ... 395
How to Enable a Command Notification Channel ... 396
How to Create Notification Subscribers ... 397
How to Create Notification Subscriptions ... 400
How to Customize Message Content for Notifications ... 402
How to Subscribe to Notifications from an Alert ... 404
How to Create Subscriptions Using Classes and Groups ... 405
How to Specify Which Alerts Generate Notifications (Conditions) ... 407
Sending Notifications for Specific Computers and Specific Alerts to Specific Teams ... 409
Using Reports in Operations Manager ... 410
Operations Manager Reports Library ... 410
How to Create Reports in Operations Manager ... 417
How to Create an Alert Logging Latency Report ... 417
How to Create an Alerts Report ... 418
How to Create an Availability Report ... 419
How to Create a Configuration Changes Report ... 420
How to Create an Event Analysis Report ... 421
How to Create an Operational Data Report ... 421
How to Save a Report ... 422
How to Run a Report ... 423
Scheduling Reports ... 424
How to Create a Report Schedule ... 425
How to Email Scheduled Reports ... 426
How to Schedule the Delivery of a Report to the SQL Report Server Cache ... 427
How to Cancel a Scheduled Report ... 428
How to Edit a Scheduled Report ... 429
How to Export a Report ... 429

How to Troubleshoot Reports that Return No Data ... 430
Not Monitored and Gray Agents ... 432
How to View All Rules and Monitors Running on an Agent-Managed Computer ... 434
Using the Visio 2010 Add-in and SharePoint 2010 Visio Services Data Provider ... 435
Install the Visio 2010 Add-in ... 436
Install the Visio Services Data Provider ... 437
Grant Visio Services with Read-Only Operator Permissions ... 438
Configure the Operations Manager Data Source in Visio 2010 ... 439
View an Operations Manager Distributed Application Diagram in Visio 2010 ... 440
Add Links to Operations Manager to a New or Existing Visio 2010 Document ... 441
Build a simple monitoring dashboard using the Visio Web Part ... 443
Publish a Visio diagram to SharePoint 2010 ... 444
Change the Way Health State is Represented in Visio 2010 ... 444
Troubleshooting the Visio 2010 Add-in ... 445
General Tasks in Operations Manager ... 447
Managing Alerts ... 448
How Heartbeats Work in Operations Manager ... 449
Resolving Heartbeat Alerts ... 451
How an Alert is Produced ... 453
Viewing Active Alerts ... 455
Viewing Alert Details ... 457
Examining Properties of Alerts, Rules, and Monitors ... 458
Impact of Closing an Alert ... 462
How to Close an Alert Generated by a Monitor ... 463
How to Reset Health ... 464
Identifying the Computer Experiencing a Problem ... 466
Using Health Explorer to Investigate Problems ... 468
Using Event View to Investigate Problems ... 471
Investigating Alert Storms ... 473
How to Set Alert Resolution States ... 474
How to Configure Automatic Alert Resolution ... 475
Diagnostic and Recovery Tasks ... 476
How to Suspend Monitoring Temporarily by Using Maintenance Mode ... 479
Creating and Managing Groups ... 481
How to Create Groups in Operations Manager ... 483
How to View Group Members, State, and Diagram ... 486
Running Tasks in Operations Manager ... 486
How to Create a Resource Pool ... 490
Managing Resource Pools for UNIX and Linux Computers ... 492
Connecting Management Groups in Operations Manager ... 494
Using Operations Manager Shell ... 497
Maintenance of Operations Manager ... 497
Monitoring the Health of the Management Group ... 498

Inventory of Operations Manager Infrastructure 501
Scheduling Maintenance in Operations Manager 505
How and When to Clear the Cache 506
How to Restart a Management Server 508
How to Configure Grooming Settings for the Reporting Data Warehouse Database 509
How to Configure Grooming Settings for the Operations Manager Database 511
Recommendations for Daily, Weekly, and Monthly Operations Manager Tasks 512
Integrating Operations Manager with Development Processes 513
Integrating Operations Manager with Development Processes in System Center 2012 R2 514
How to Configure Integration with TFS in System Center 2012 R2 515
How to Change the Frequency of Synchronization for Integration with TFS in System Center 2012 R2 522
How to Manually Import an Operational Issue WITD to TFS in System Center 2012 R2 524
How to Configure Whether Files Are Attached or Linked in Synchronization with TFS in System Center 2012 R2 525
How to Configure Notifications when Developers Reassign Work Items to IT Operations in System Center 2012 R2 526
How to Automatically Assign New Alerts to Engineering in System Center 2012 R2 ... 527
How to Automatically Close Alerts When Work Items Are Resolved in TFS in System Center 2012 R2 529
How to Stop and Resume Synchronization with TFS in System Center 2012 R2 530
How to Configure File Attachments for Operations Manager Alerts in System Center 2012 R2 532
How to Synchronize Alerts with TFS in System Center 2012 R2 534
How to Configure Integration with IntelliTrace Historical Profiling in System Center 2012 R2 536
How to Collect IntelliTrace Historical Profiling Traces from System Center 2012 R2 537
Monitoring Integration between Operations Manager and TFS in System Center 2012 R2 541
Integrating Operations Manager with Development Processes in System Center 2012 SP1 543
How to Configure Integration with TFS in System Center 2012 SP1 544
How to Change the Frequency of Synchronization for Integration with TFS in System Center 2012 SP1 550
How to Manually Import an Operational Issue WITD to TFS in System Center 2012 SP1 553
How to Configure Whether Files Are Attached or Linked in Synchronization with TFS in System Center 2012 SP1 554
How to Configure Notifications when Developers Reassign Work Items to IT Operations in System Center 2012 SP1 555
How to Automatically Assign New Alerts to Engineering in System Center 2012 SP1 . 556

How to Automatically Close Alerts When Work Items Are Resolved in TFS in System Center 2012 SP1 558
How to Stop and Resume Synchronization with TFS in System Center 2012 SP1 559
How to Configure File Attachments for Operations Manager Alerts in System Center 2012 SP1 561
How to Synchronize Alerts with TFS in System Center 2012 SP1 563
How to Configure Integration with IntelliTrace Historical Profiling in System Center 2012 SP1 564
How to Collect IntelliTrace Historical Profiling Traces from System Center 2012 SP1 565
Monitoring Integration between Operations Manager and TFS in System Center 2012 SP1 569
Monitoring with Microsoft Monitoring Agent 571
Installing Microsoft Monitoring Agent 571
Monitoring Web Applications with Microsoft Monitoring Agent 573
Comparing Monitoring Approaches for .NET Applications 575
Microsoft Monitoring Agent Compatibility 578

About This Document

The content in this guide is written primarily for online presentation in the TechNet Library. The document version of this guide (.doc or .pdf) compiles the online topics into a single file. Because the individual online topics must include the appropriate context and navigation to other topics, you will note some redundancy between topics in the document version of this guide.

Feedback

Send suggestions and comments about this content to opsmgrdocs@microsoft.com.

Revision History

Release Date	Changes
July 15, 2011	Original release of this guide.
Oct 28, 2011	Content updated from the beta release of Operations Manager and released to TAP customers on the Connect site.
Nov 10, 2011	Content updated from the beta release of Operations Manager and released publicly on the Download Center.
Dec 12, 2011	Content for Operations Manager Release Candidate updated with bug fixes and added topics.

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
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.

To perform this task	Do this
• 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 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.

To perform this task	Do this
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.

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_SETTINGS 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.

Option	Action
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 • Performance Library • Process Monitoring Library • Health Internal Library • Health Library • Default Management Pack • Baselining Tasks Library

Purpose	Associated management packs
	• 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) • 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

Purpose	Associated management packs
	• 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 • Microsoft.SystemCenter.Visualization.Library • System Center Core Monitoring Views
Notifications	• Notifications Internal Library • Notifications Library
Reporting	• Data Warehouse Internal Library • Date Warehouse Library

Purpose	Associated management packs
	• 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

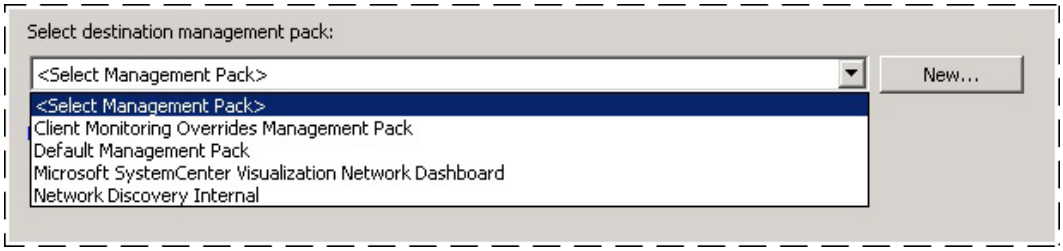
How to Add Knowledge to a Management Pack

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:

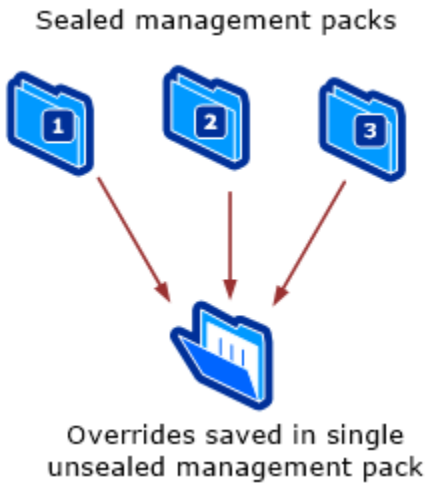
- A folder in the **Monitoring** workspace
- A unit, aggregate, or dependency monitor
- An attribute
- A group
- A rule
- A task
- A Run As profile
- Monitoring by using a management pack template
- Monitoring of a distributed application
- Tracking of service level objectives

Saving Overrides

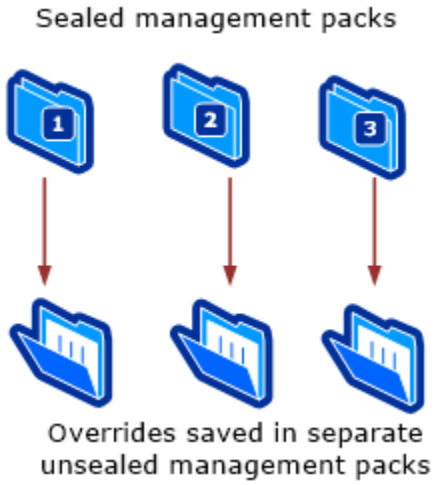
As a best practice, save all overrides for each sealed management pack to an unsealed management pack that is named ManagementPack_Override, where ManagementPack is the name of the sealed management pack to which the overrides apply. For example, overrides to the management pack Microsoft.InformationWorker.Office.XP.mp 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 **System Center 2012 - 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

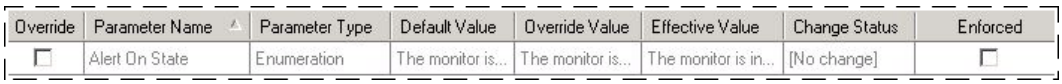
How to Override a Rule or Monitor

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

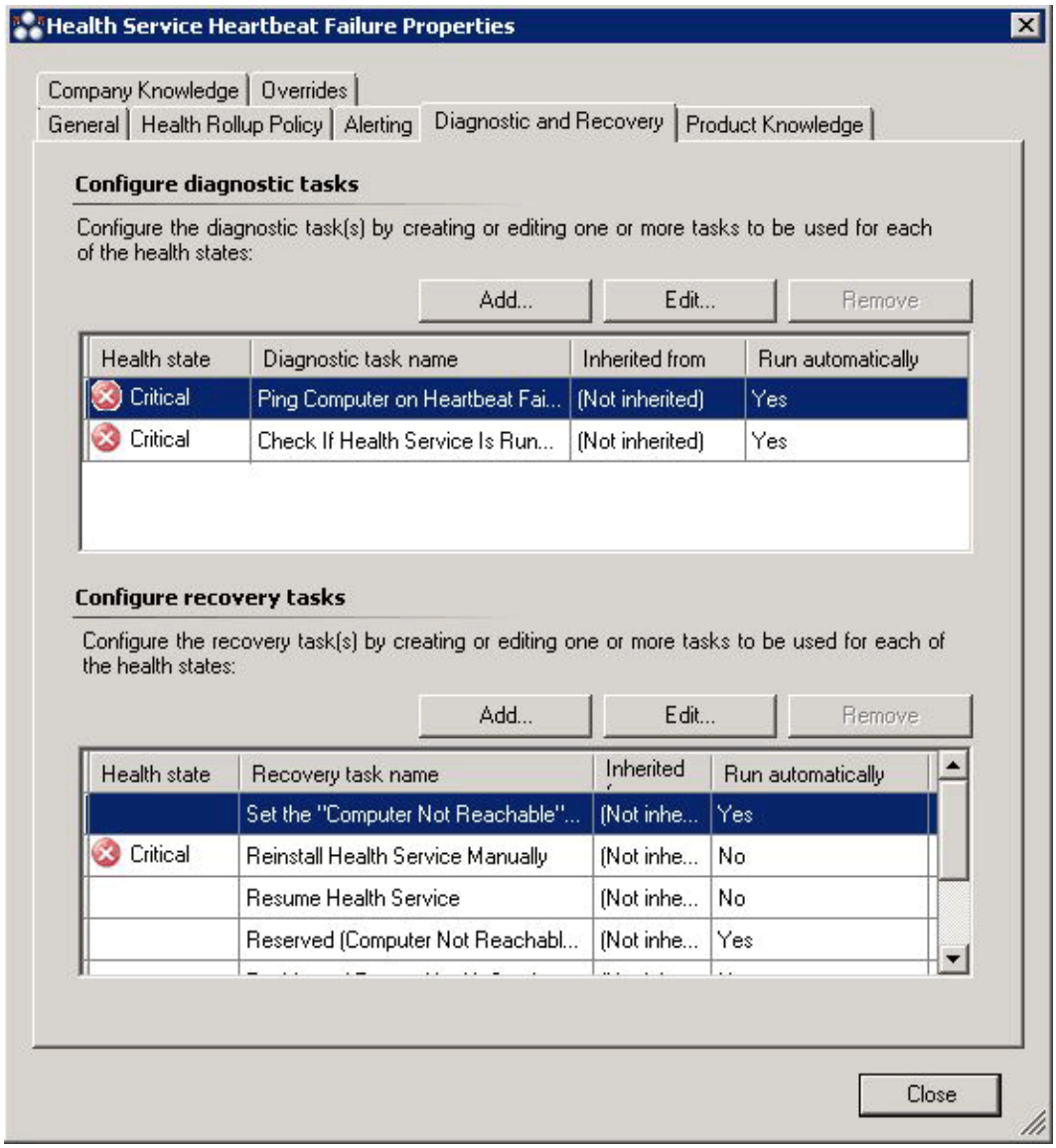
How to Enable Recovery and Diagnostic Tasks

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

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

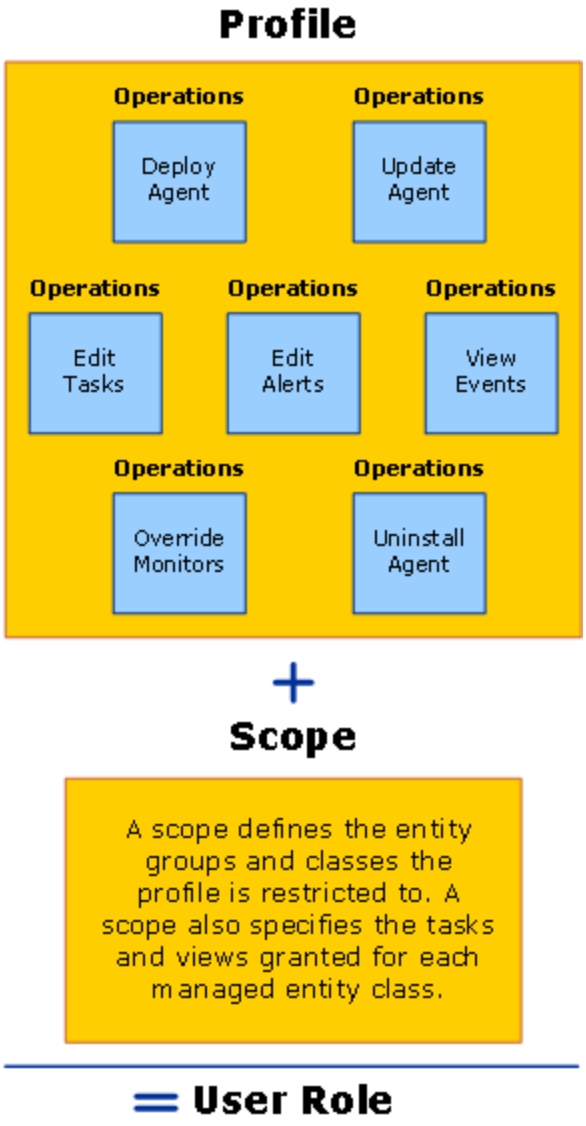
Managing Run As Accounts and Profiles

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

Profile	Job Functions and Scope
	that they would not otherwise have access to in views that use data from the operational database.
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 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.

User role	Description
	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

UNIX and Linux profile	Required capabilities

	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 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,

UNIX and Linux profile	Required capabilities
	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.
	• 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

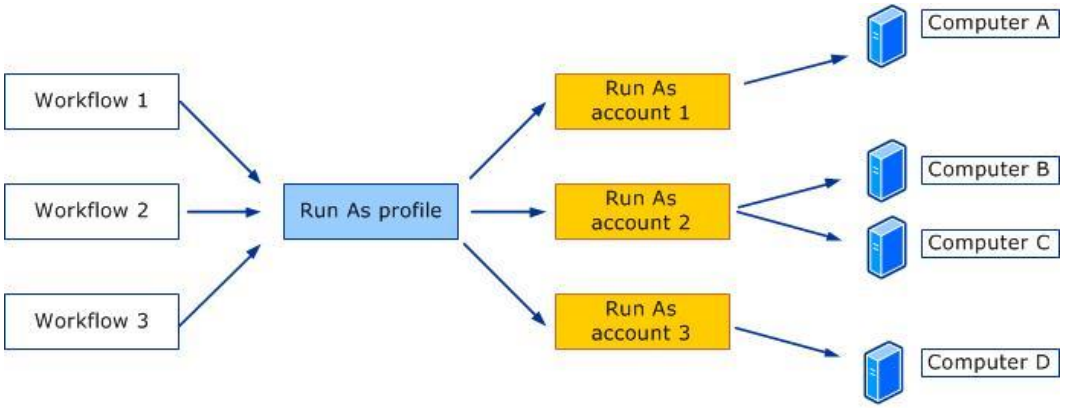
Managing Discovery and Agents

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.

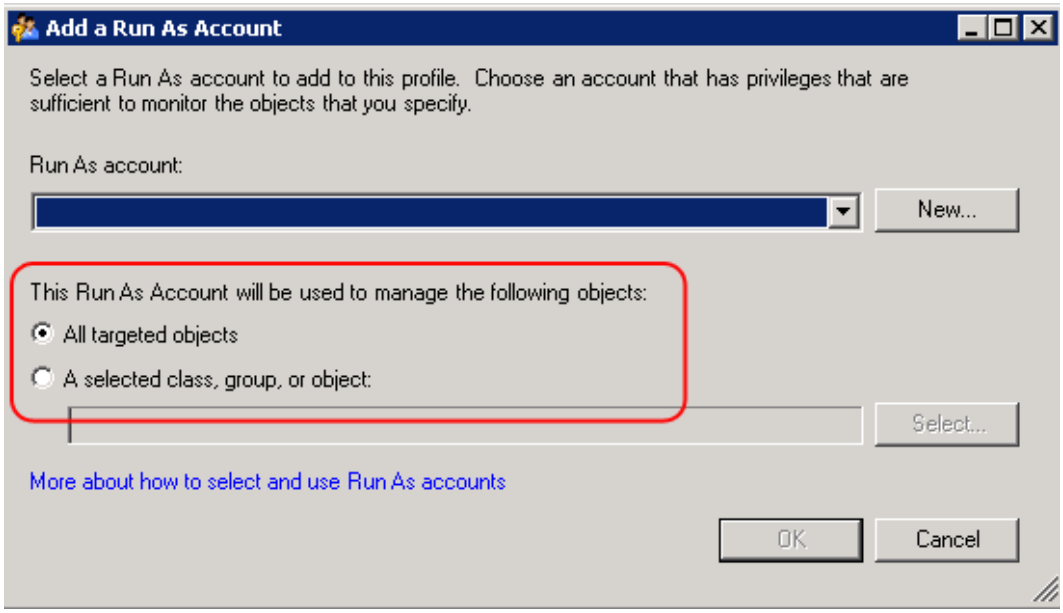
Other resources for Operations Manager

- 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

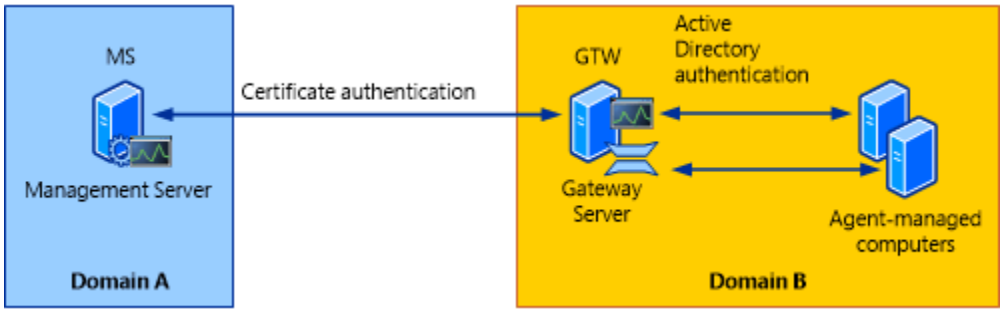
About Gateway Servers in Operations Manager

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

Setting	Location	Notes
		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* **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	**Devices** page, **Advanced**	If you specify **ICMP and SNMP**

Setting	Location	Notes
milliseconds)	**Discovery Settings** button	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. 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**

Setting	Location	Notes
		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 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. <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

Character	Description	Example
\	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 • 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)

Rule	Description	Types
		• 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 (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-

Rule	Description	Types
		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 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)

Rule	Description	Types
		• 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 (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

Rule	Description	Types
		(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) • 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

Rule	Description	Types
		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)
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)

Rule	Description	Types
		• 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-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)

Rule	Description	Types
		• 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) • 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-

Rule	Description	Types
		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)
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)

Rule	Description	Types
		• 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 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

Rule	Description	Types
		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) • 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

Rule	Description	Types
		(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 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)

Rule	Description	Types
		• 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 performance) • Network adapter (netcor) • Port (MIB2 Dot3

Rule	Description	Types
		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) • 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

Rule	Description	Types
		(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 per Second	Collects giant inbound packets per second.	Interface (Cisco Router)
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)

Rule	Description	Types
		• 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) • 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)

Rule	Description	Types
		• 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)
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

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)
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	Determines the change in the SNMP	Port (Dot3 ethernet)

Rule	Description	Types
Transmit Errors Rate	dot3StatsInternalMacTransmitErrorsRate value for the dot3_Ethernet_Performance_Port since the last polling.	

