

Operations Manager 2007 R2 Design Guide

Microsoft Corporation

Published: September 2010

Author

Christopher Fox

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, ActiveSync, Internet Explorer, JScript, SharePoint, SQL Server, Visio, Visual Basic, Visual Studio, Win32, Windows, Windows PowerShell, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Revision History

|  |  |
| --- | --- |
| Release Date | Changes |
| May 2009 | The Operations Manager 2007 R2 version of this guide contains the following updates and additions:   * Removed the document roadmap * Added UNIX or Linux monitoring security information, as well as performance and scale numbers * Updated scale numbers |
| July 2009 | * Removed broken link, fixed visual errors |
| September 2009 | * Added task load content for server roles |
| December 2009 | * Updated the sizing information in the “Collective Client Monitoring Guidelines and Best Practices” section. |
| February 2010 | * Added procedures and equations for sizing ACS topologies * Added Appendix A, which is an application of the ACS sizing procedures in a hypothetical situation |
| August 2010 | * Added reference to Operations Manager 2007 R2 Sizing Helper |
| September 2010 | * Updated for failover design in Disaster Recovery Functionality section |

Contents

[Introduction to the Operations Manager 2007 R2 Design Guide 6](#_Toc273360976)

[Overview of Operations Manager 2007 7](#_Toc273360977)

[Identifying Requirements for Operations Manager 2007 17](#_Toc273360978)

[Mapping Requirements to a Design for Operations Manager 2007 21](#_Toc273360979)

[Developing an Operations Manager 2007 Implementation Plan 41](#_Toc273360980)

[Appendix A 43](#_Toc273360981)

Introduction to the Operations Manager 2007 R2 Design Guide

Every IT environment is unique, and therefore the infrastructure used to monitor it must accommodate that uniqueness in order to be effective. There is no "one-size-fits-all" solution to monitoring that delivers a satisfactory experience. On the other hand, companies cannot afford to custom develop monitoring solutions from the ground up. The amount of money and effort required to do this is prohibitive.

Microsoft System Center Operations Manager 2007 strikes a balance between these two points by providing the building blocks necessary for a solution that accommodates your business needs. How you arrange the building blocks and the relationships that you establish between them is up to you and is referred to as topology planning. Your topology must be driven by the business, technology, security, and regulatory needs of your company, and it is during the design process that the uniqueness of your particular environment is built into your Operations Manager topology.

Prior to starting your design, you must have a thorough understanding of Operations Manager 2007 security, including the required accounts and groups and the permissions they need. It is critically important to your design process that you understand roles and role-based security as implemented in Operations Manager 2007, as well as the implications of mandatory mutual authentication. For a complete primer on Operations Manager 2007 Security, see the Operations Manager 2007 Security Guide at <http://go.microsoft.com/fwlink/?LinkId=64017>.

Operations Manager 2007 takes a model-based approach to monitoring. In model-based management, all items that participate in providing a function or service in your organization are represented as models. For more information on model-based management, see the Operations Manager 2007 Key Concepts guide at <http://go.microsoft.com/fwlink/?LinkId=124799>.

About This Guide

This guide consists of sections that step you through the design and testing process for your Operations Manager 2007 implementation. This guide will help you understand the building-block-level components in Operations Manager 2007 by presenting summaries of these roles. It will help you to ask the right questions to make sure your design meets your company's needs. It will make sure that you have answered the most fundamental design questions to ensure your design is flexible and scalable. It will help you plan and size your Operations Manager 2007 topology using data from the Performance and Sizing Guide. It provides guidance on how to validate your design in the lab.

After you have completed working through this guide, you will have a detailed infrastructure diagram and planned configuration of Operations Manager 2007 components. You will have validated these blueprints in a lab setting, and you will be ready to start your pilot deployment in production. When you reach this point, the next guide to use is the Operations Manager 2007 Deployment Guide.

Please note that this guide is intended to do just as its name says, to guide you. The decisions that you make and the design you come to in the end must ultimately be based on your needs. The guide helps make sure that you have all the information you need to make the best decisions for your particular situation.

Understanding the Operations Manager 2007 Design Process

Designing an Operations Manager implementation is really the process of achieving the following:

 Understanding the features and functions that Operations Manager 2007 provides.

 Understanding your company's business and technical requirements, the current infrastructure, and your current monitoring procedures.

 Mapping those requirements to an Operations Manager 2007 infrastructure that will meet them.

 Validating the Operations Manager 2007 infrastructure design in a lab setting.

During this process, you will have to perform sizing and capacity planning for your Management Groups; the data for this is included in this guide

Overview of Operations Manager 2007

An Operations Manager 2007 infrastructure is composed of certain core components that must be implemented and a set of optional components and features that you can choose to implement as needed. This section presents these components and features according to their required and optional classification. In general, a component is something that you will install from your source media, and a feature is something that you will configure and make use of once all the required components for that feature have been installed.