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 • 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	Aggregate monitor that rolls up queue drop percentage health	• BPX Port (Cisco)

Monitor	Description	Targets
Percentage	monitors	• 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 device	• Interface • Network Adapter

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

Reports for Network Monitoring in 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

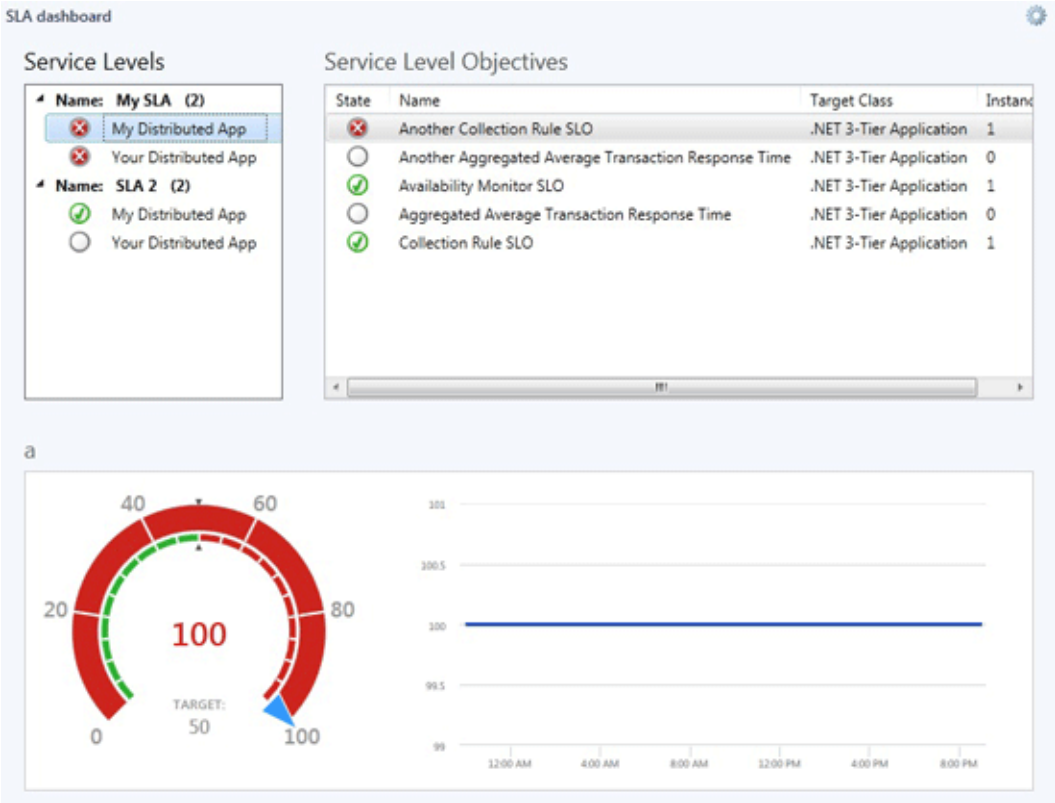
Defining a Service Level Objective Against a Group

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

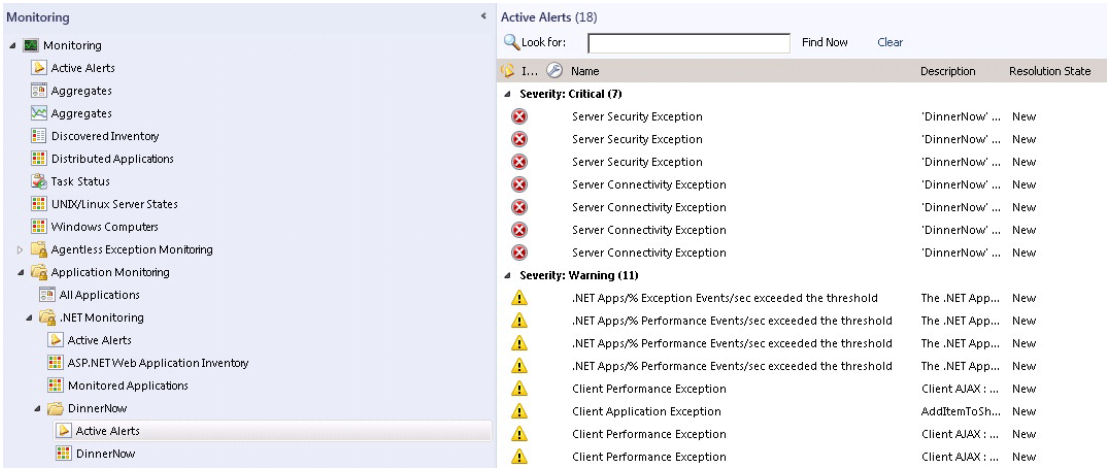
Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

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**.

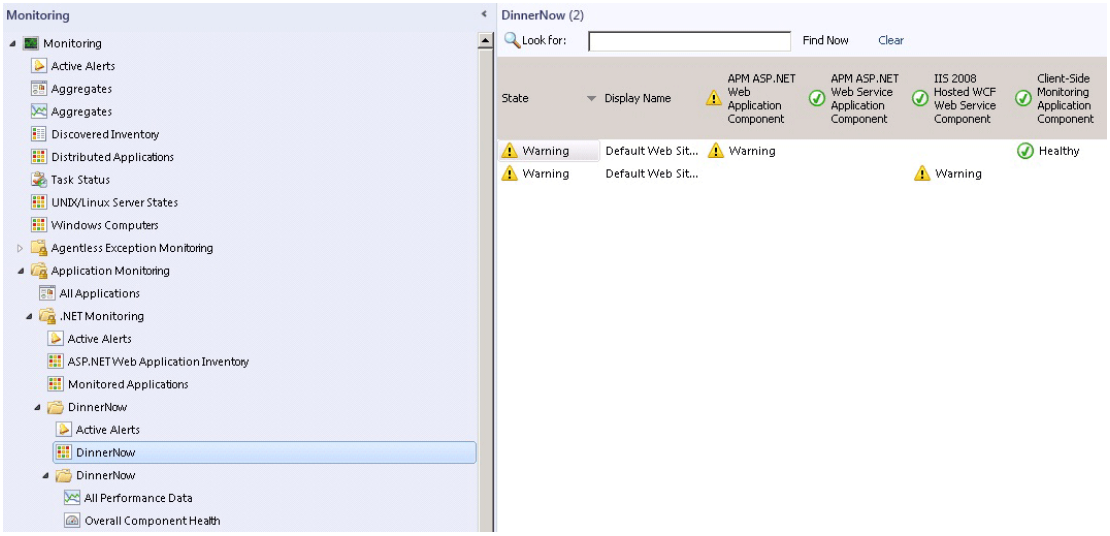
   View alerts by application group



   Additional views:

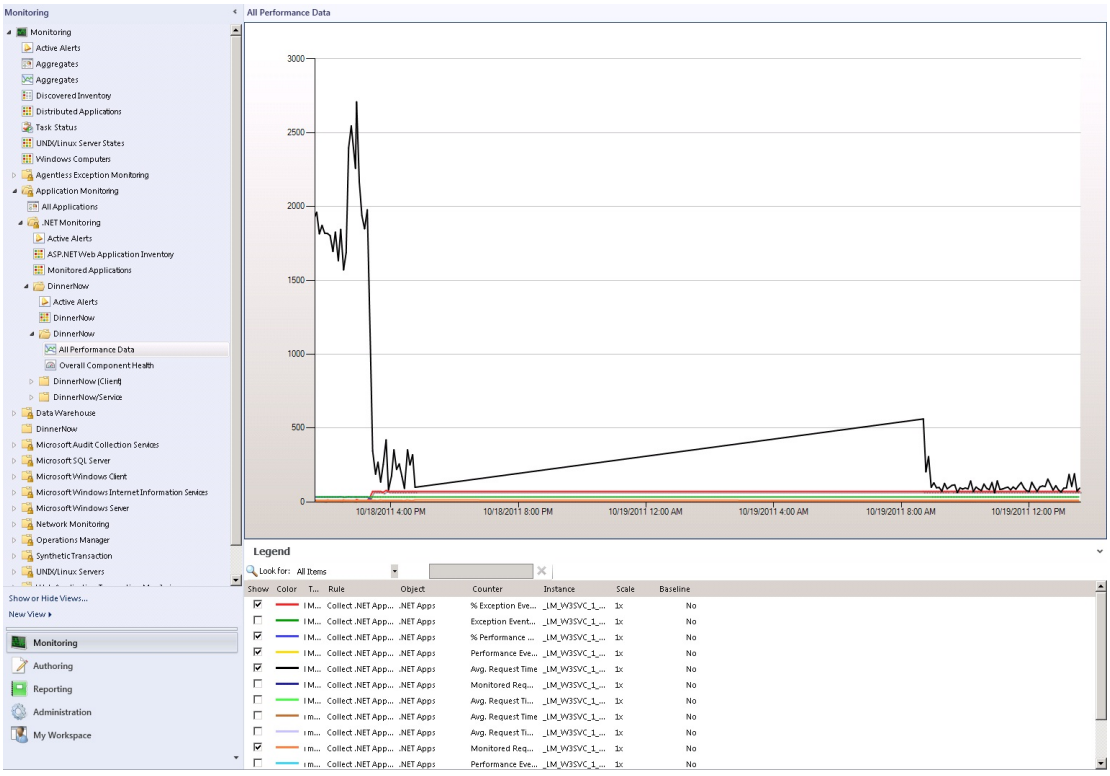
   - To see why a monitoring aspect is unhealthy, use the application group state view and click the state view cell related to it. The Details View will show you the instance and the state of the Availability, Configuration, Performance, and Security monitors. You can also start the Health Explorer in 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.

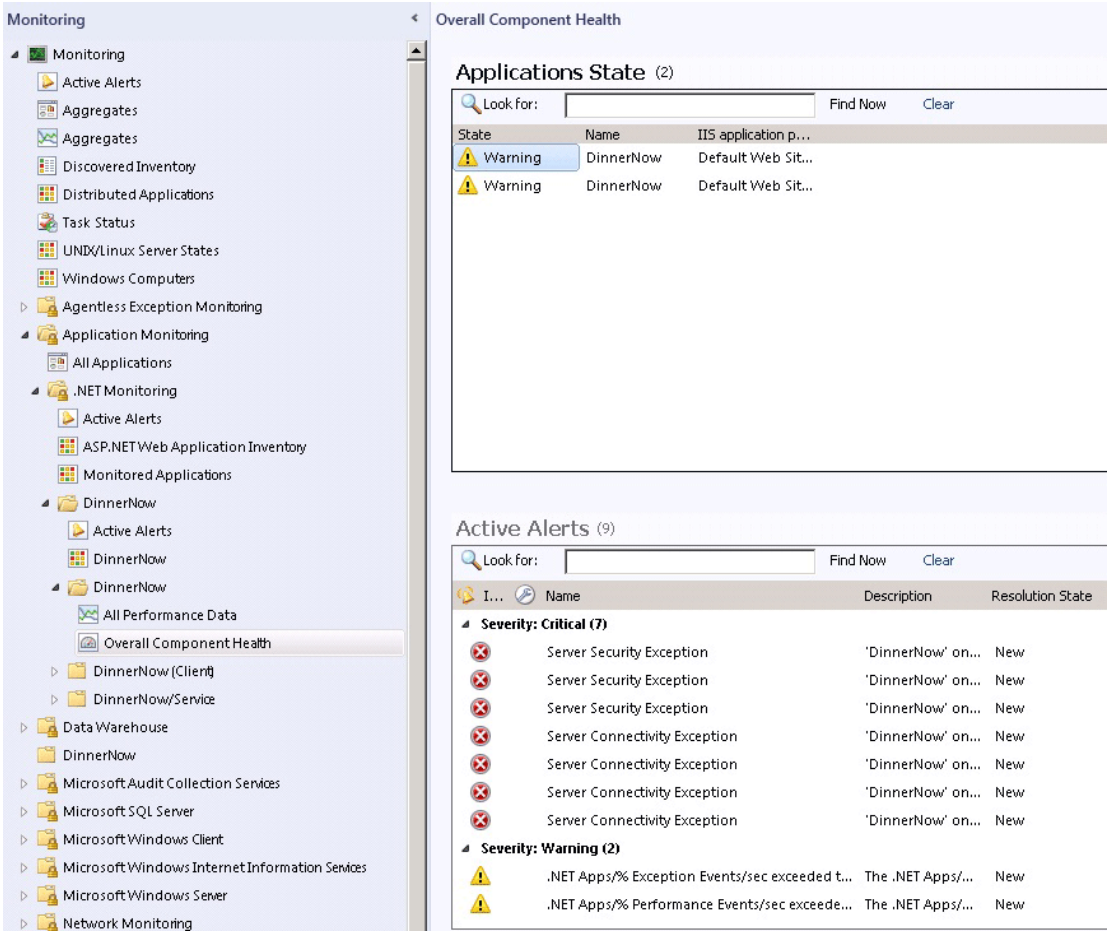
All performance data



- 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.

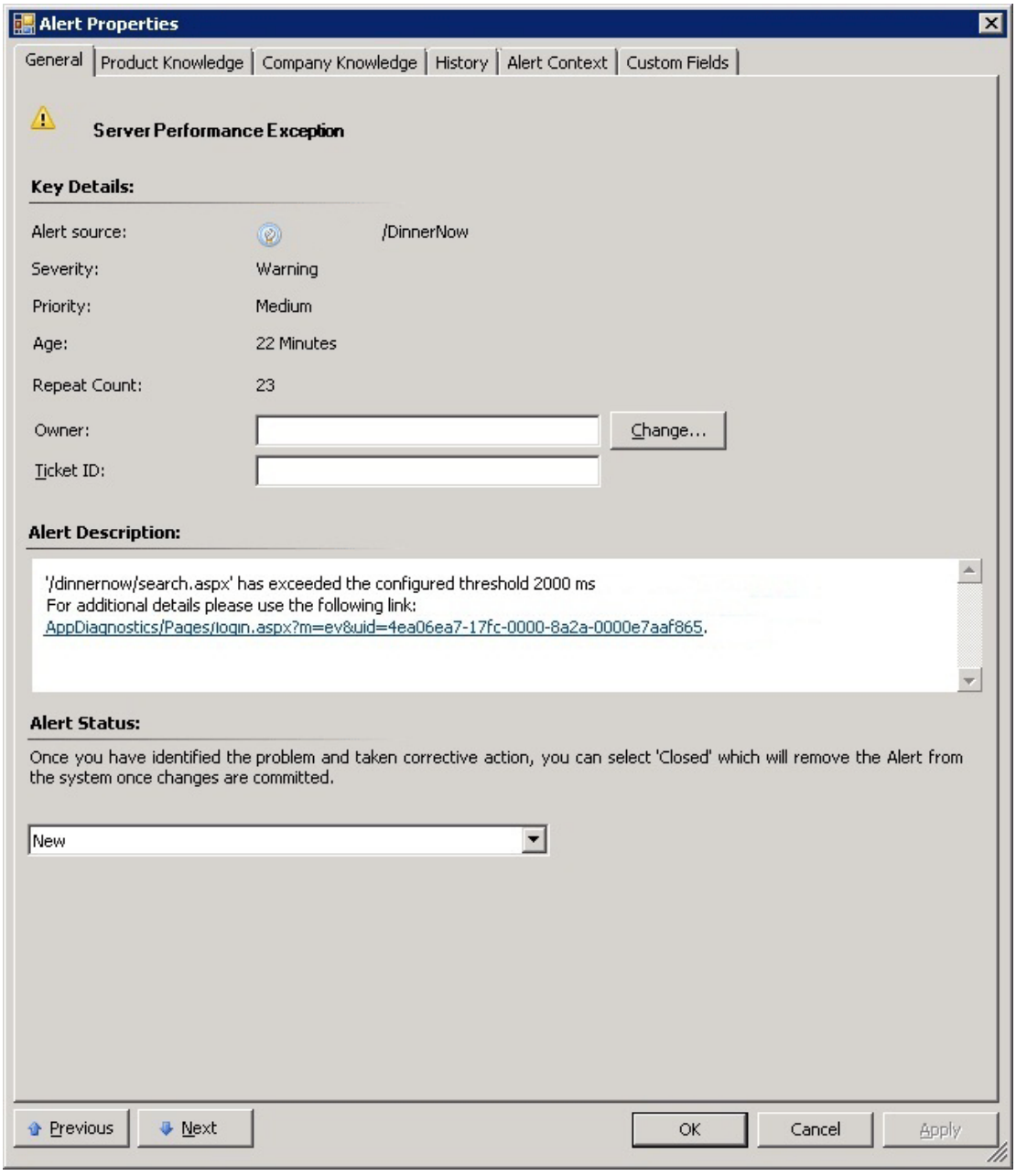
To make sure client-side application monitoring is working, go to the application group state view and the **CSM Application Component** will have application monitoring status filled in.

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



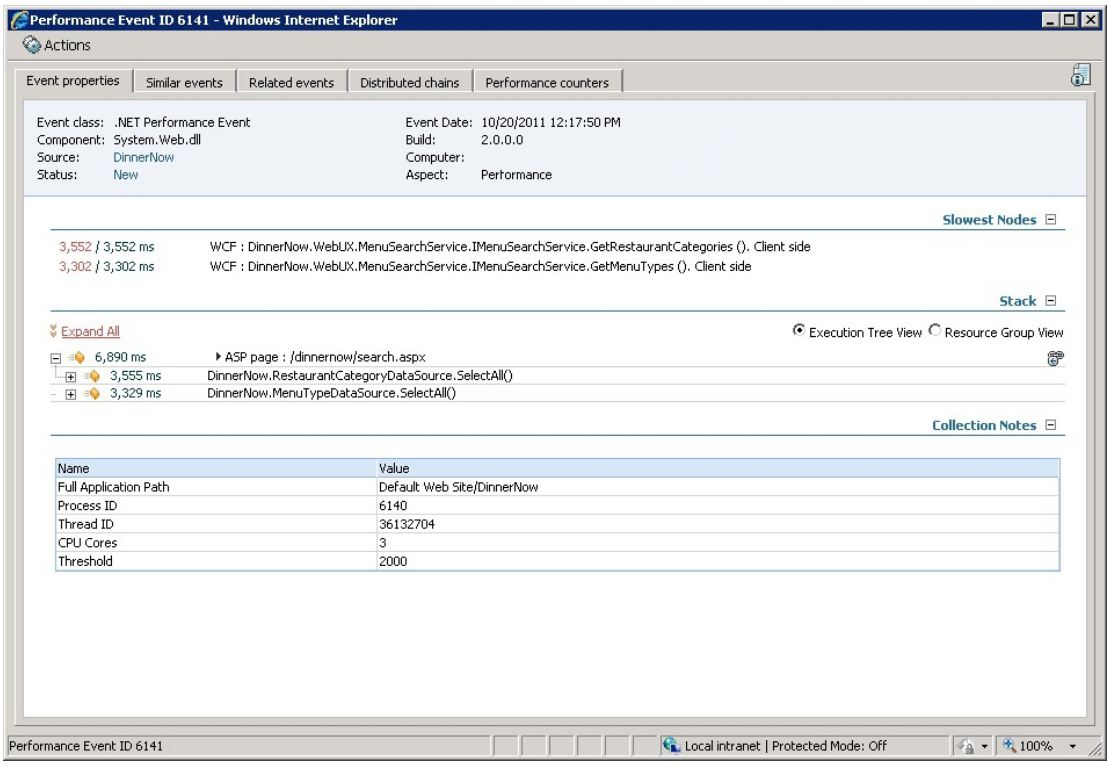
Note

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.

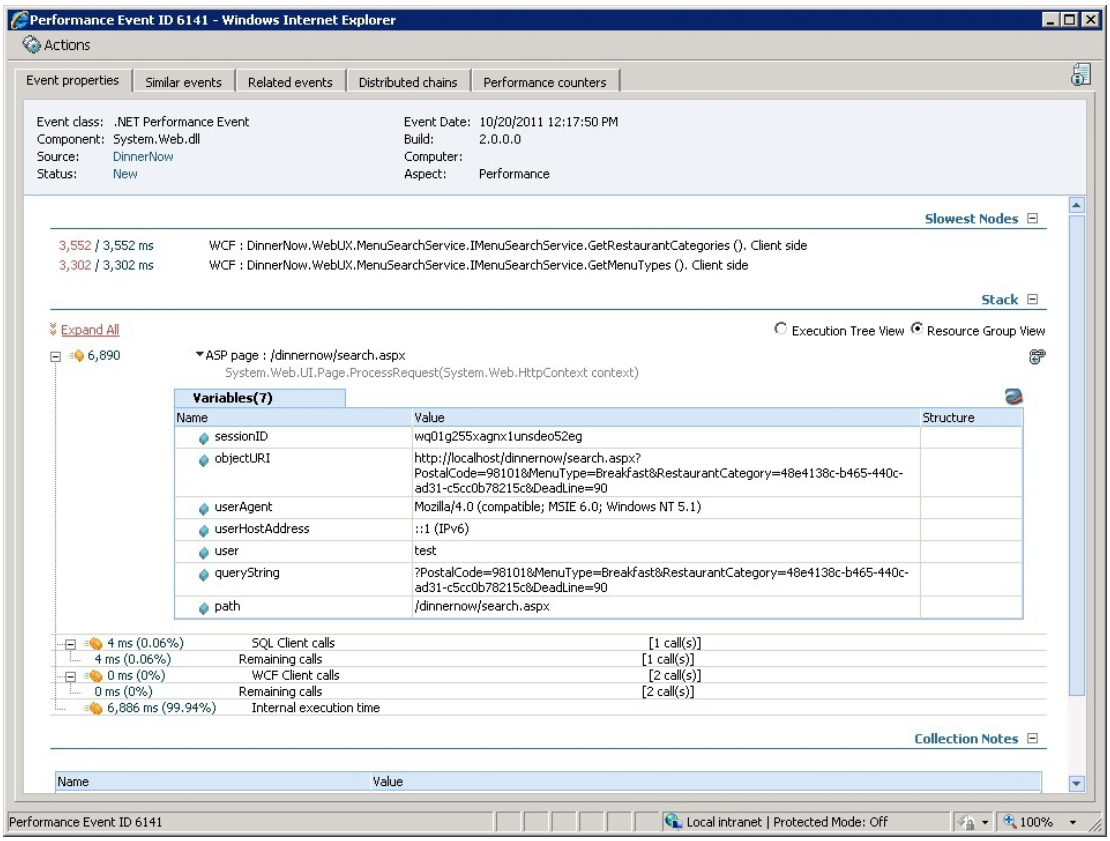
   Note
   This link to Application Diagnostics is also on the **Alert Context** tab.

5. **Application Diagnostics Event properties**



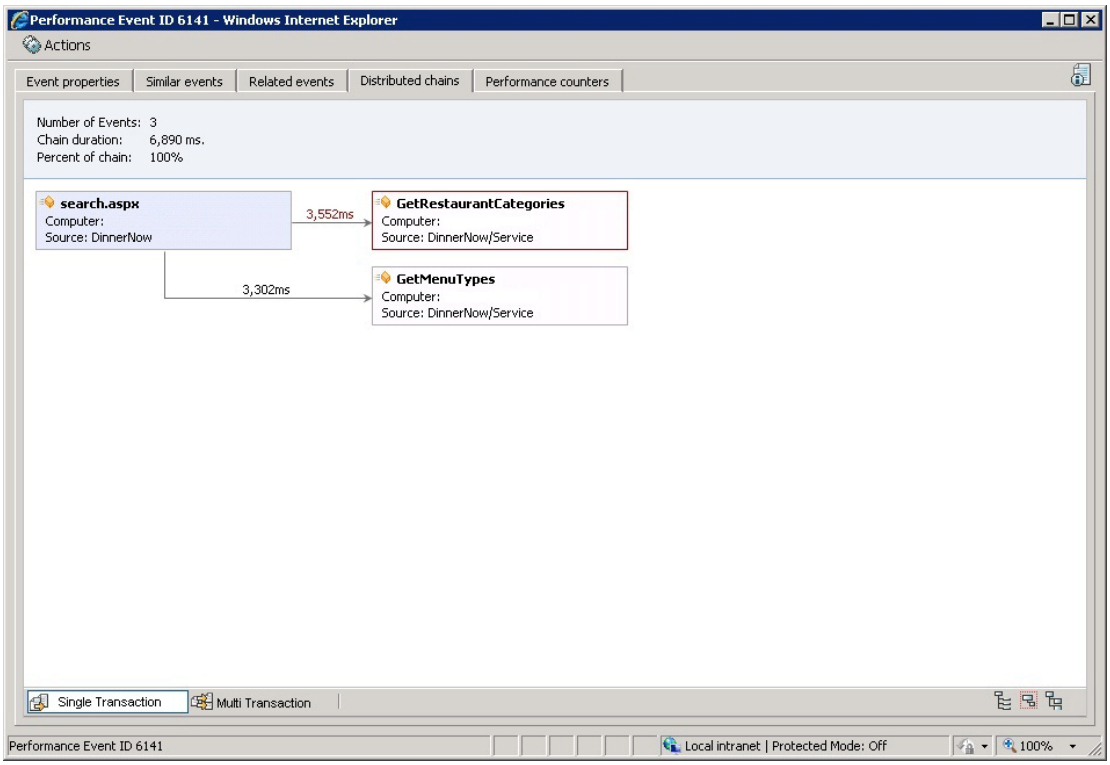
6. On the **Event Properties** tab, expand the **Stack** section. The stack is the order in which events happened. The **Resource Group View** and **Execution Tree View** allow you to expand nodes to investigate the various calls. This view helps answer which tier the problem is in, or where is it occurring.

   Application Diagnostics tree views lets you see exactly what went wrong where and when.



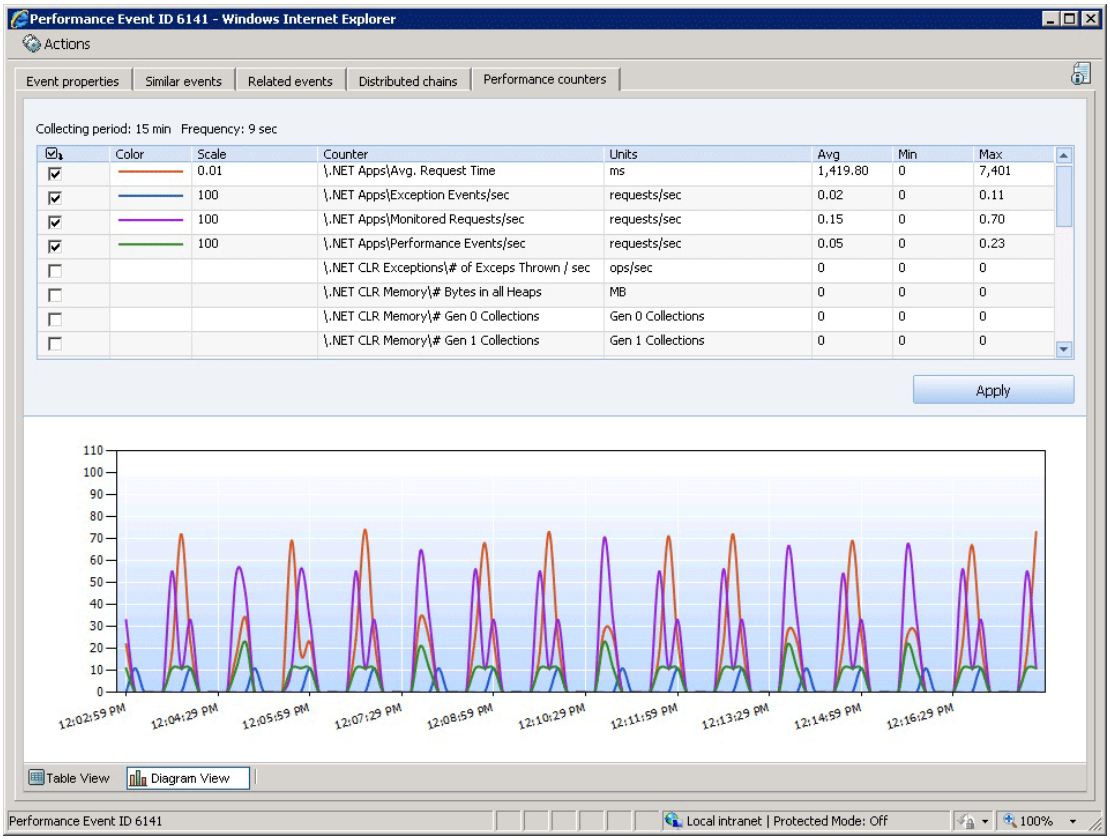
7. To see how this event relates to other events in the chain of events, on the Application Diagnostics page, click the **Distributed chains** tab. This view shows all of the components that are involved in the request.

   Application Diagnostics Distributed chains show how events relate to each other.



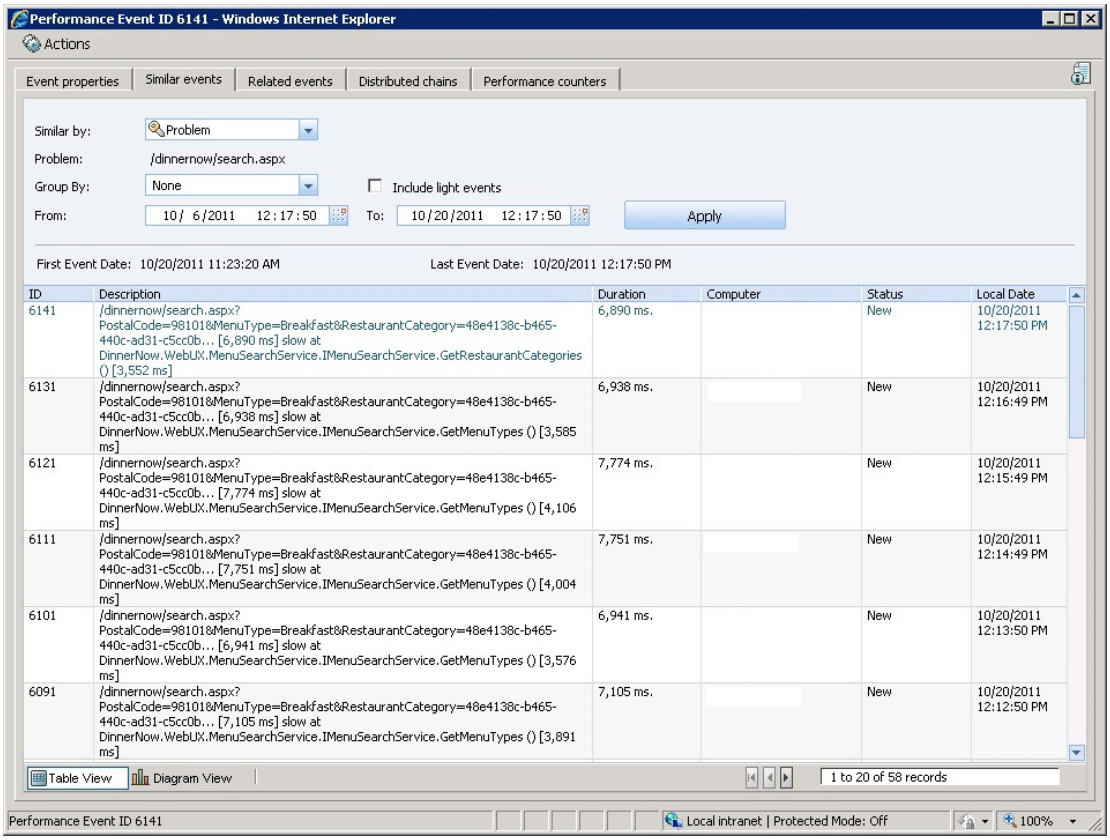
8. To pinpoint the root cause of the problem or incident, click the last event in the chain. This is the latest event that broke the performance threshold. The **Event Properties** tab for that event will open.
9. On the **Application Diagnostics** page, click the **Performance counters** tab. Performance 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.



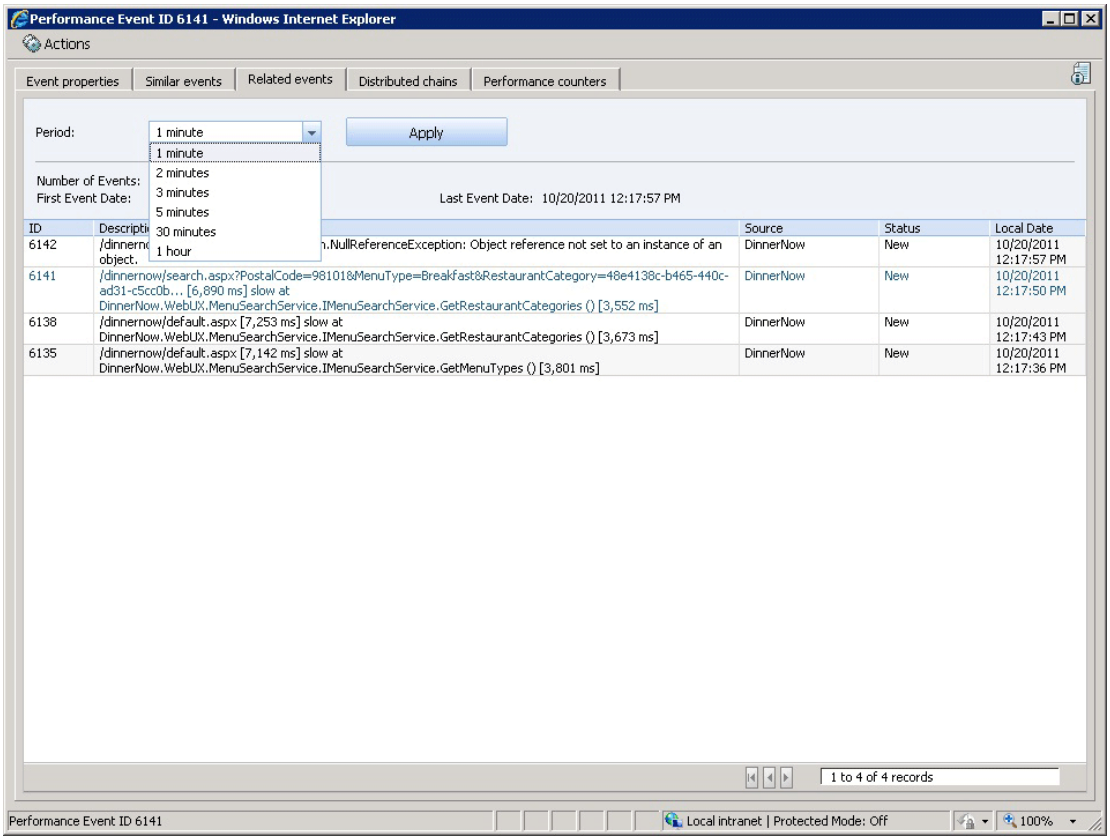
10. On the **Application Diagnostics** page, click the **Similar events** tab. Similar events are the other events that are in the same problem group. On this page you can filter similar events by **Problem** and **Heaviest Resource** to help you identify trends.

    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

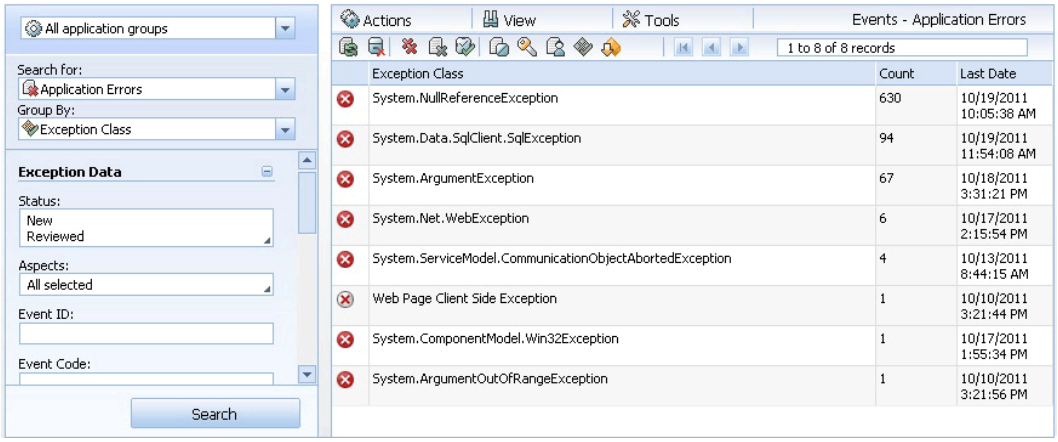
- **Problem** What it displays: All events in this grouping are coming from the same entry point into the application (for example, a method or a web page) and have the same call stack. Value: Consolidating events by problem allows you to prioritize your efforts to correct an issue based on the number 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.

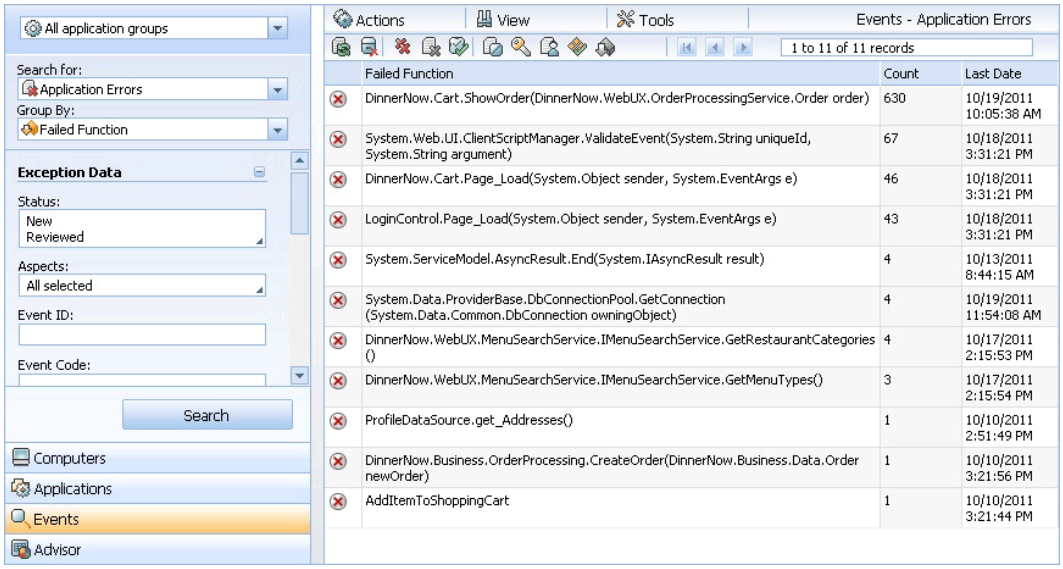


To group application errors by exception class

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.

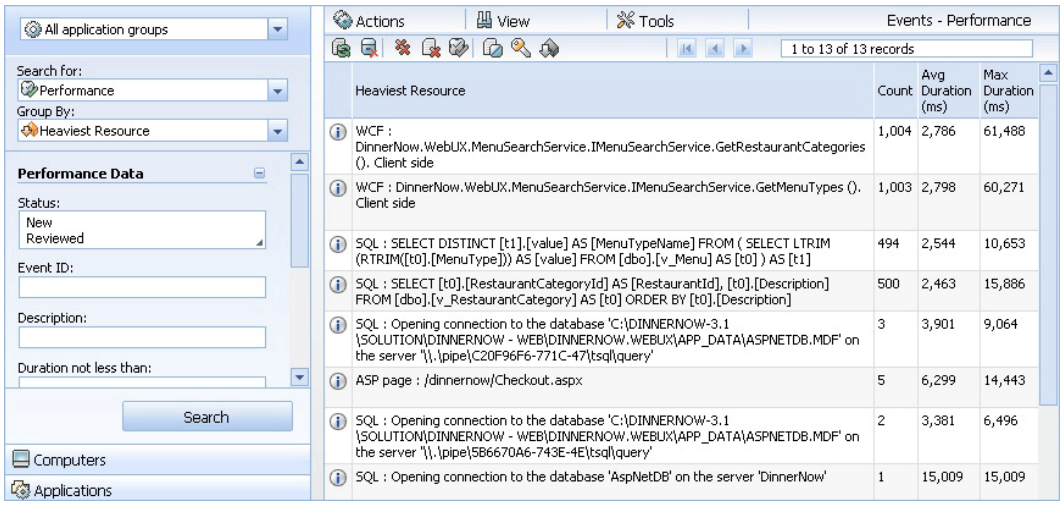


To group application errors by failed function

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.

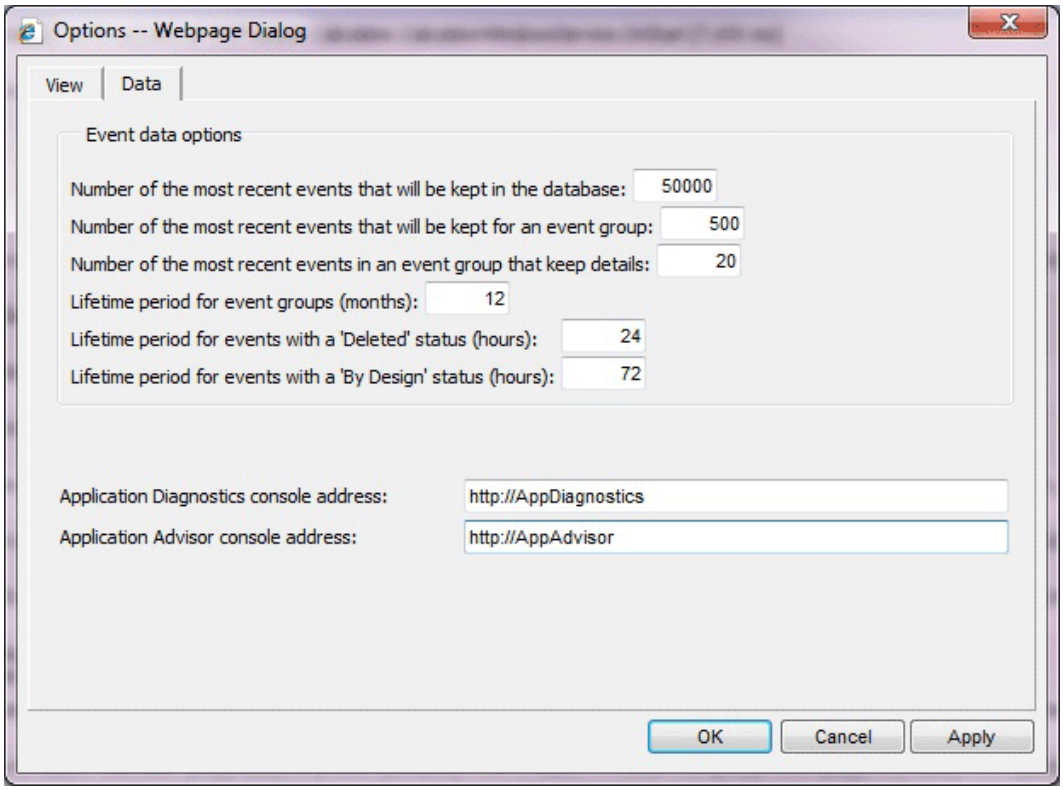
How to Configure Grooming Settings for .NET Application Performance Monitoring Events

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**.

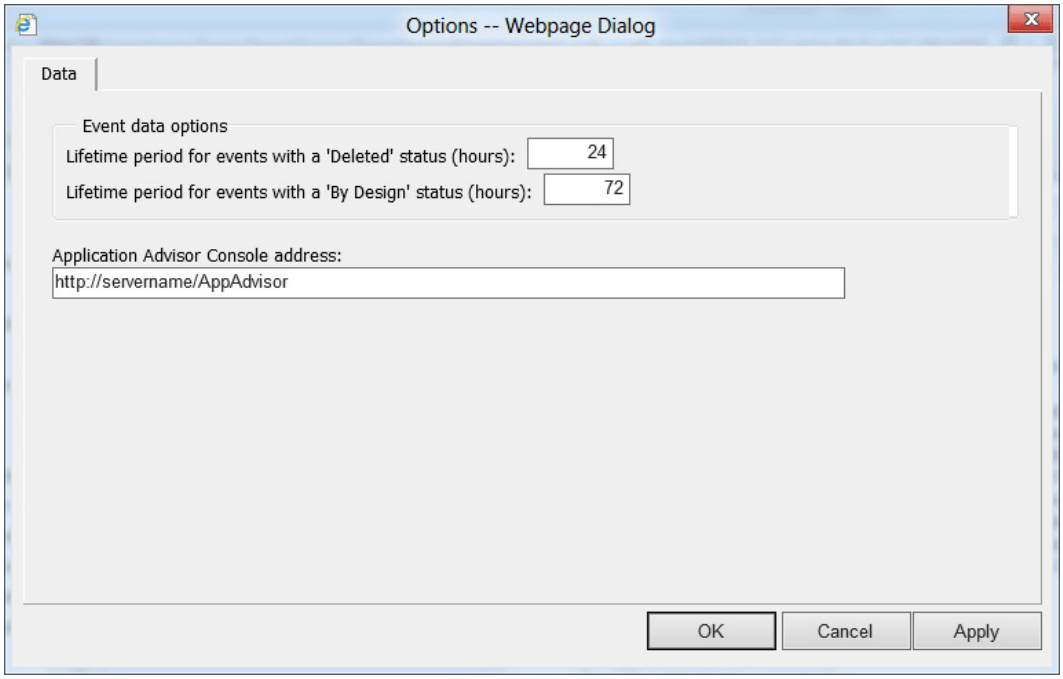
   Access to Application Diagnostics is controlled through the Application Monitoring Operator and Administrator roles. You must be a member of one of these roles to have

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**.

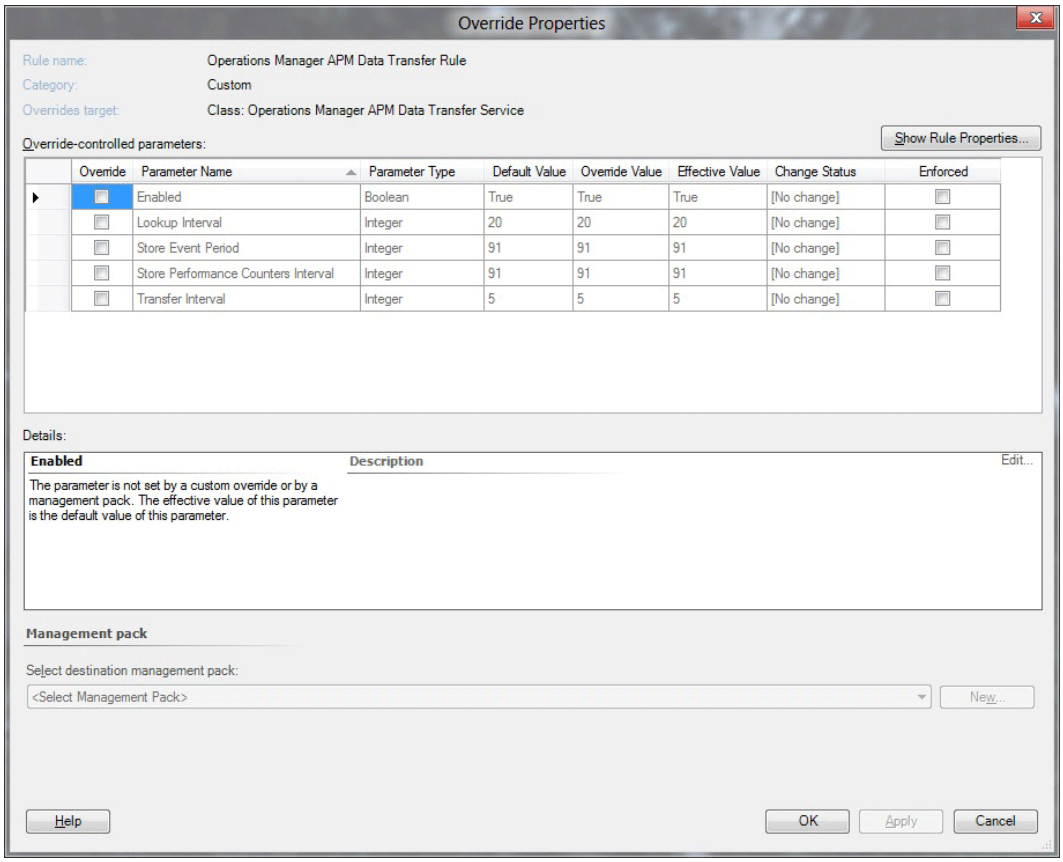
Using the Data Transfer rule to configure grooming settings for APM events and performance data from the Data Warehouse

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

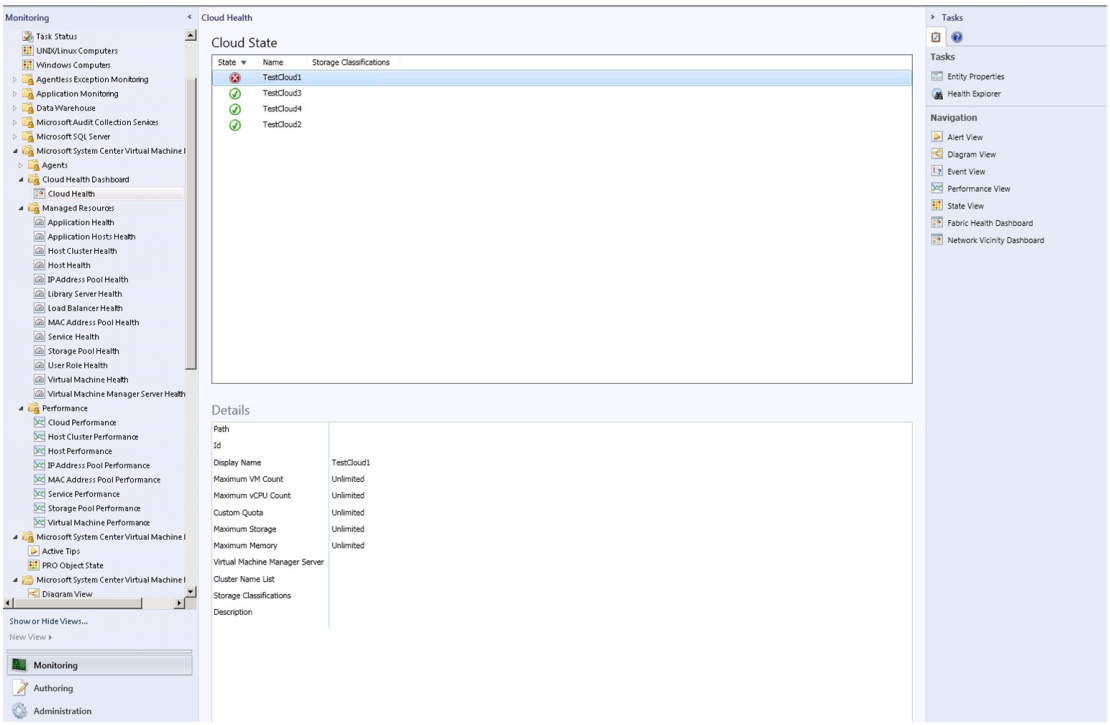
Getting Started with the Fabric Health Dashboard

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.

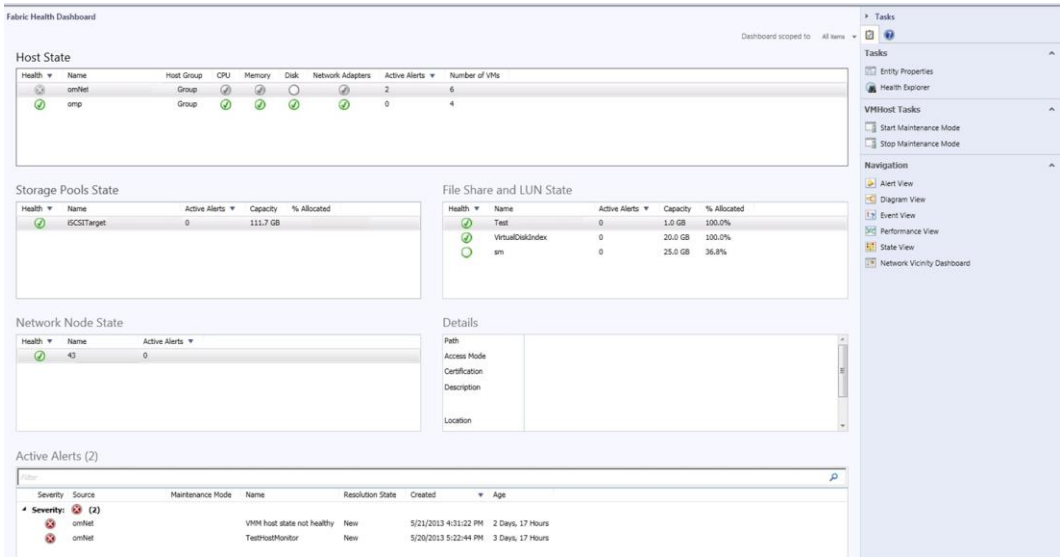
About the Fabric Health Dashboard

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

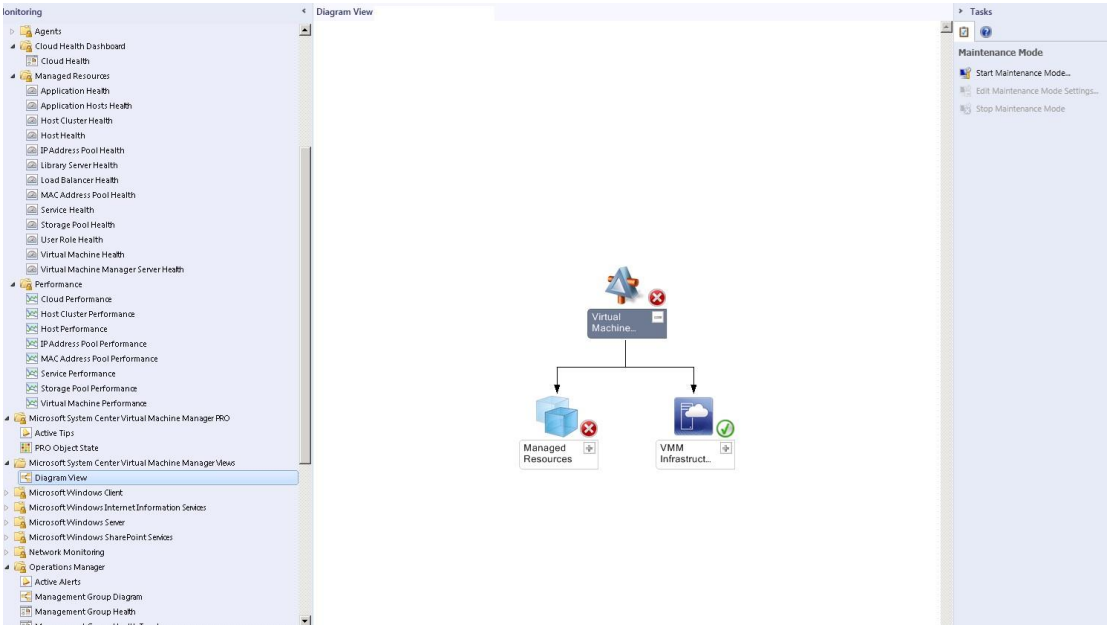
The Fabric Monitoring Diagram view gives you a diagram of the entire infrastructure and shows the health state of each part of the fabric. The Diagram view helps you answer questions, such as "What is the health of my entire fabric?" Improvements to the diagram ensure that health rolls up and that the 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 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	A.00.09.07l.003

Required Package	Description	Minimum Version
	Protocol	
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

Required Package	Description	Minimum Version
		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	0.9.8b-8.3.el5

Required Package	Description	Minimum Version
	Network Communications Protocol	
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
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
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

Required Package	Description	Minimum Version
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 Protocol	0.9.8 or 1.0
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 Deploy 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 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.

Vari-able	Definition	Registry Key	Entry Name
M	Maximum number of events queued in memory on the ACS collector	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdtServer\Parameters	MaxQueueLength
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	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdtServer\Parameters	StringCacheSize

Vari-able	Definition	Registry Key	Entry Name
	the ACS database. Size of the string cache on 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,	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdtServer\Parameters	PrincipalCacheSize

Variable	Definition	Registry Key	Entry Name
	expressed as the maximum number of entries 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

Counter	Description
	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

Counter	Description
	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

Parameter	Description
	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

Subparameter	Description
	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 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.

Subparameter	Definition
/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.
/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.

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.

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

Subparameter	Definition
	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 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

Statistic Parameter	Definition
	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.
/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

Subparameter	Definition
	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.
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

Viewing System Center Advisor Alerts

System Center Advisor is an online service that analyzes installations of Microsoft server software. With the latest preview version of Advisor and Update Rollup 2 of System Center 2012 SP1: Operations Manager, 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.

In previous versions of Advisor, the Advisor agent used a gateway to communicate with the Advisor service. When you use Advisor as an attached service in Operations Manager, the agent communicates directly with the management server, which in turn talks to the Advisor service.

You can continue to use Advisor as a standalone service, using the Advisor gateway for communication with the service; using Advisor as an attached service in Operations Manager simply extends the value of Advisor to Operations Manager.

Note
During the preview release of the Advisor connector, you cannot use Advisor to proactively monitor an Operations Manager gateway or management server that contains a Health Service agent that is multi-homed in a second management group.

You can learn more about Advisor, including the workloads that it analyzes, in the online help system, available at http://go.microsoft.com/fwlink/?LinkID=194601.

Use the following information to configure the Operations console so you can view Advisor alerts.

Pre-requisites

Before you can view Advisor alerts in the Operations console, ensure the following pre-requisites are met:

- System Center 2012 SP1: Operations Manager Update Rollup 2. This update needs to be applied to the management server, agents, and Operations console for the Advisor as an attached service scenario to work.

  If you have Microsoft Update enabled, this update will be automatically installed.
- If you want to view Advisor alerts about SharePoint Server 2010 or Lync Server 2010, you need to configure a Run As account. See Set the Run As Account for SharePoint for information about creating this account for SharePoint Server and Set the Run As Account for Lync Server for information for Lync Server.

  Note
  The Run As account you use must be a Windows account.

Configure the Operations console to display Advisor alerts

Use the following steps to configure the Operations console to view Advisor alerts.

1. Download the System Center Advisor Connector preview from http://go.microsoft.com/fwlink/?LinkId=311952. Extract the contents of the file (management packs) to a folder on your computer.
2. In the Operations Manager Operations console, import the management packs that you downloaded and extracted. For information about how to import a management pack, see How to Import an Operations Manager Management Pack.
3. On the Administration workspace, click **System Center Advisor** and then **Advisor Connection** in the navigation pane to open the Advisor page in the console.
4. Click **Register with Advisor**.
5. Follow the instructions in the Advisor Onboarding wizard to complete your configuration.
6. If your environment requires the use of a proxy server to communicate with the internet, configure the proxy server. See Firewall Information for System Center Advisor for details on the domains and URLs that need to be accessible through the firewall.

7. Add computers to analyze with Advisor. Click **System Center Advisor** and then **Advisor Managed** in the navigation pane. Click **Add a Computer**, and then follow the instructions in the UI.

   Important
   If you have already installed an Advisor gateway or agent on a computer that you want to view through the Operations console, you need to uninstall System Center Advisor (through Add/Remove Programs) before you can do so.

View Advisor alerts

You can view Advisor alerts on the Monitoring workspace. Open the Monitoring workspace, click **System Center Advisor**, and then click **Active Alerts** to see the alerts. Click any alert to view detailed information.

An Advisor alert contains information about the computer or instance where the alert was discovered and remediation information to address the issue. To view the remediation information, in the **Alert Details** section, click **View additional knowledge**. This will open a KB or TechNet article about the issue detected.

You can also learn more about Advisor from an alert by clicking the **Learn more about Advisor** link in the **Knowledge** section.

Manage Advisor alerts

You can view, close, or ignore an Advisor alert through the Operations console.

To close an alert, click **Close Alert** in the Advisor Tasks list.

To ignore an alert, click the specific alert in the results pane, and then click **Ignore Alert**. You can manage alerts, including those that you have ignored, by clicking **Manage Alert Rules**. For more information about ignoring Advisor alerts, see Ignore an Alert in the Advisor online help system.

View configuration information

In addition to viewing alerts from Advisor, you can also view the configuration information that Advisor collects about the computers listed as “Advisor Managed.” To view configuration information, from the System Center Advisor page on the Monitoring workspace, click **View Configuration** in the Advisor Tasks list.

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:

<table>
<tr><td colspan="3">Toolbar: search, find, scope</td></tr>
<tr><td rowspan="4">Navigation pane: displays a navigation tree that changes when you click a navigation button.</td><td>Results pane: displays information based on the item you select in the Navigation pane</td><td rowspan="4">Tasks pane: displays the actions that are available. The actions that are displayed depend on the information in the Navigation and Results panes.</td></tr>
<tr><td rowspan="3">Details pane: displays information about the item selected in the Results pane</td></tr>
<tr><td></td></tr>
<tr><td>Navigation buttons</td></tr>
</table>

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

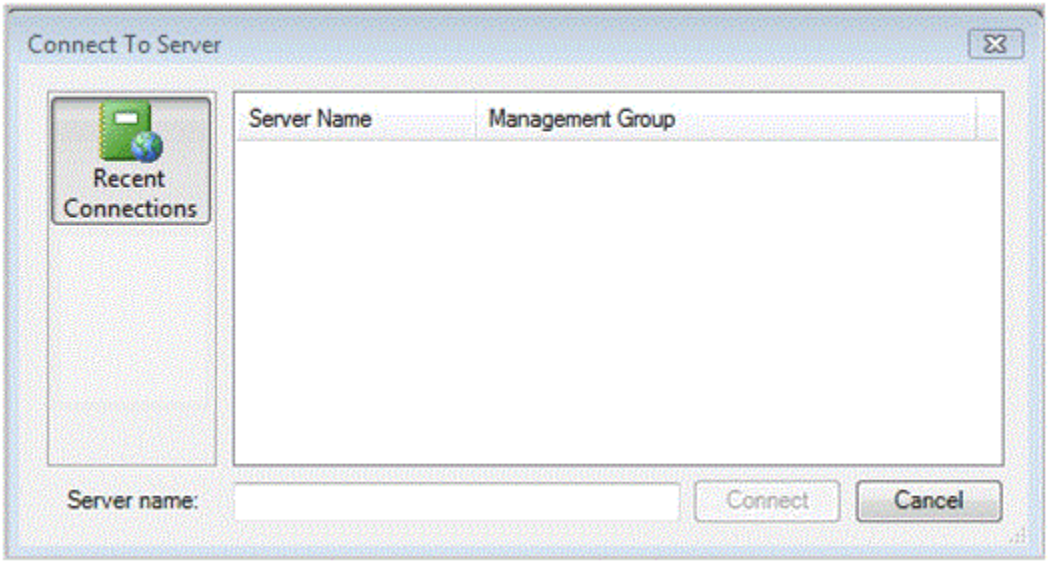
In the Operations console, you can change the navigation buttons into small icons and increase the space available in the navigation pane by clicking on the top border of the navigation buttons and dragging downward. You can also hide and reveal the navigation and task panes.

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.



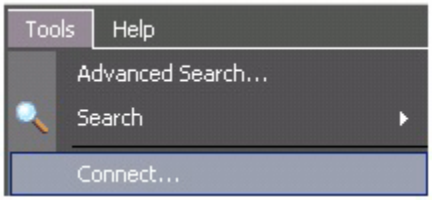
To connect an Operations console to a management server

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

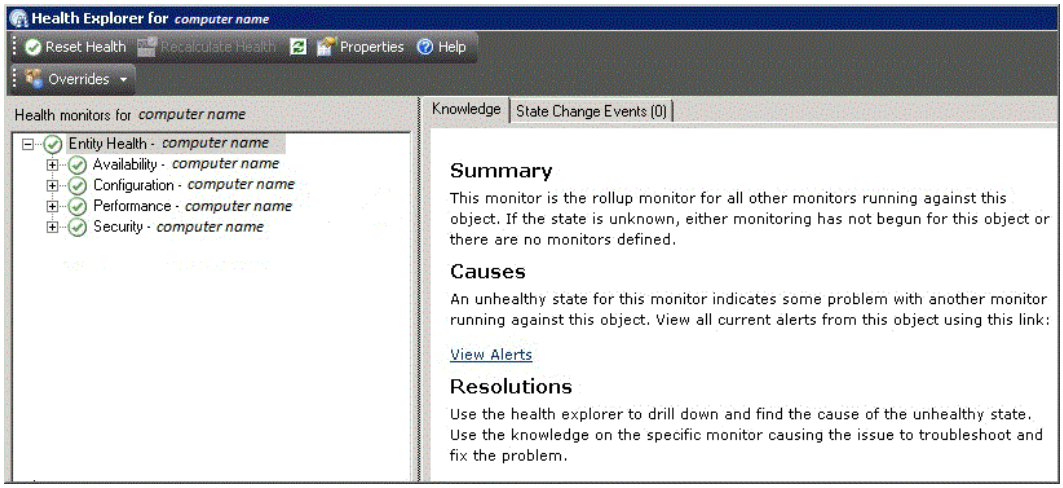
Using Health Explorer in Operations Manager

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)

Icon	Meaning
	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	• 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

Item	Use	For more information
	computer to critical. • Override the Management Group Manual Agent Installs setting and configure a management server to reject or put in 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.	in the Deployment Guide
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 in the operational database.	Maintenance of Operations Manager
Privacy	To modify the settings for the	Sending Data to Microsoft in

Item	Use	For more information
	following programs: • Customer Experience Improvement Program (CEIP) • Operational Data Reporting • Error Reporting	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

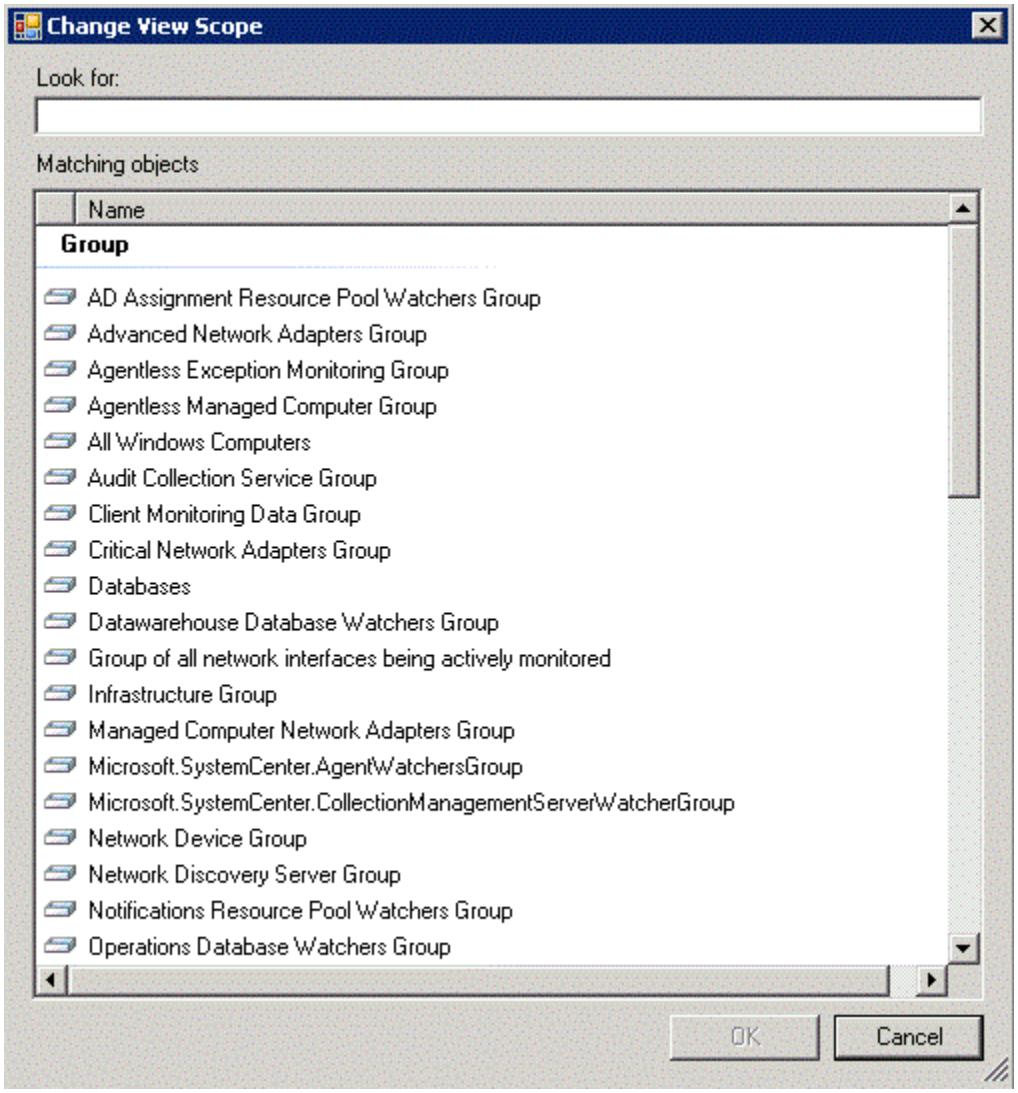
Filter	When to use	For more information, see
Time	Use to limit the data displayed to only that data (such as alerts) that has been generated within a defined time frame.	How to Change the Time Criteria

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 • 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

Object type	Criteria associated with the object type
	• 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 • 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

Object type	Criteria associated with the object type
	• 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

To find	Use this object, condition, and value
	group/Unix Computer Group

See Also

Finding Data and Objects in the Operations Manager Consoles

Using Advanced Search

Using Views in Operations Manager

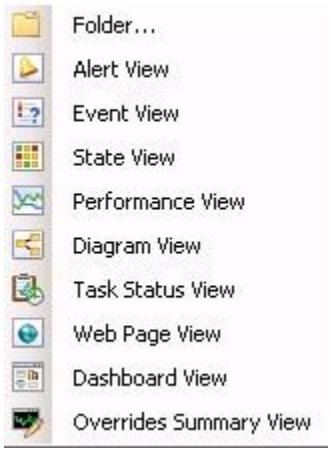
For a description of the differences between dashboard views and reports, see this System Center Operations Manager blog post.

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.

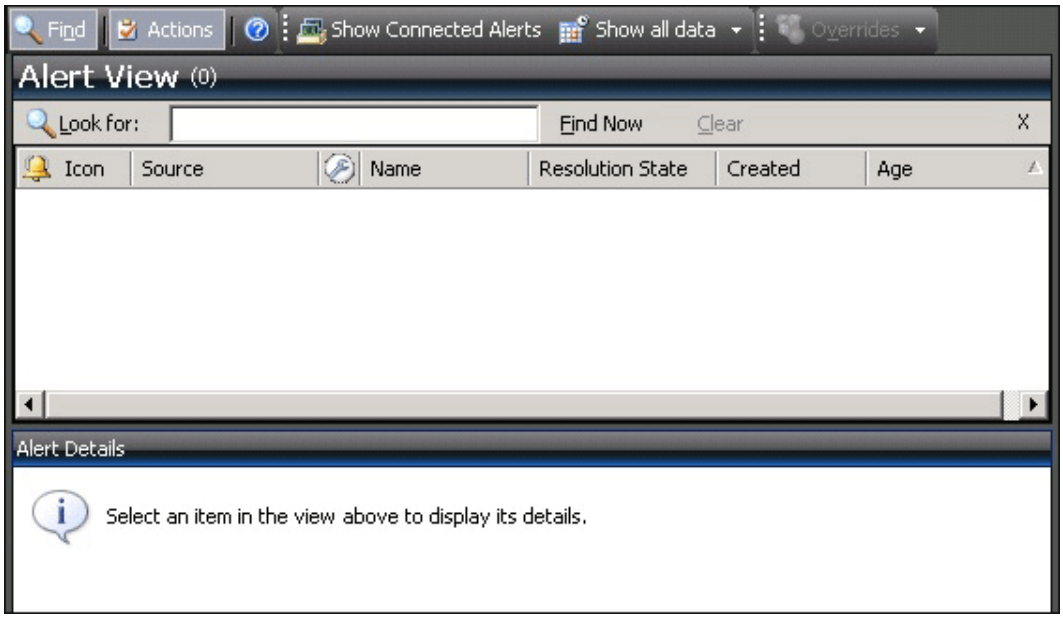


For more information on specific view types, see:

- 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

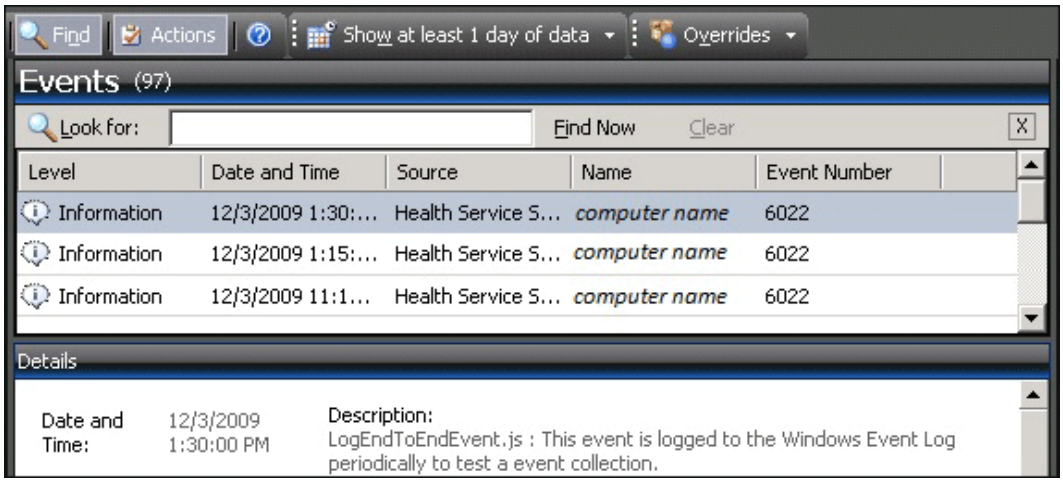
Alert View Type

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.



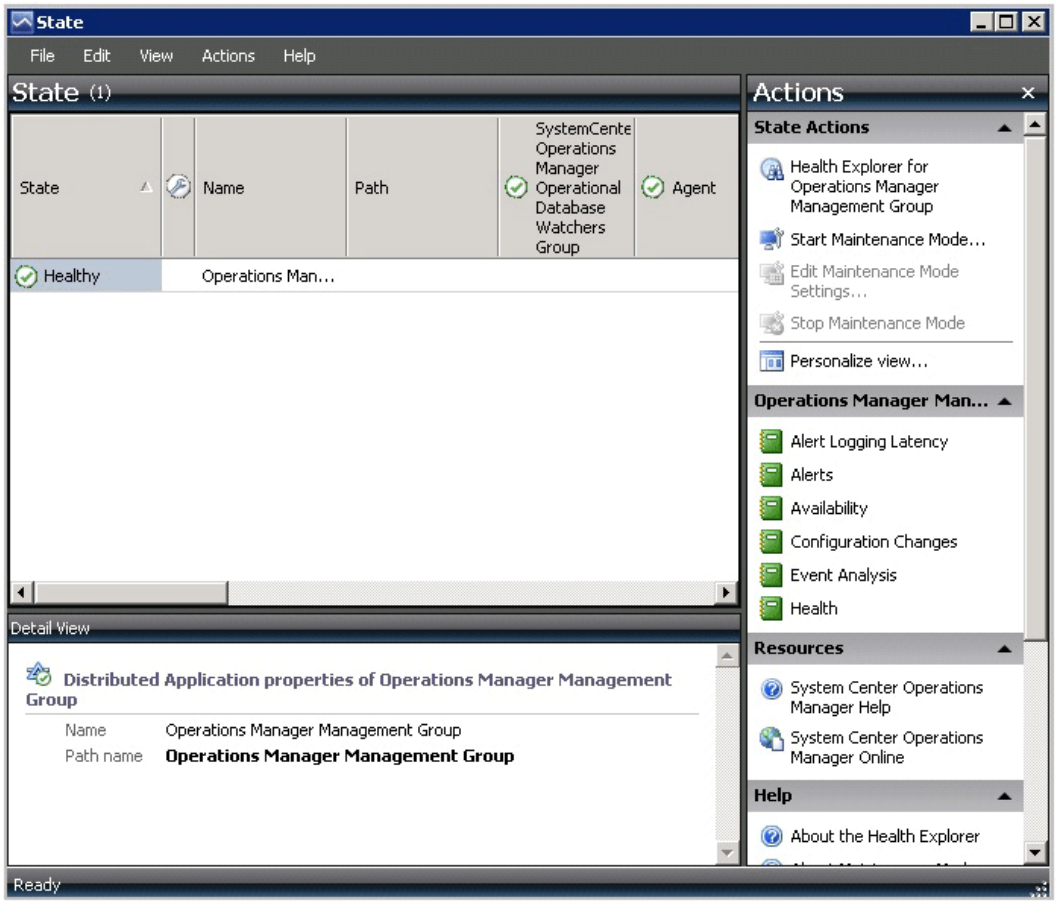
Event View Type

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](#).

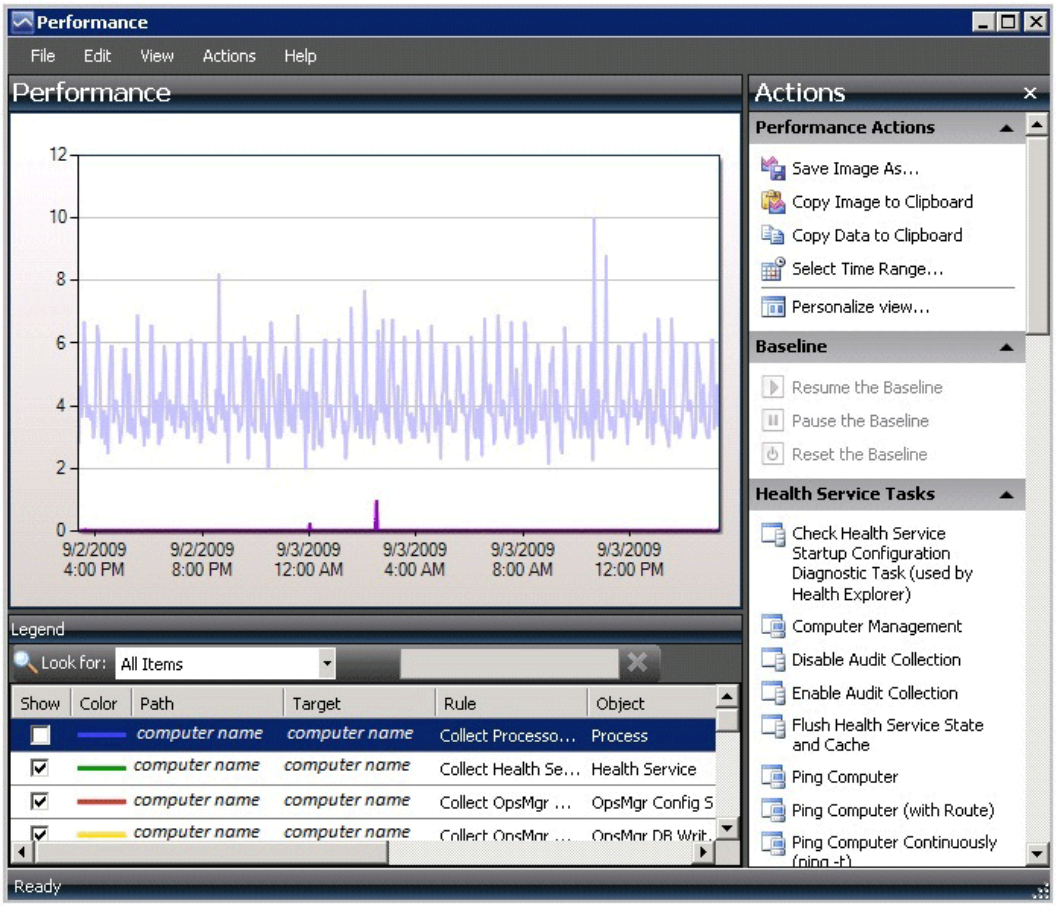
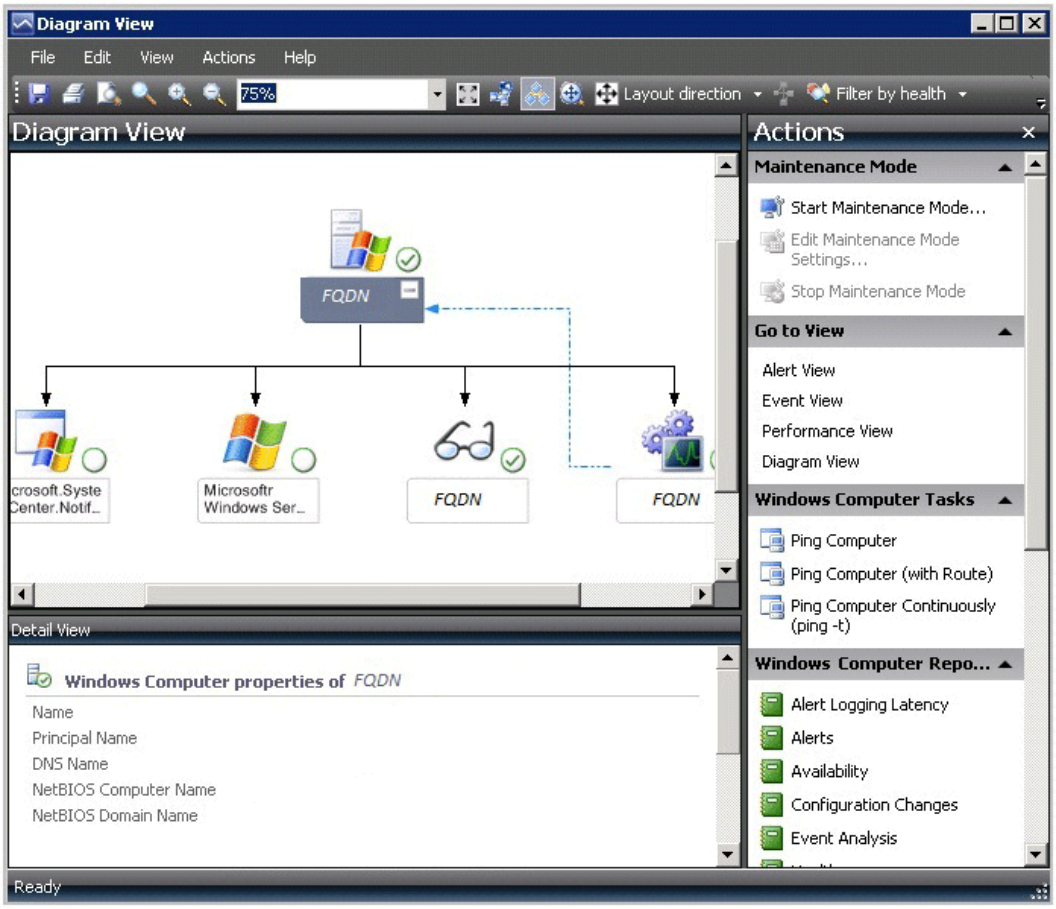


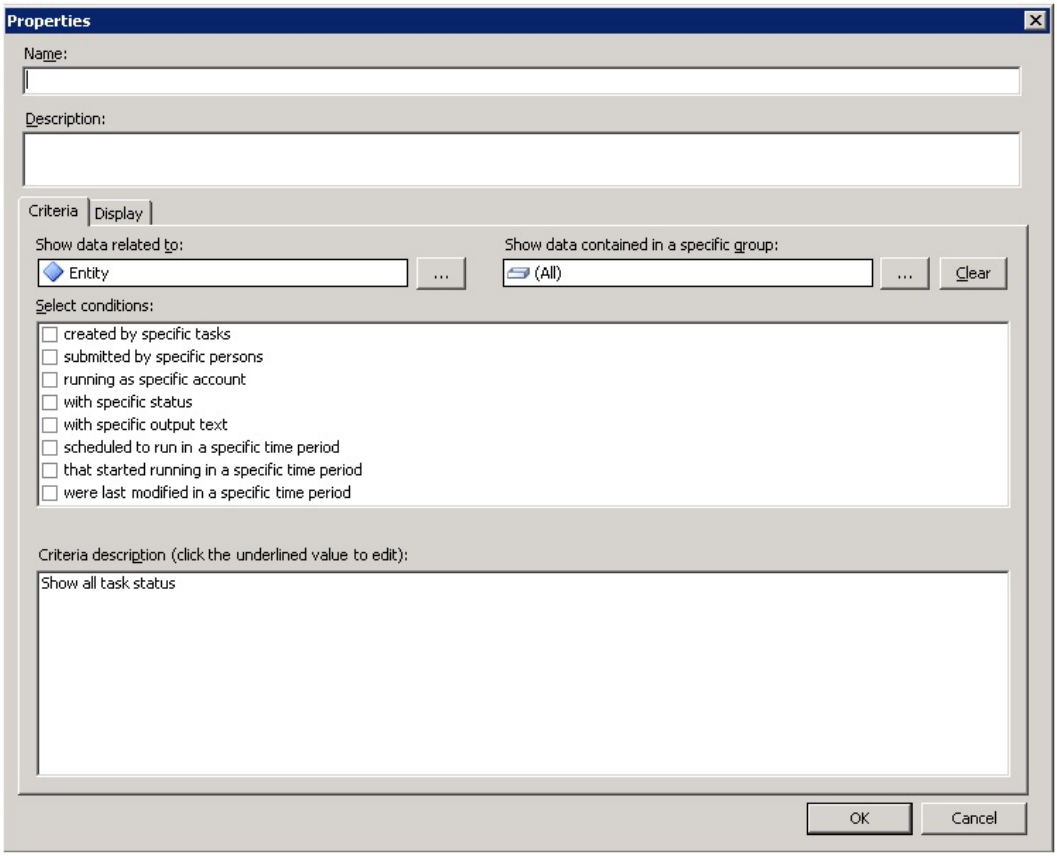
Diagram View Type

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.

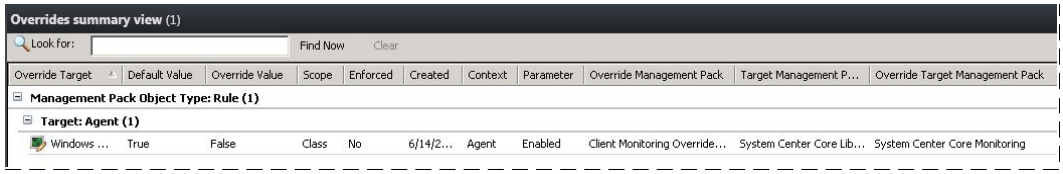
Web Page View Type

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.

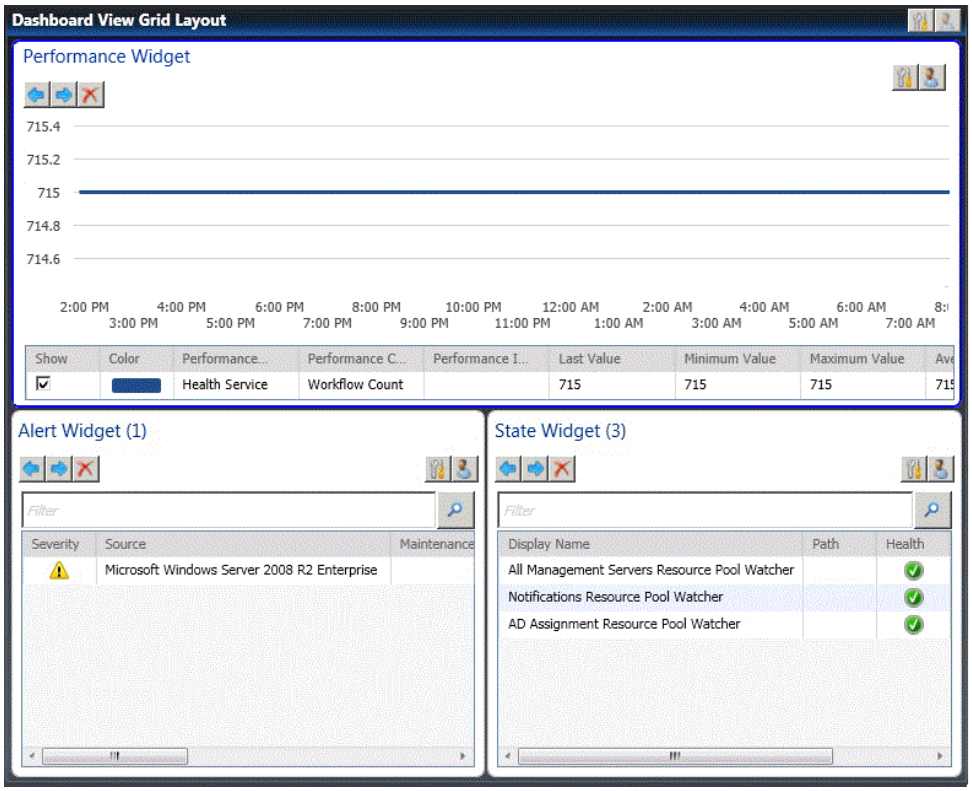


Dashboard View Type

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

View or View Folder	Description
	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… For more information, see Using Health

View or View Folder	Description
	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)

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.

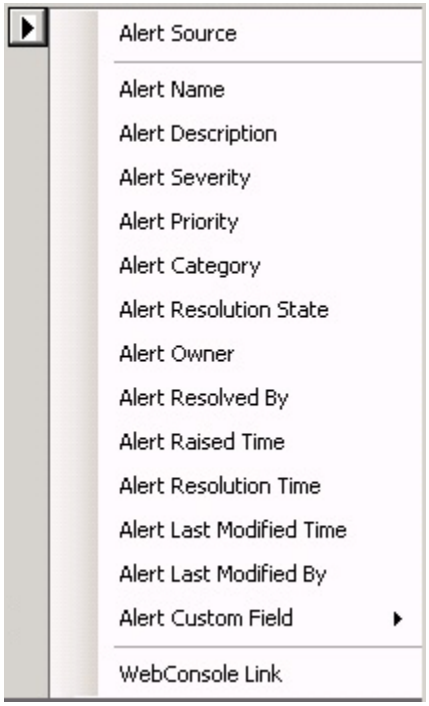
Channel type	Default notification format
Email	**Subject**: Alert: *alert name* Resolution state: *new or closed* Alert: Source: Path: Last modified by: Last modified time: Alert description: Alert view link: Notification subscription ID generating this message:
Instant message (IM)	Alert: *alert name* 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.

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

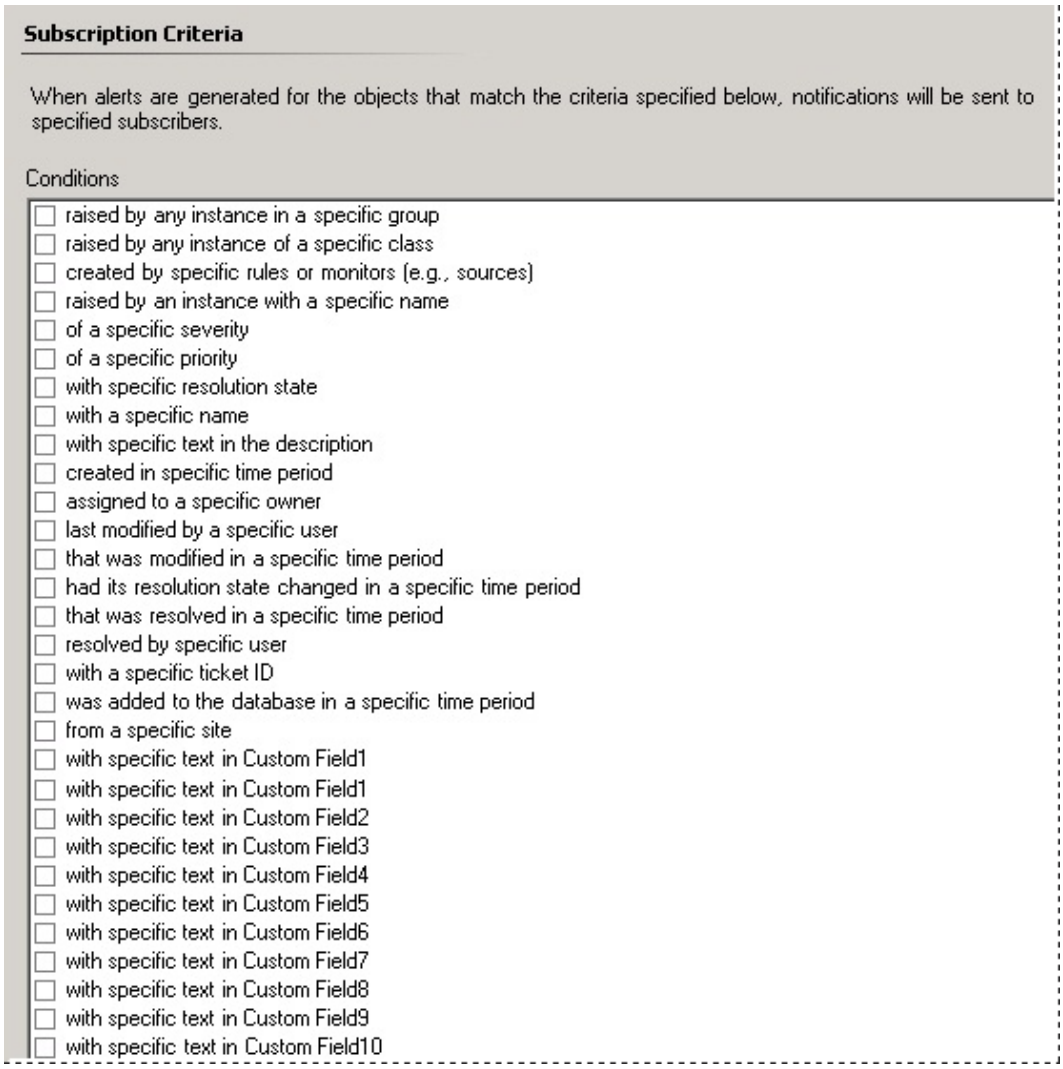
How to Enable an Email Notification Channel

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 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

Report	Description
	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.
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.

Report	Description
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 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.
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.

Report	Description
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 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	This report provides performance analysis for

Report	Description
Resources Analysis	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.
(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	This reports highlights servers that have the

Report	Description
Utilization Analysis	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

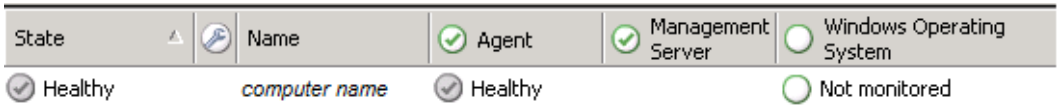
Scheduling Reports

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

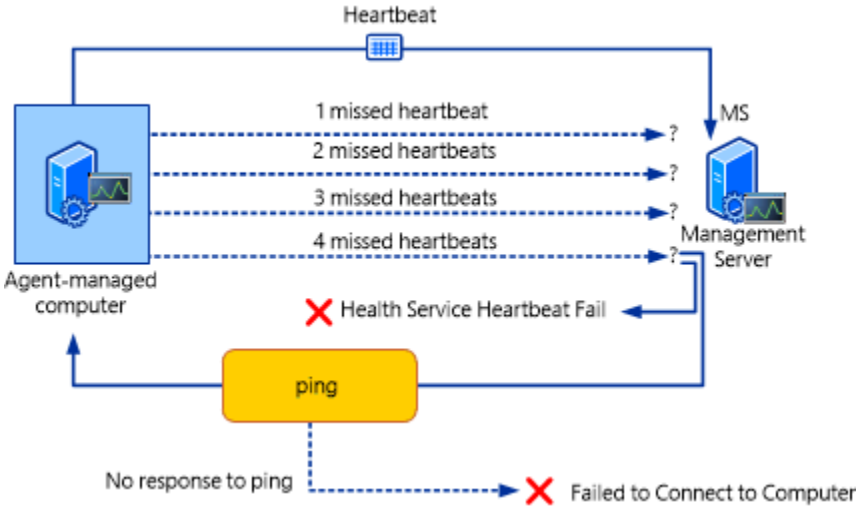
- TechNet Library main page for Operations Manager
- Operations Guide for System Center 2012 - Operations Manager
- Subscribing to Alert Notifications
- General Tasks in Operations Manager

- 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.



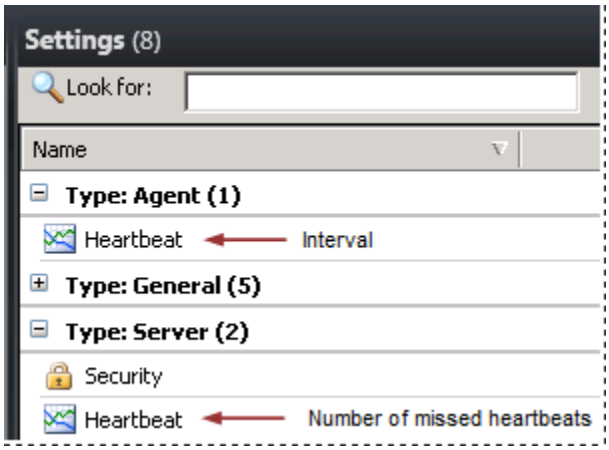
When you see both alerts, you know the computer cannot be contacted by the management server. When you see only the heartbeat failure alert, you know the computer can be contacted but there is a problem with the agent. Both alerts are closed automatically when heartbeats resume.

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]

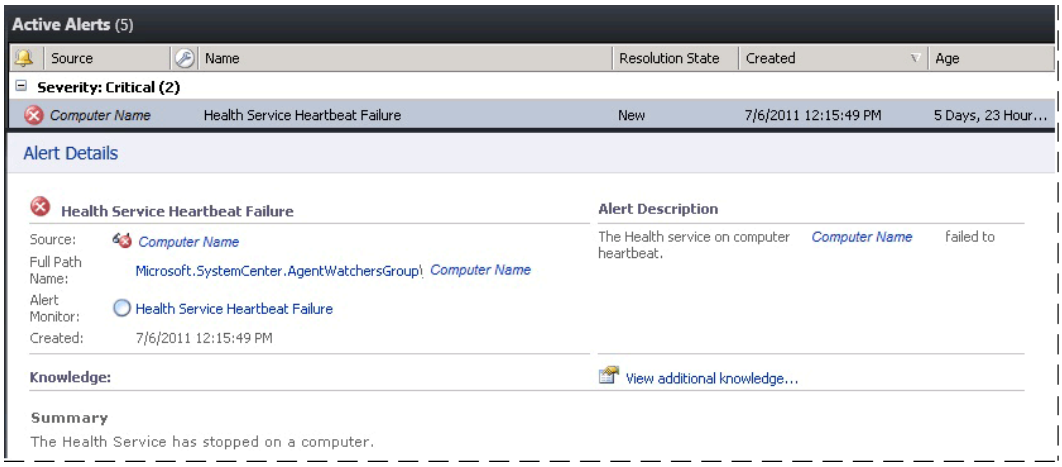
[Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)]

[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 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

Tab	Description
	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 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

Tab	Description
	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.
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

Diagnostic and Recovery Tasks

Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

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

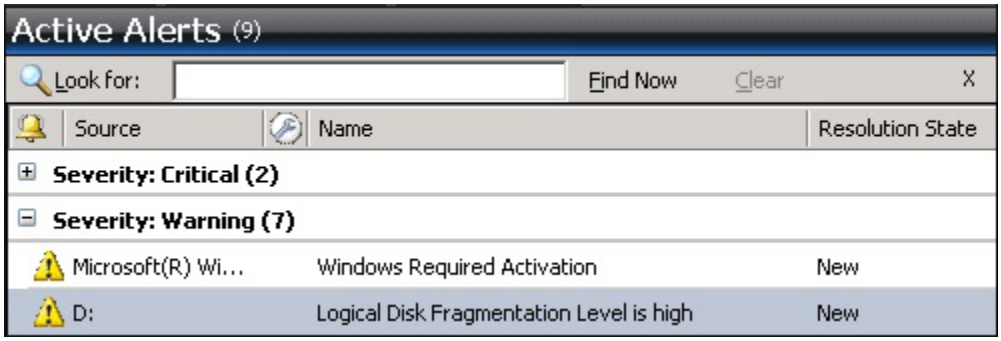
Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

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

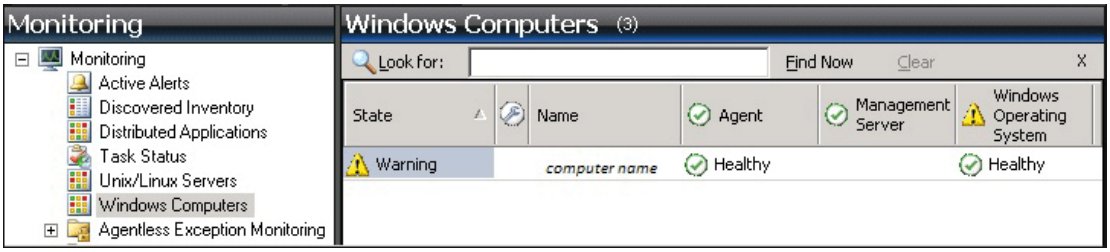
1. Click the alert.



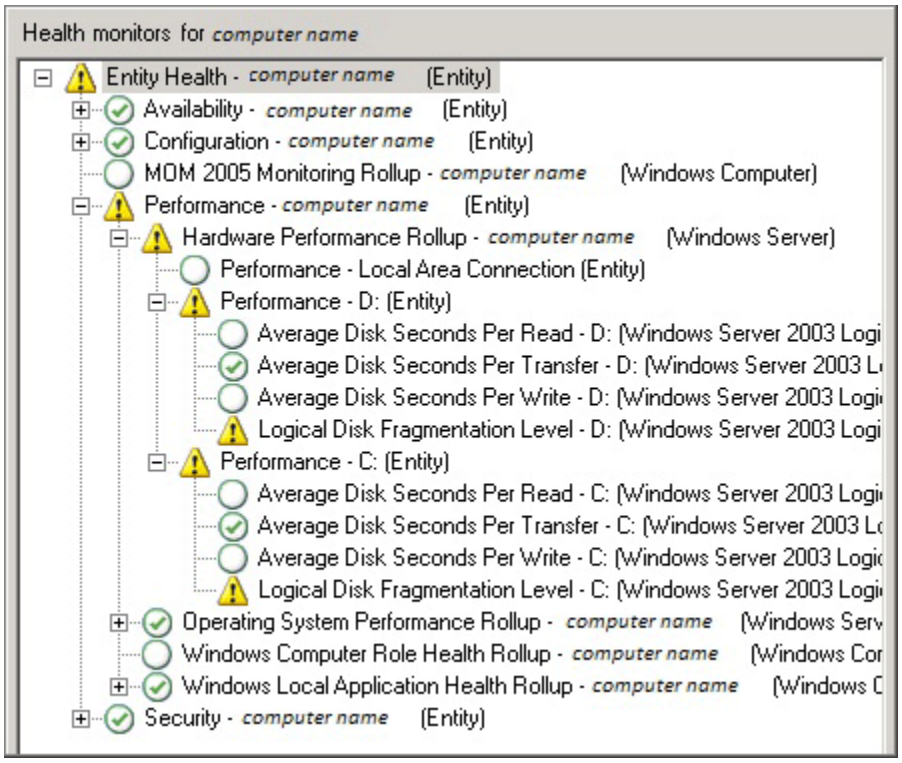
2. Look in the **Details** section for the **Path**.

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

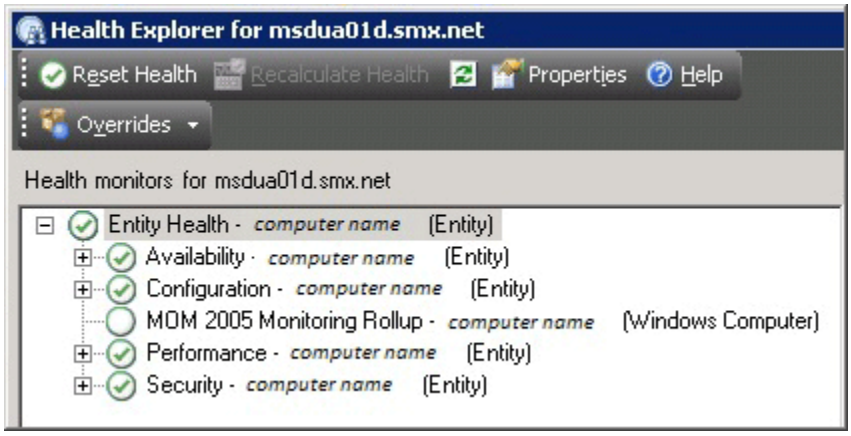
Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)

Using Health Explorer to Investigate Problems

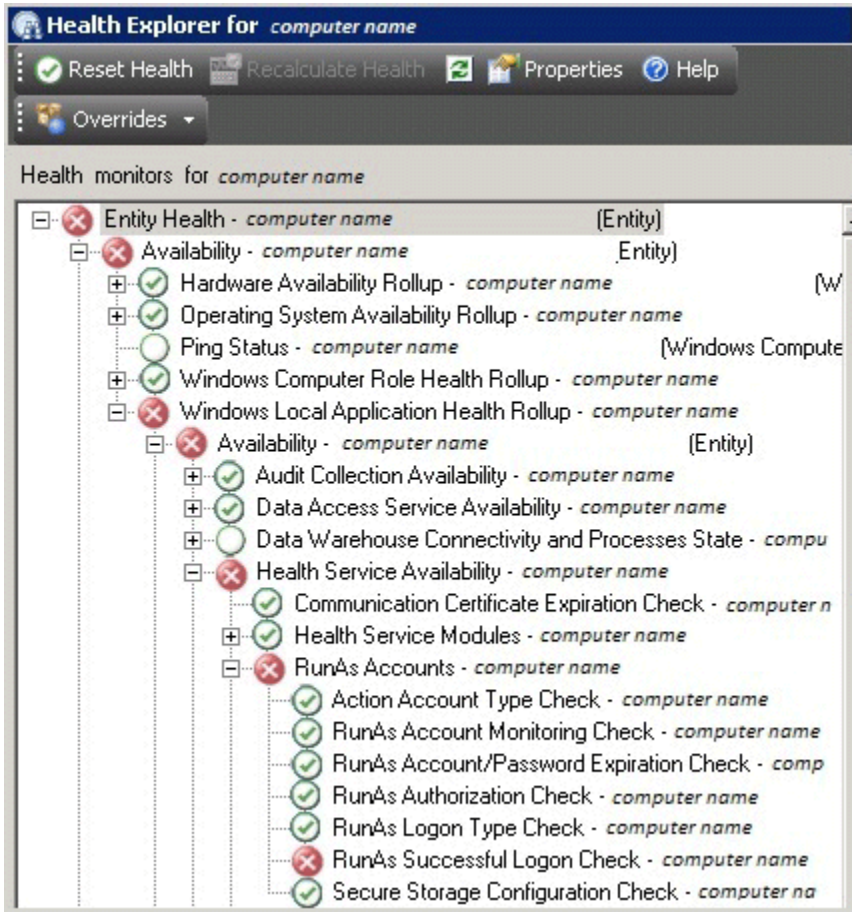
Use Health Explorer to find out which monitor is reacting and to review knowledge about the monitor and possible causes for actions related to it. In the **Active Alerts** view, click the alert to highlight it. The Health Explorer link under **Alert Actions** in the **Tasks** pane becomes active.

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.

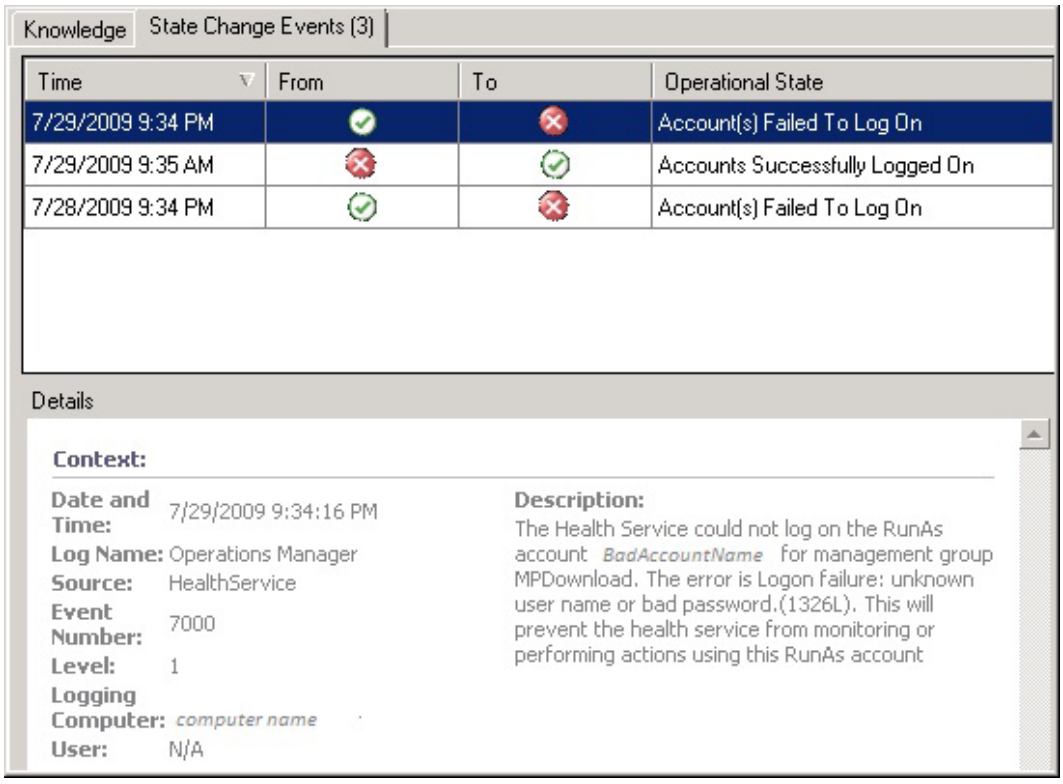
The following illustration shows monitors in a healthy state:



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]

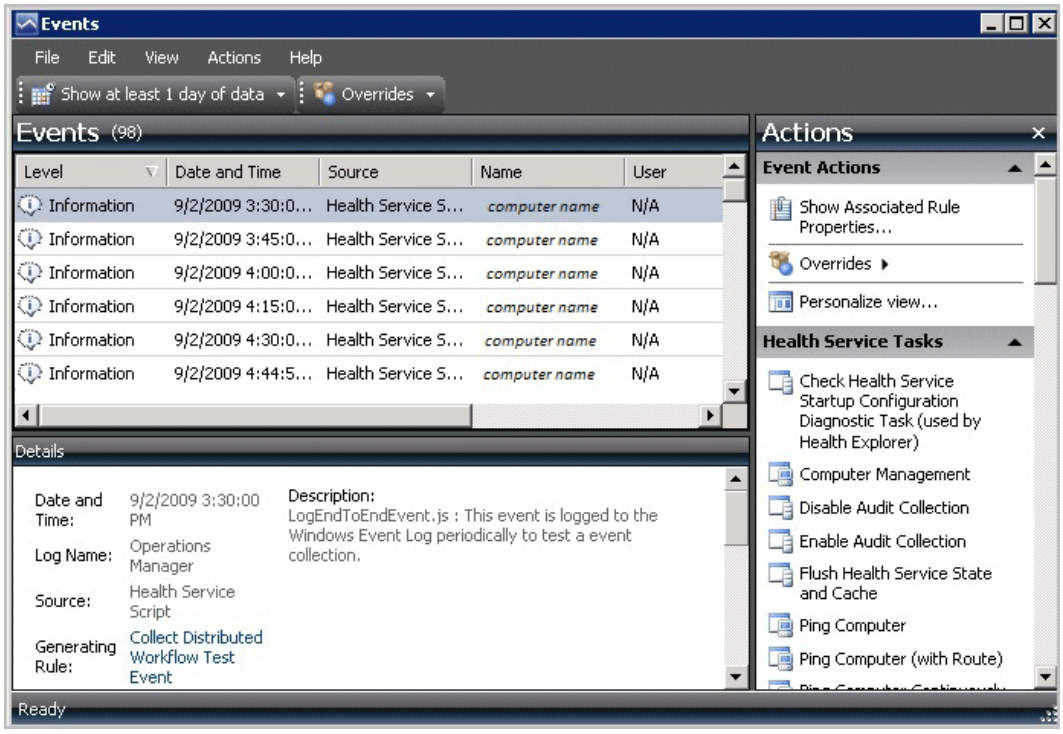
[Viewing and Investigating Alerts for .NET Applications (Server-side Perspective)]

[Using Health Explorer in Operations Manager]

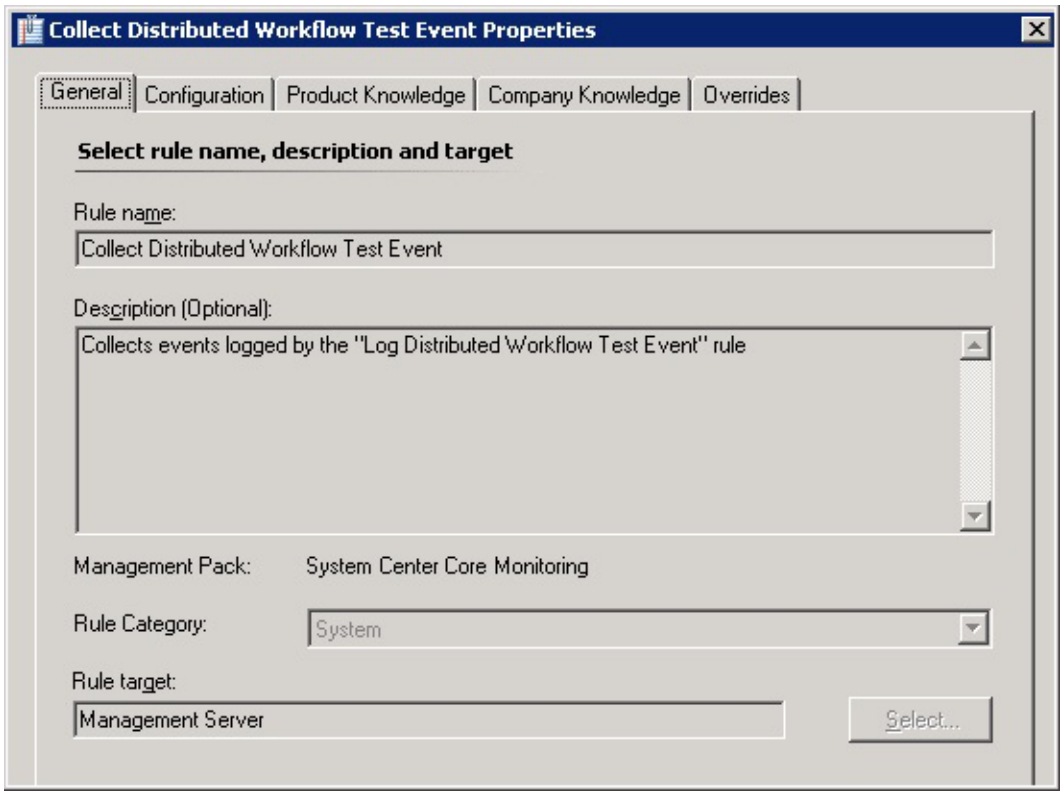
Using Event View to Investigate Problems

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)

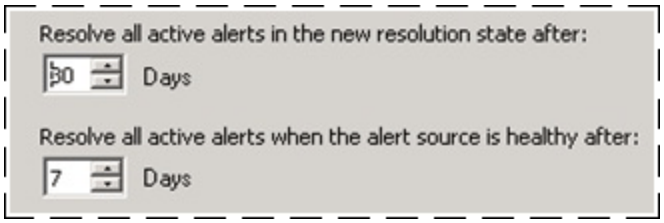
How to Configure Automatic Alert Resolution

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).

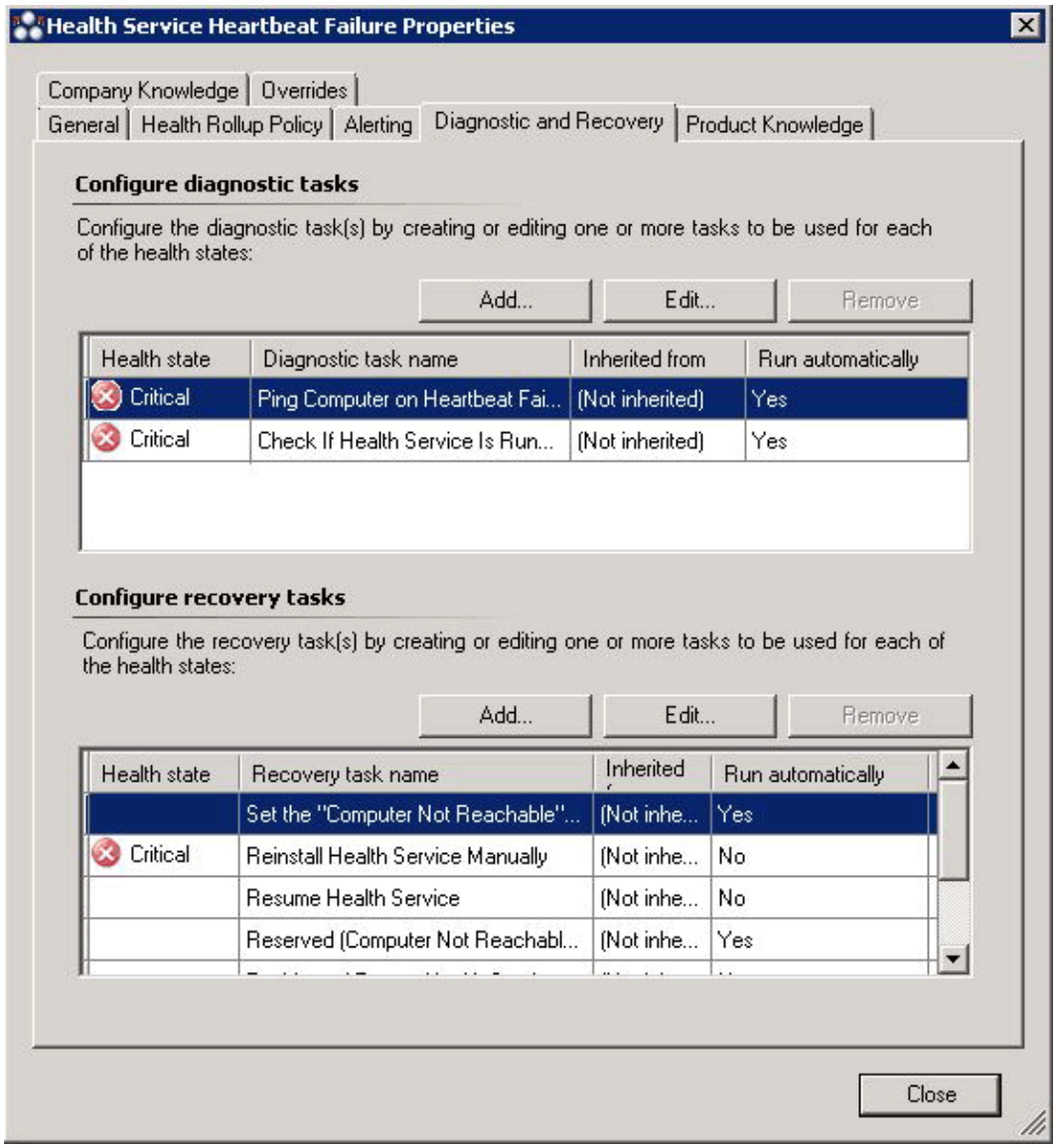
- **Set the "Computer Not Reachable" monitor to success because the "Ping Computer on Heartbeat Failure" diagnostic succeeded**

  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

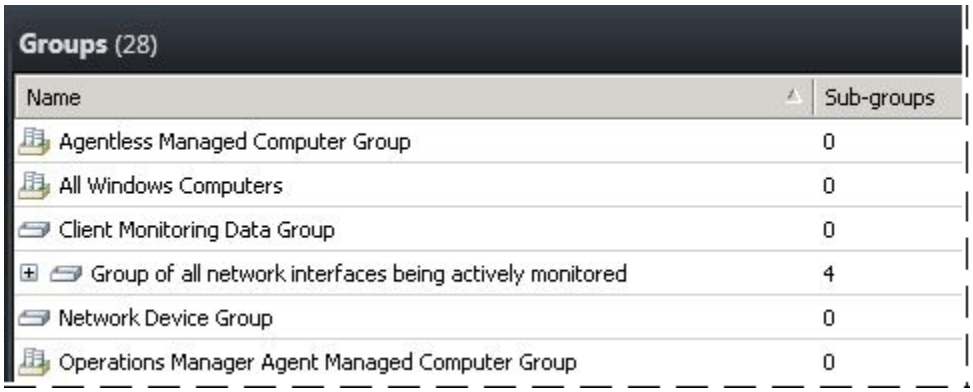
Creating and Managing Groups

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

How to Create Groups in Operations Manager

You can use groups in System Center 2012 – Operations Manager to scope views, reports, overrides, and alert notifications. You create groups in the **Authoring** workspace in the Operations console.

In the Operations console, you can only create instance groups. The difference between instance groups and computers groups 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.

To create a group based on a hosting relationship, such as all computers that are running SQL Server, you must use the Authoring console or work directly in the XML of a management pack.

The most common objects you will place in your groups are **Windows Computer** objects. The most common way to dynamically assign computers to the groups is by using a *property* of the **Windows Computer** class. For example, **Organizational Unit** is a property of the **Windows Computer** class, so you can create a group that makes all computers in a specific organizational unit members of the same group. The following image shows the properties of an object in the **Windows Computer** class, which you can view in the details pane of the **Monitoring** workspace by selecting the **Windows Computers** state view.

You can assign both explicit and dynamic members in the same group definition, and you can exclude explicit members. For examples of dynamic group queries and formulas, see Operations Manager Dynamic Group Examples.

To create a group in Operations Manager

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 **Authoring**.
3. Right-click **Groups**, and then click **Create a new Group** to start the Create Group Wizard.
4. On the **Enter a name and description for the new group** page, do the following:
   a. Type the **Name** for the group.
   b. Optionally, type the **Description** for the group. A description of the group membership makes it easier to select the right group for views, overrides, and so forth.
   c. Select a **destination management pack** from the list, or click **New** to create a management pack with the Create a Management Pack Wizard.
   d. Click **Next**.
5. On the **Explicit Members** - **Choose Members from a List** page, you can add explicit objects to the group or click **Next** to continue to the **Dynamic Members** configuration. To add explicit group members, click **Add/Remove Objects** and then perform the following

steps:

a. In the **Search for** list, select an object type, such as **Windows Computer**.

b. Optionally, in the **Filter by part of the name** box, type all or part of the object name, and then click **Search**.

c. In the **Available items** box, select the desired objects, click **Add**, and then click **Next**.

6. On the **Dynamic Members** - **Create a Membership Formula** page, you can add a dynamic membership formula to the group or click **Next** to continue to the **Subgroups** page. To add a dynamic membership formula, click **Create/Edit rules** and then perform the following steps:

   Warning

   This procedure tells you how to create a query for Windows computers based on NetBIOS computer name.

   a. In the **Query Builder** dialog box, leave the default **Windows Computer** and click **Add**.

   b. In the **Property** list, select **NetBIOS computer name**.

   c. In the **Operator** list, select **Contains**.

   d. Set **Value** to part of the name of the computers you want in the group, such as **NY** or **MKTG**.

      Note

      Click **Insert** to add an **Expression** or group expressions with **OR** or **AND** operators. Repeat the preceding steps to add additional object types to the rule.

   e. Click **OK**, review the **Query formula**, and then click **Next**.

7. On the **Choose Optional Subgroups** page, either click **Next** to not add groups to the group, or click **Add/Remove Subgroups** to add groups, for example.

   a. In the **Group Selection** dialog box, in **Filter by part of name**, you can optionally type part or the all of the group's names, and then click **Search**.

   b. In the **Available items** text box, select the desired groups, click **Add**, click **OK**, and then click **Next**.

8. On the **Excluded Members** - **Specify Exclude List** page, click **Finish** to not exclude objects from the group, or click **Exclude Objects**, and then perform the following steps:

   a. In the **Object Exclusion** dialog box, from the **Search for** list, select an object type, such as **Windows Computer**.

   b. Optionally, in the **Filter by part of the name** box, type all or part of the object name, and then click **Search**.

   c. In the **Available items** text box, select the objects you want to exclude, click **Add**, click **OK**, and then click **Finish**.

   Note

   It can take approximately one minute to populate the membership of a group.

See Also

Creating and Managing Groups

Define a Scope Using Operations Manager Groups

Using Classes and Groups for Overrides in Operations Manager

How to View Group Members, State, and Diagram

How to Create Subscriptions Using Classes and Groups

Guidance for Scoping and Targeting Views

How to View Group Members, State, and Diagram

Use the following procedure in System Center 2012 – Operations Manager to view the objects that are members of a specific group.

To view members, state, and diagram of a group

1. In the **Authoring** workspace, click **Groups**.
2. In the results pane, click the group you want to view.
3. In the **Tasks** pane, click:
   - **View Group Members** to view a list of all members of the group with the health state of each member.
   - **View Group State** to view a state view of the group.
   - **View Diagram** to view a diagram of the group.

See Also

Creating and Managing Groups

Define a Scope Using Operations Manager Groups

Using Classes and Groups for Overrides in Operations Manager

How to Create Groups in Operations Manager

How to Create Subscriptions Using Classes and Groups

Guidance for Scoping and Targeting Views

Running Tasks in Operations Manager

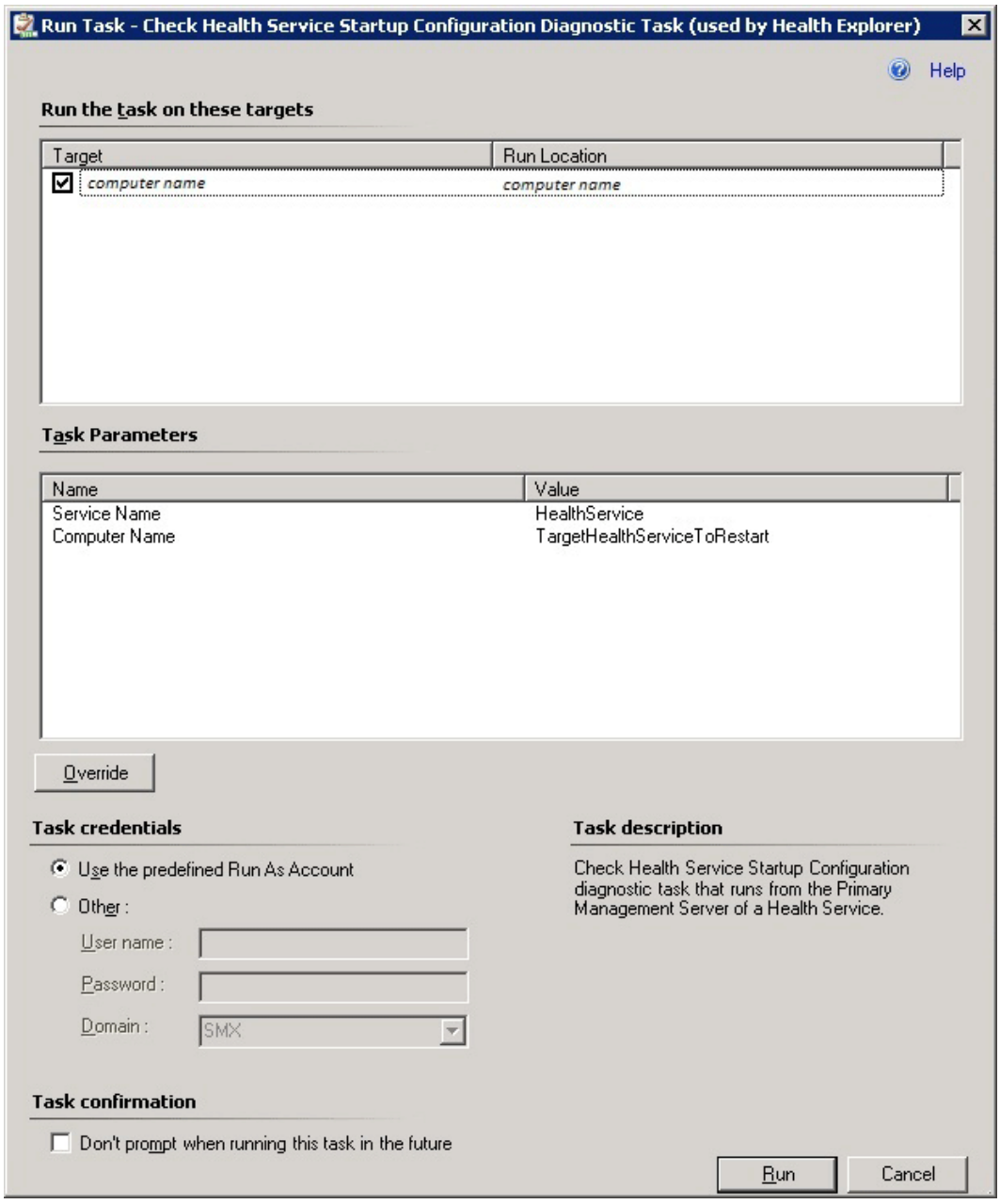
In the System Center 2012 – Operations Manager Operations console, the **Tasks** pane provides links to tasks. A task is a user-initiated action from the Operations console that is run on an Operations Manager agent. The tasks that are available depend on the management packs that are installed. For 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.

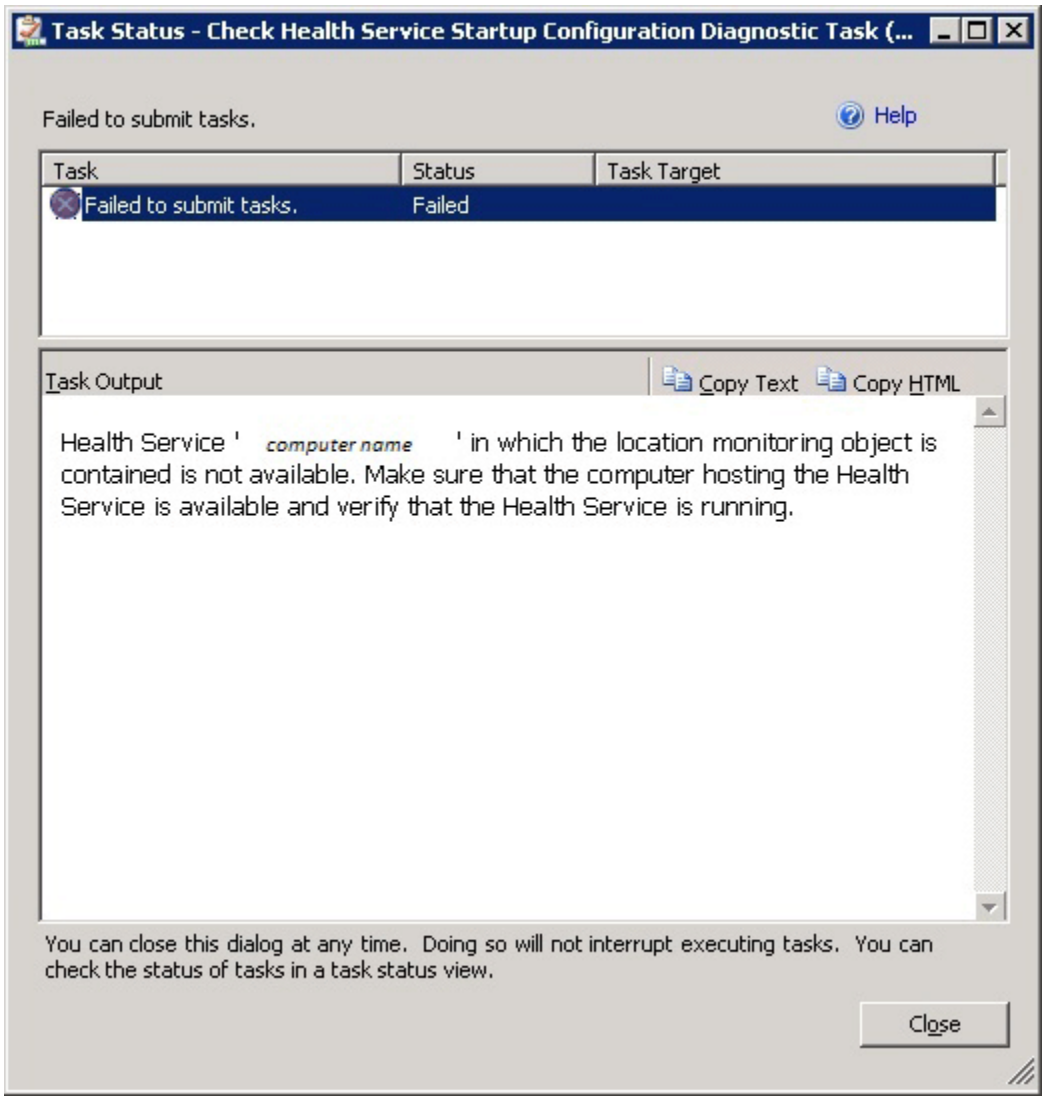
Click an alert or object to see tasks for that alert or object. Click a task to run the task.

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.

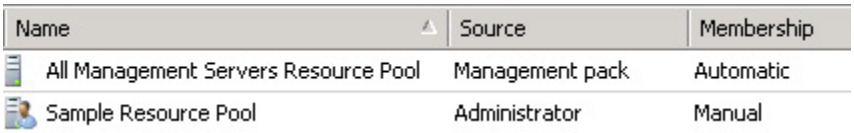
To create a resource pool

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.



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

Monitoring the Health of the Management Group

System Center 2012 – Operations Manager introduces a new dashboard view that provides a comprehensive picture of the health of your management group. The dashboard tries to answer the question, “do I need to do anything?”

The **Management Group Health** view allows you to see at a glance the health state of all management group functions, such as resource pools, and the management group infrastructure, such as management servers. It also shows you recent agent health state including gray agents, agent configuration for agents pending management, and agent versions.

You can display **Management Group Health** on a SharePoint site by using the Operations Manager Web Part, giving all authorized users a useful summary of management group status. For more information, see Using SharePoint to View Operations Manager Data.

Management Group Health automatically refreshes every 15 minutes by default. To manually refresh the view, right-click the view and click **Refresh**. It may take some time before the dashboard starts to show data. The agent data is recalculated every 15 minutes, and not when you refresh the dashboard.

This topic describes the specific information you will see in each cell of the **Management Group Health** dashboard view.

Management Group Functions

Management Group Functions shows you the health state of any of the following functions that are installed in your management group:

- Agentless exception monitoring
- Audit collection services
- System Center Data Access service group
- System Center Management service group
- Network discovery
- Resource pools
- Web user interfaces (web console and reporting web site)

You can open Health Explorer, alert view, diagram view, event view, performance view, and state view for any of the functions listed. To open a different view, right-click the display name for the function, and click **Health Explorer** or **Navigation**.

Management Group Infrastructure

Management Group Infrastructure shows you the health state of any of the following infrastructure features that are installed in your management group:

- Operational database
- Data warehouse database
- Management group
- Management servers
- Gateway servers

- Agents

You can open Health Explorer, alert view, diagram view, event view, performance view, and state view for any of the features listed. To open a different view, right-click the display name for the feature, and click **Health Explorer** or **Navigation**.

Agent Health State

Agent Health State displays a graph of health states for all agents over the past 7 days.

Note

The screenshot for **Agent Health State** displays 9 hour's worth of data. As additional data is collected, the scale will compress to show a maximum of 7 day's worth of data.

The graph captures all possible agent states, including "unavailable", or "gray", agents. It is possible to unselect health states, if you only want to focus on certain health states.

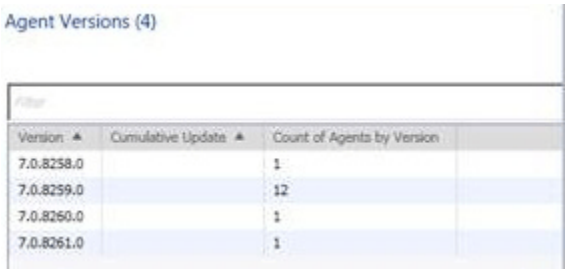
Agent Configuration

In **Agent Configuration**, you can see how the status of agents in the **Pending Management** folder in the **Administration** workspace. Agents can be pending management for the following reasons:

- Manual agent install

- Installation in progress
- Agent update in progress
- Repair in progress
- Agent license limit exceeded
- Failed agent installation
- Agent requires update
- Repair failed

Agent Versions



Agent Versions lists the number of agents running each agent version number, including cumulative updates.

See Also

Maintenance of Operations Manager

How to Configure Grooming Settings for the Reporting Data Warehouse Database

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

Recommendations for Daily, Weekly, and Monthly Operations Manager Tasks

Inventory of Operations Manager Infrastructure

Both maintaining and troubleshooting System Center 2012 – Operations Manager can be easier when you have a comprehensive inventory of the Operations Manager infrastructure. Ideally, the inventory is started when you first install Operations Manager, and updated as you add features and extend monitoring. If you have an existing infrastructure and no inventory, we recommend that you invest the time to document a complete inventory. Recommendations for Daily, Weekly, and Monthly Operations Manager Tasks includes a monthly task to review and update the inventory.

The following is a list of information you will find useful to include in your inventory.

- Management group information:
  - Name of the management group
  - How many agents are being used (or, how many servers/clients are being monitored)
  - Agentless exception monitoring (AEM) setting
  - Operational data reporting (ODR) setting
  - Customer Experience Improvement Program (CEIP) setting
  - Database grooming aetting
  - Number of allowed missed heartbeats
  - Manually installed agents
    - Are they allowed
    - Are they approved automatically
  - Connectors, per connector:
    - Name
    - Functionality
    - Active Directory accounts with passwords (encrypted)
    - Used FQDNs and IP addresses
    - Configured settings
  - Whether non-Microsoft software is being used
  - History:
    - When was the management group installed
    - Which version of Operations Manager was originally used
    - Whether it has ever been migrated to other hardware, or from physical to virtual or vice versa
    - Any major issues such outages and other major downtimes
  - Installed language
  - Reporting feature:
    - What is the SSRS url
    - What SQL server is hosting is the Data Warehouse
  - Web console:
    - What is the url
    - Is SSL used
    - Is it published to the internet
- Placement:
  - Fully qualified domain name (FQDN) of forest
  - LAN segment
  - Environment, such as production, testing, or anything else
- Version of Operations Manager, including any cumulative updates
- Management servers:

- FQDN
- IP address
- LAN segment
- Physical location (even when it is virtualized)
- Physical or virtual computer
- Amount of CPU, RAM, disks
- Operating system and patch level
- Disk configuration, RAID settings, and sizes
- Whether it is clustered or not
- Any SMS-enabled devices attached to it
- Accounts and passwords (encrypted)
    - Operations Manager SDK Account
    - Operations Manager Action Account
    - Operations Manager Data Warehouse Read Account
    - Operations Manager Data Warehouse Write Account
    - Operations Manager Health Account
    - Any third party software account
    - Run-As-Profile accounts (such as accounts used for the SQL Server and Active Directory management packs)
- Backup of encryption key and its location

- The total amount of gateway servers and per gateway server:
    - FQDN
    - IP address
    - LAN segment
    - Physical location (even when it is virtualized)
    - Physical or virtual computer
    - Amount of CPU, RAM, disks
    - Operating system and patch level
    - Disk configuration, RAID settings, and sizes
    - Functions of gateway server: what is being monitored and how many
    - Whether the gateway server is configured in a fail-over configuration
    - FQDN of PKI which is used
    - Operations Manager Action Account for the forest (and its password) where the gateway server resides
- SQL Server and Operations Manager databases
    - FQDN
    - IP address
    - LAN segment

    - Physical location (even when it is virtualized)
    - Physical or virtual computer
    - Amount of CPU, RAM, disks
    - Operating system and patch level
    - SQL Server:
        - Version
        - Edition
        - Architecture
        - Patch level (service packs, cumulative updates, and so forth)
        - Installed features
    - Disk configuration, RAID settings, and sizes
    - Whether it is clustered or not
    - If the SQL server also hosts other databases or SQL instances
    - Operations Manager database sizes and locations
- Management packs:
    - Which Microsoft management packs are imported and configured, including version information
    - Which management packs are custom-made, including version information
    - Which non-Microsoft management packs are imported and configured, including version information
- Backups:
    - Are the Operations Manager databases backed up on a regular basis
        - What tooling is used
        - Where are the backups stored
        - What retention policy is used
    - Are the Operations Manager servers backed up on a regular basis
        - What tooling is used
        - Where are the backups stored
        - What retention policy is used
    - Are the unsealed management packs backed up on a regular basis
    - Are the backups tested on their validity on a regular basis

See Also

Maintenance of Operations Manager

Monitoring the Health of the Management Group

How to Configure Grooming Settings for the Reporting Data Warehouse Database

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]

[Recommendations for Daily, Weekly, and Monthly Operations Manager Tasks]

Scheduling Maintenance in Operations Manager

This topic details the default schedule for System Center 2012 – Operations Manager maintenance tasks.

Maintenance Tasks Schedule

By default, Operations Manager performs maintenance tasks daily to maintain optimal performance of the Operations Manager database. These maintenance tasks are defined as system rules in the Operations Manager management pack.

The following table displays the maintenance tasks and the time they are scheduled to run:

Task	Description	Schedule
Discovery Data Grooming	A rule that deletes aged discovery data from the Operations Manager database.	Every day at 2 AM
Partition and Grooming	A rule that runs workflows to partition and deletes aged data from the Operations Manager database.	Every day at 12 AM
Detect and Fix Object Space Inconsistencies	A rule that repairs data block corruption in database schema objects.	Every 30 minutes
Alert Auto Resolve Execute All	A rule that automatically resolves active alerts after a period of time.	Every day at 4 AM

To check the schedules for the grooming jobs

1. In the Operations console, click **Authoring**.
2. Under **Authoring**, expand **Management Pack Objects**, and then click **Rules**.
3. In the **Rules** pane, change the scope of management pack objects by clicking **Scope**.
4. In the **Scope Management Pack Objects by target(s)** dialog box, click **Clear All**.
5. In **Look for**, type **All Management Servers Resource Pool** to locate the target from the System Center Core Library.
6. Select **All Management Servers Resource Pool**, and then click **OK**.

7. In the **Rules** pane, right-click the specific rule, and then click **Properties**.
8. In the **Properties** dialog box, click the **Configuration** tab.
9. Under **Data Sources**, click **View** to display the configured schedule for the rule.
10. Click **Close** twice to close the **Properties** dialog box.

> **Note**
> The scheduled times of the grooming jobs cannot be reconfigured by using an override. If you need to change the schedules of these maintenance tasks, you must first disable them with an override and then create new system rules that match the configuration of the original rules with new schedules.

See Also

Maintenance of Operations Manager

Monitoring the Health of the Management Group

Inventory of Operations Manager Infrastructure

How to Configure Grooming Settings for the Reporting Data Warehouse Database

How and When to Clear the Cache

How to Restart a Management Server

How to Configure Grooming Settings for the Operations Manager Database

Recommendations for Daily, Weekly, and Monthly Operations Manager Tasks

How and When to Clear the Cache

In System Center 2012 – Operations Manager, when troubleshooting an issue with the Operations console or with an agent, you may see recommendations to “clear the cache”. (For example, see the Knowledge Base article Troubleshooting gray agent state.) The following table explains how and when to clear the console cache or agent cache.

Cache	How to clear	When	Results
Operations console	Open the Operations console with the /clearcache parameter. `"C:\Program Files\System Center Operations Manager 2012\Console\Microsoft.EnterpriseManagement.Monitoring.Console.exe" /clearcache`	Use this method to open the Operations console if you experience errors trying to retrieve data in	Opening the Operations console with /clearcache deletes the following file: %systemdrive%\Users*username*\AppData\Local\Microsoft\Microsoft.EnterpriseManagement.Monitoring.Console\momcache.mdb

Cache	How to clear	When	Results
		views, such as ObjectNotFoundExceptions, or when the cache file grows too large and you want to reduce its size on disk.	
Health service on agent-managed computer	1. In the **Monitoring** workspace, expand **Operations Manager** and then expand **Agent Details**. 2. Click **Agent Health State**. 3. In **Agent State**, click an agent. 4. In the **Tasks** pane, click **Flush Health Service State and Cache**.	This should be the final step when troubleshooting issues with the agent, before uninstalling and reinstalling the agent.	Clearing the agent cache can cause data loss of monitoring data from that system. 1. Stops the System Center Management service. 2. Deletes the health service store files. 3. Resets the state of the agent, including all rules, monitors, outgoing data, and cached management packs. 4. Starts the System Center Management service. When the service restarts, the agent requests configuration from the management server. **Note** Because this task deletes the cached data in the health service store files, including the record of this task itself, no task status will be reported on completion of the task.
Health service on manage	1. In the **Monitoring** workspace, expand **Operations Manager** and then expand **Management Server**. 2. Click **Management Servers State**. 3. In **Management**	Run this task on a management server when the management server	Clearing the agent cache can cause data loss of monitoring data from agents to the management server. 1. Stops the System Center Management service. 2. Deletes the health service store files. 3. Resets the state of the agent, including all

Cache	How to clear	When	Results
ment server	**Server State**, click a management server. 4. In the **Tasks** pane, click **Flush Health Service State and Cache**.	is not functional, a restart has not fixed the problem, and you have exhausted other troubleshooting options.	rules, monitors, outgoing data, and cached management packs. 4. Starts the System Center Management service. **Note** Because this task deletes the cached data in the health service store files, including the record of this task itself, no task status will be reported on completion of the task.

See Also

Maintenance of Operations Manager

Monitoring the Health of the Management Group

Inventory of Operations Manager Infrastructure

Scheduling Maintenance in Operations Manager

How to Configure Grooming Settings for the Reporting Data Warehouse Database

How to Restart a Management Server

How to Configure Grooming Settings for the Operations Manager Database

Recommendations for Daily, Weekly, and Monthly Operations Manager Tasks

How to Restart a Management Server

Sometimes you need to restart a System Center 2012 – Operations Manager management server, such as when you update the operating system. To reduce the impact on your monitoring activities, follow these guidelines:

- When your management group has only one management server, do not place the management server in maintenance mode before restarting. Schedule the restart for a time when you expect the least activity, such as after business hours.
- When your management group has more than one management server:
  - Restart half or fewer management servers at one time.
  - Place the management servers to be restarted in maintenance mode before restarting. Maintenance mode will initiate failover of workloads to other management servers in the resource pool. After the server is restarted, remove it from maintenance mode.

When maintenance mode is not used, after the server is restarted, you might seem some availability alerts for the server. The alerts will close automatically after the server is running again.

See Also

Maintenance of Operations Manager

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 Configure Grooming Settings for the Reporting Data Warehouse Database

How to Configure Grooming Settings for the Operations Manager Database

Recommendations for Daily, Weekly, and Monthly Operations Manager Tasks

How to Configure Grooming Settings for the Reporting Data Warehouse Database

The Reporting data warehouse stores data for a specified length of time, depending on the data (Alert, State, Event, Aem, or Performance) and the aggregation type (raw data, hourly aggregations, daily aggregations). The database is set up to delete older data. Deleting the older data is called **grooming**.

The following table shows the default retention settings for the different types of data.

Data Set	Aggregation Type	Days To Be Kept
Alert	Raw data	400
State	Raw data	180
State	Hourly aggregations	400
State	Daily aggregations	400
Event	Raw data	100
Aem	Raw data	30
Aem	Daily aggregations	400
Perf	Raw data	10
Perf	Hourly aggregations	400
Perf	Daily aggregations	400

Settings for grooming the data warehouse can be changed through Microsoft SQL Server Management Studio.

To change grooming settings in the Reporting data warehouse

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 Reporting data warehouse (for example, computer\INSTANCE1); in **Authentication** list, select **Windows Authentication**; and then click **Connect**.
3. In the Object Explorer pane, expand **Databases**, expand **OperationsManagerDW**, and then expand **Tables**.
4. Right-click **dbo.Dataset,** and then click **Open Table**.
5. Locate the dataset for which you want to change the grooming setting in the **DatasetDefaultName** column and make note of its GUID in the **DatasetId** column.
6. In the Object Explorer pane, right-click **dbo.StandardDatasetAggregation** and then click **Open Table**.
7. In the **DatasetId** column, locate the dataset GUID you noted in step 5. Multiple entries of the same GUID might display.
8. Locate the aggregation type from the list in the **AggregationTypeId** column by using the following values:
   - 0 = raw, nonaggregated data
   - 10 = subhourly
   - 20 = hourly
   - 30 = daily

   After you have located the dataset and its aggregation type, scroll to the **MaxDataAgeDays** column, and then edit the value there to set the grooming interval.

See Also

Maintenance of Operations Manager

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 .NET Application Performance Monitoring Events

Recommendations for Daily, Weekly, and Monthly Operations Manager Tasks

How to Configure Grooming Settings for the Operations Manager Database

The grooming process removes unnecessary data from the Operations Manager database in order to maintain performance by managing its size. It deletes unnecessary records. You can configure the grooming setting for the following record types:

- Resolved alerts

  Note
  Active alerts are never groomed. You must close an alert before it will be groomed.
- Event data
- Performance data
- Task history
- Monitoring job data
- State change events data
- Performance signature
- Maintenance mode history
- Availability history

Any updates to the grooming settings are applied immediately.

Use the following procedure to specify when specific record types are deleted or groomed from the Operations Manager database of an Operations Manager management group. The default grooming setting for all record types is data older than 7 days.

To configure database grooming settings for a management group

1. In the Operations console, click **Administration**.
2. In the navigation pane, expand **Administration**, and then click **Settings**.
3. In the **Settings** pane, right-click **Database Grooming**, and then click **Properties**.
4. In the **Global Management Group Settings - Database Grooming** dialog box, select a record type, and then click **Edit**.
5. In the dialog box for the record type, specify **Older than** days, and then click **OK**.
6. In the **Global Management Group Settings - Database Grooming** dialog box, select another record type to **Edit** or click **OK**.

See Also

Maintenance of Operations Manager

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 Reporting Data Warehouse Database
How to Configure Grooming Settings for .NET Application Performance Monitoring Events
Recommendations for Daily, Weekly, and Monthly Operations Manager Tasks

Recommendations for Daily, Weekly, and Monthly Operations Manager Tasks

Daily Tasks

	Task	References
☐	Check the **Management Group Health** dashboard view.	Monitoring the Health of the Management Group
☐	Check open alerts.	Viewing Active Alerts
☐	Back up the operational database (incremental).	Recommended Backup Schedule for Operations Manager

Weekly Tasks

	Task	References
☐	Back up operational database (full).	Recommended Backup Schedule for Operations Manager
☐	Back up data warehouse database (incremental).	Recommended Backup Schedule for Operations Manager
☐	Back up Audit Collection database (incremental).	Recommended Backup Schedule for Operations Manager
☐	Run the **Data Volume by Management Pack** and **Data Volume by Workflow and Instance** reports.	• How to Run a Report • Operations Manager Reports Library

Monthly Tasks

	Task	References
☐	Back up data warehouse database (full).	Recommended Backup Schedule for Operations Manager
☐	Back up Audit Collection database (full).	Recommended Backup Schedule for Operations Manager
☐	Back up custom management packs.	How to Back Up Custom Management Packs
☐	Check for updates to management packs.	How to Import an Operations Manager Management Pack (Using the “To import a management pack from the catalog” procedure, select to view updates available for management packs that are already imported.)

See Also

Maintenance of Operations Manager

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

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**.

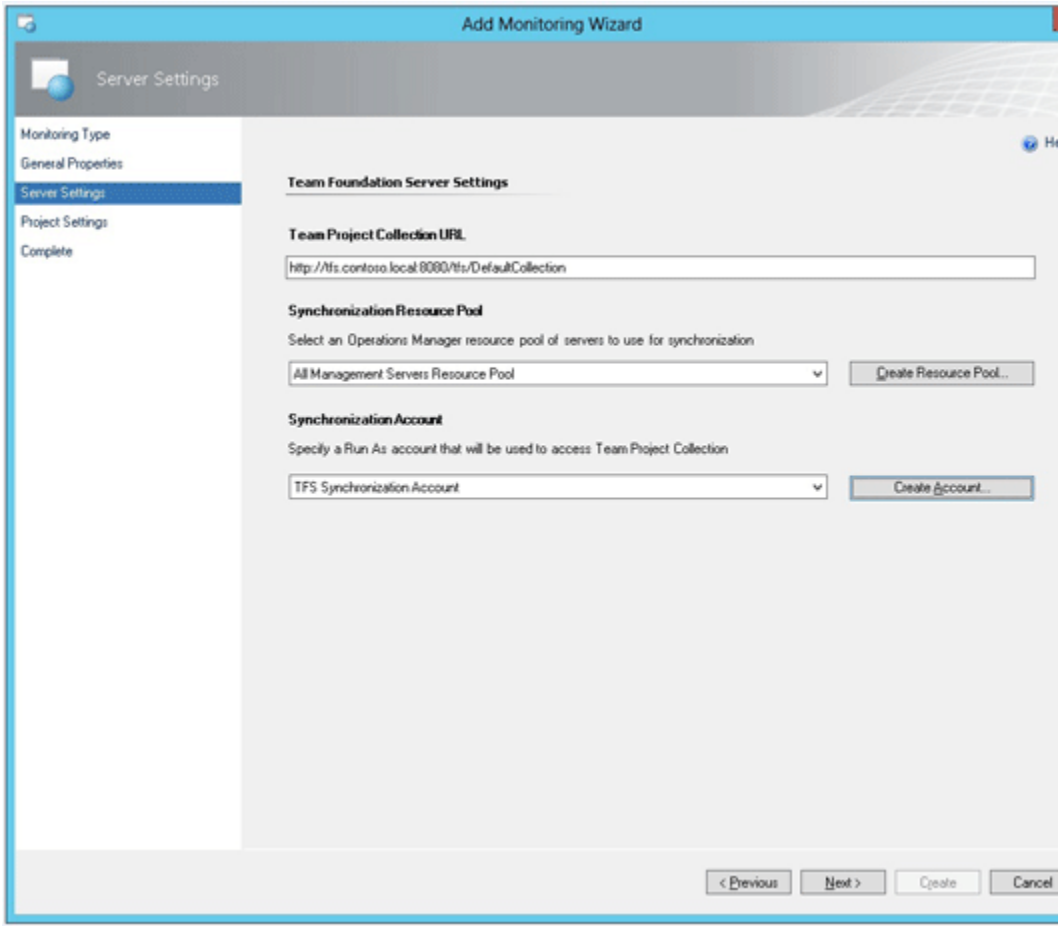
   Important

   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.

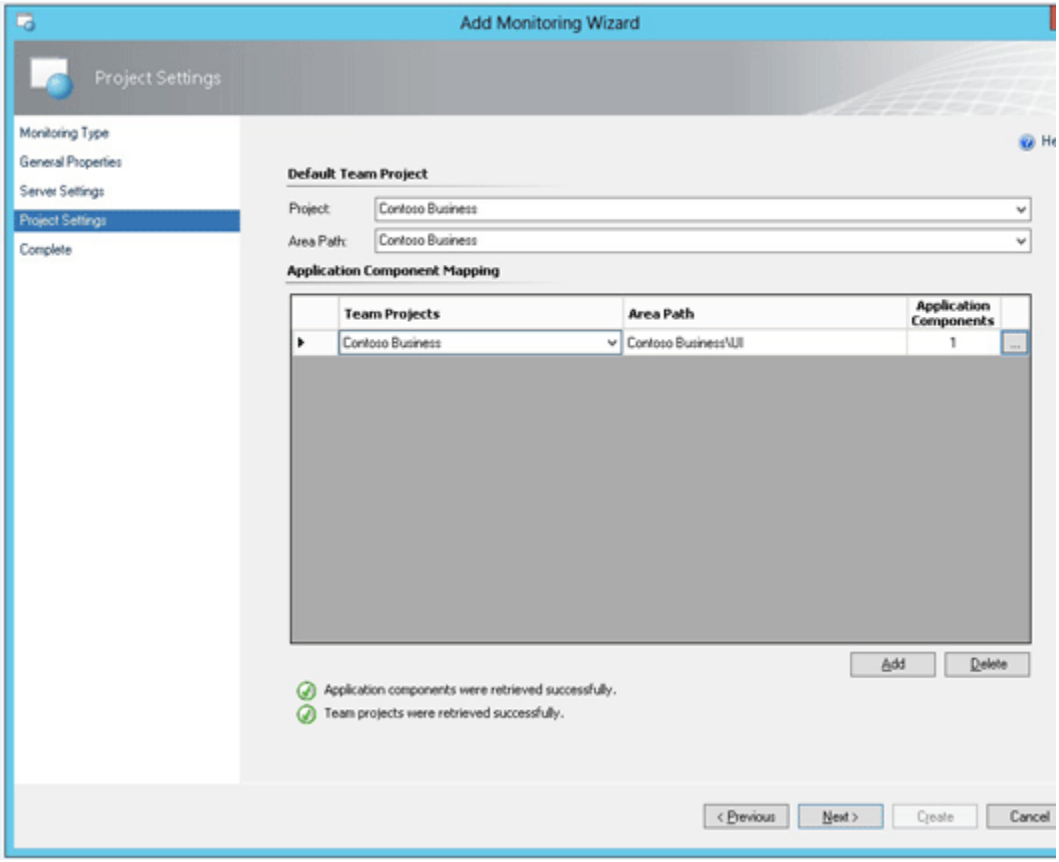
   Note
   You can get the TFS Team Project Collections URL from the Team Foundation Server Administration Console. If the TFS Team Project Collection that you choose is offline or otherwise unavailable, the wizard will warn you, but it will still let you finish the configuration. Additionally, when TFS 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 assigned to Engineering	TFS Connector	TFS Work Items Creation Rule	Interval Seconds	300 seconds
How often alerts assigned to Engineering and their associated	TFS Collection	TFS Work Items Synchronization Rule	Interval Seconds	900 seconds

Override description	Target object	Rule	Parameter	Default Value
TFS work items are synchronized				
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 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 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.

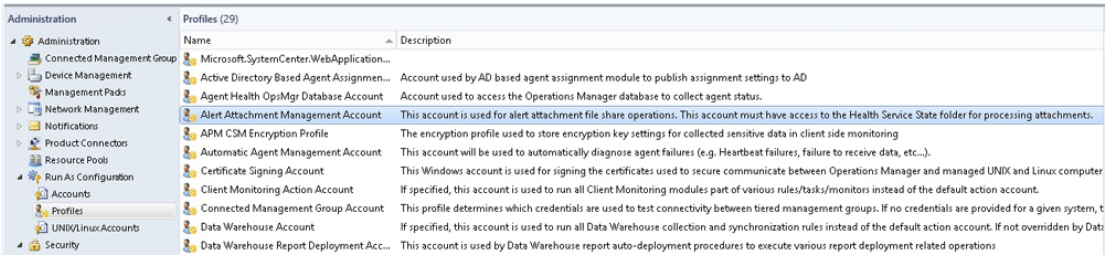
   Important
   Some alert attachments can be very large. For example, a typical production IntelliTrace Historical Profiling snapshot might be several hundred megabytes (MB). Make sure you allocate enough storage space to meet your business needs.

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].

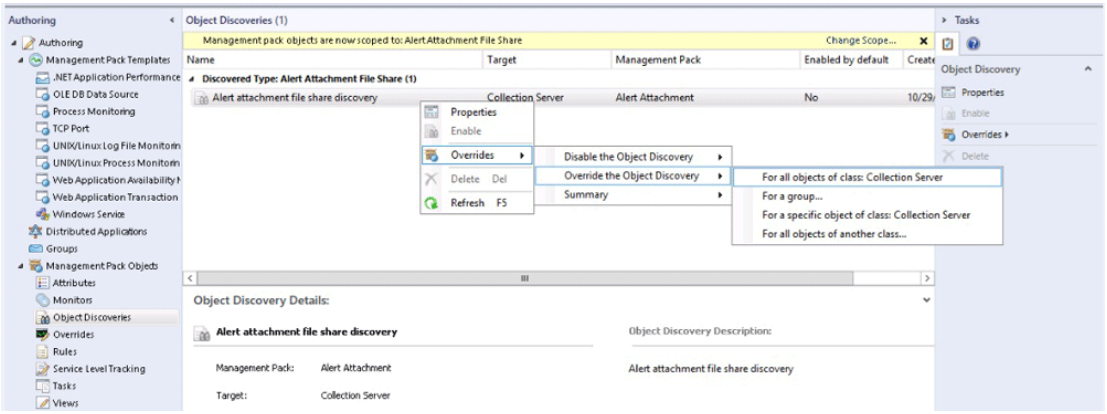
   The location of the Alert Attachment Management Account to be configured



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



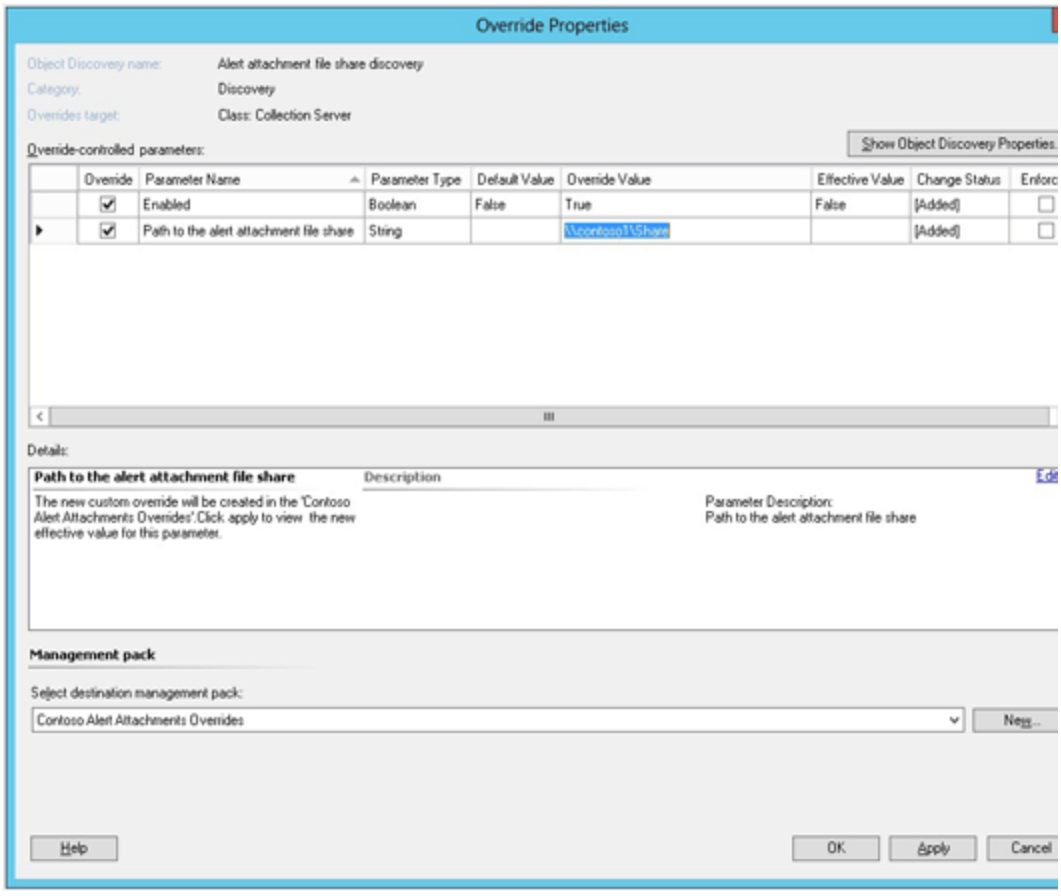
   On the **Override Properties** page, set **Enabled** to **True**, and then set **Path to the alert attachment file share** to the location of the network file share you created.

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 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**.

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 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.

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	• Microsoft Team Foundation Server 2012 • Operations Manager 2007 R2 • System Center 2012 – Operations Manager	Microsoft Download Center

Management Pack	Description	Use with …	Where to get it
	instances, team project collections, build servers, and proxy servers.	• Operations Manager in System Center 2012 SP1 • System Center 2012 R2 Operations Manager	
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 • System Center 2012 R2 Operations Manager	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 • 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**.

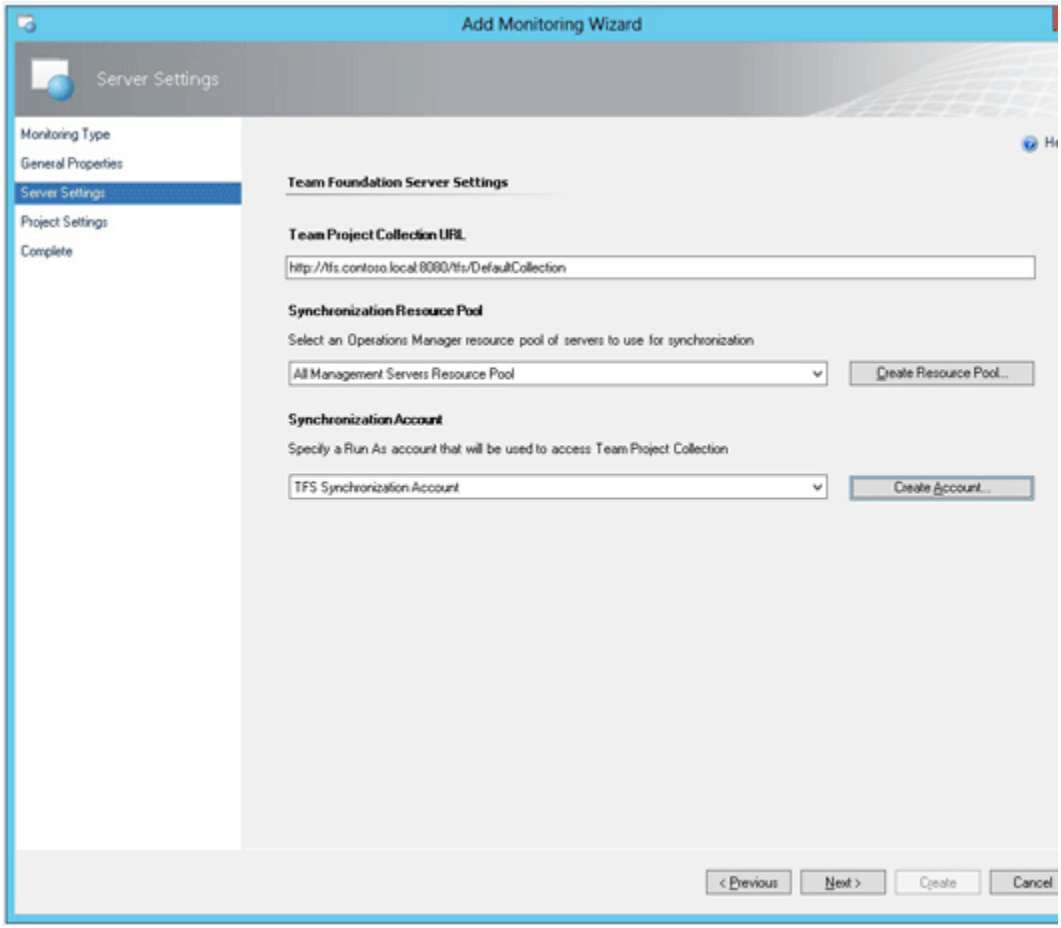
   Important
   You must run the Add Monitoring Wizard for each team project collection that you want to synchronize alerts with.
3. To open the TFS Work Item Synchronization template, in the Add Monitoring Wizard, on the **Monitoring Type** page, select **TFS Work Item Synchronization**.
4. On the **General 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.

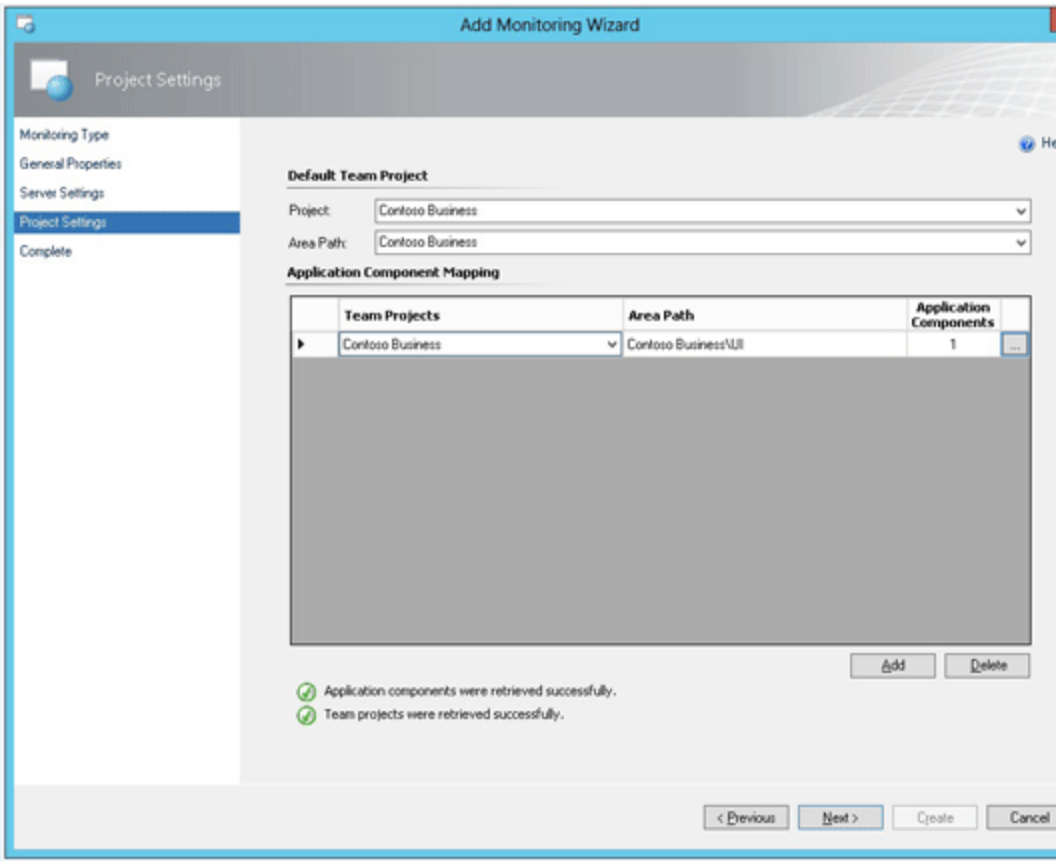
Server Settings page



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 history that reflects the associated TFS work item history	TFS Collection	TFS Work Items Synchronization Rule	Delta in Hours	24 hours

Override description	Target object	Rule	Parameter	Default Value
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

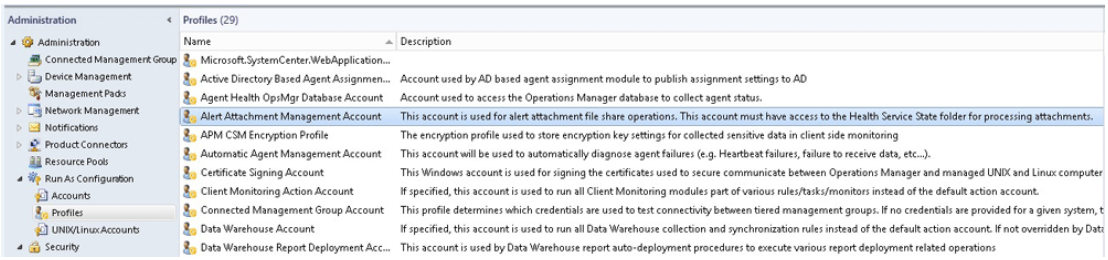
1. Create an Alert Attachment network file share with enough space to accommodate your anticipated storage needs.

   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.

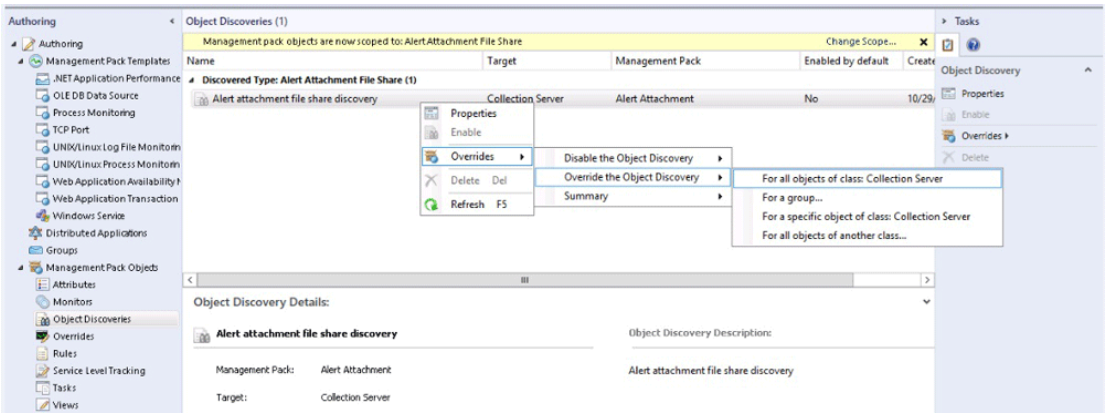
The location of the Alert Attachment Management Account to be configured



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

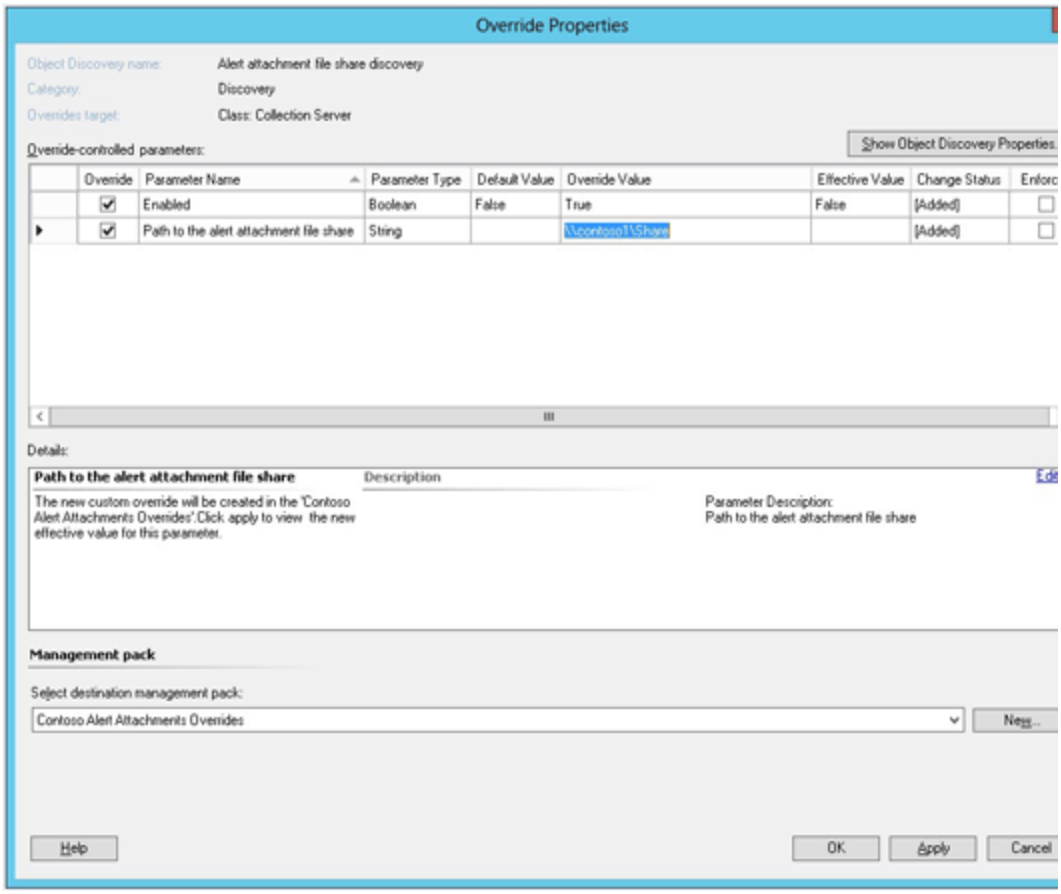


   On the **Override Properties** page, set **Enabled** to **True**, and then set **Path to the alert attachment file share** to the location of the network file share you created.

   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 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**.

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 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.

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	• Microsoft Team Foundation Server 2010 • Operations Manager 2007 R2 • System Center 2012 – Operations Manager • Operations Manager in	Microsoft Download Center

Management Pack	Description	Use with …	Where to get it
	servers, and proxy servers.	System Center 2012 Service Pack 1 (SP1)	
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
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.MonitoringAg
ent.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	Use the .NET Application Performance Monitoring template. For more information, see .NET Application Performance Monitoring Template

Monitoring approach	When to use	How to control monitoring
	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.	
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 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.	Use Windows PowerShell cmdlets **Start-WebApplicationMonitoring** and **Checkpoint-WebApplicationMonitoring**. **Start-WebApplicationMonitoring** starts monitoring. **Checkpoint-WebApplicationMonitoring** collects a snapshot 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	Use this approach	Use Windows PowerShell cmdlets **Start-**

Monitoring approach	When to use	How to control monitoring
collection that temporarily overrides the settings of continuous monitoring with System Center APM	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.	**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 temporarily overrides settings of continuous monitoring with Microsoft Monitoring Agent local collection	Use this approach when you have 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	Use Windows PowerShell cmdlets **Start-WebApplicationMonitoring** and **Stop-WebApplicationMonitoring**. When you stop monitoring, the trace is written to a local file in the location that you specified when you started monitoring.

Monitoring approach	When to use	How to control monitoring
	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.	

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 • 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	• Microsoft Visual Studio Ultimate 2013 RC • Microsoft Visual Studio Ultimate 2013 Preview • Microsoft Visual Studio Ultimate 2012 Update 2	If you want to use local monitoring with Application Performance Monitoring in 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) • 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) • System Center 2012 R2 Operations Manager (only when you are multihoming by using System Center 2012 R2 Operations Manager or during upgrades to System		

Service	Build	Supported versions of System Center	Supported versions of Visual Studio	Interoperability information
		Center 2012 R2 Operations Manager)		