Required Server Roles and Components

The basic unit of functionality of all Operations Manager 2007 implementations is the management group. It consists of an installation of Microsoft SQL Server 2005 or Microsoft SQL Server 2008, which hosts the OperationsManager database, the root management server, the Operations console, and one or more agents that are deployed to monitored computers or devices are the base components of a management group.

OperationsManager Database

The OperationsManager database is the first component to be installed in all management groups. This database holds all the configuration data for the management group and stores all the monitoring data that has been collected and processed by the agents.

To optimize performance of Operations Manager, you must keep the size of the OperationsManager database under control. Testing has shown that staying under 50 GB is a good practice. To keep from exceeding this limit, Operations Manager 2007 will automatically groom out older, unnecessary data according to parameters that you set.

Because only one OperationsManager database can be in a management group, it must be functional for the management group to function. To mitigate the single instance of the OperationsManager database from being a single point of failure, the OperationsManager database can be placed in a Cluster service (formerly known as MSCS) failover cluster. In addition, log shipping can be configured so that current operations data and configuration information can be sent to another Microsoft SQL server of the same version that is hosting a duplicate copy of the primary OperationsManager database. Should there be a failure in the primary database, the duplicate can be updated and switched to. The OperationsManager database is involved in these activities:

 management pack import – Management pack imports place a load on the CPU, the memory, and the disk of the database server.

 discovery – As the discovery process occurs, agents return data to the management servers. Ultimately, this data is inserted into the OperationsManager database. This process places a load on the disk and on the CPU of the database server.

 monitoring operations – All data that is collected from agents and all management group configuration information is stored in the OperationsManager database.

Root Management Server

The root management server (RMS) is a specialized type of management server in a management group, and it is the first management server installed in a management group. Only one RMS can be active per management group at a time. In brief, the RMS is the focal point for administering the management group configuration, administering and communicating with agents, and communicating with the OperationsManager database and other databases in the management group.

The RMS also serves as the target for the Operations console and the preferred target for the Web consoles.

The RMS hosts the System Center Data Access service and the System Center Management Configuration service. These services run only on the RMS. The System Center Data Access service provides secure access to the OperationsManager database for all clients, including the Operations console, Operations shell, and Web console. The System Center Management Configuration service is responsible for calculating and distributing the configuration of all management servers and agents, including which management packs they should receive.

Like the OperationsManager database, the RMS role can be installed into an MSCS failover cluster to make it highly available. In addition, other management servers in the management group (if you have them) can be manually promoted to the role of RMS.

The RMS participates in the functions:

 management pack import – When you import management packs, the RMS first verifies that the management pack is valid. Then, it converts the XML-formatted data of the management pack to relational database format. Finally, it sends the data to the OperationsManager database. Both operations place a load on the RMS CPU, disk, and memory.

 maintenance of the Instance space – The System Center Management Configuration service calculates the configurations for all monitored devices in the management group. To do this, the service maintains a copy of all the configuration information in memory and performs its calculations there. This places a load on memory. After the instance space calculations are run, agents send a synchronization request to their management server, which sends the request to the RMS. The RMS stores these requests until it can act upon them in an in-memory queue.

 discovery – After management packs are sent to the agents, the discovery process starts. Agents return the discovery data to their management servers and then to the RMS. This data is inserted into the OperationsManager database and incorporated in the Instance space. Both activities place a load on the disk, the CPU, and the memory on the RMS.

Agent

An Operations Manager 2007 agent is a service that is deployed to a computer that you want to monitor. On the monitored device, an agent is listed as the System Center Management service. Every agent reports to a management server in the management group. This management server is referred to as the agent's primary management server. Agents watch data sources on the monitored device and collect information according to the configuration that is sent to it from its management server. The agent also calculates the health state of the monitored object and reports back to the management server. When the health state of a monitored object changes or other criteria are met, an alert can be generated from the agent. This lets operators know that something has gone awry and requires attention.

Agents also have the ability to take many different types of action to help diagnose issues or correct them. By feeding health data to the management server about the monitored device, the agent provides an up-to-date picture of the health of the device and all the applications that it hosts.

It is possible to monitor devices in an agentless fashion. In this case, a management server performs the monitoring remotely.

Operations Console

The Operations console provides a single, unified user interface for interacting with Operations Manager 2007. The Operations console provides access to monitoring data, basic management pack authoring tools, Operations Manager 2007 reports, all the controls and tools necessary for administering Operations Manager 2007, and a customizable workspace.

For a user to access the Operations console, the user's Active Directory user account must be assigned to an Operations Manager 2007 user role. A user role is the combination of a scope of devices that access is granted to and a profile that defines what the role can do within its defined scope. Role-based security is enforced in the Operations console so that Operations Manager administrators can define what any given user can see in the console and what actions the user can take on those items. For more information, see the "Role-Based Security" section in this document.

Management Packs

Management packs contain an application's health definition as defined by the application developers. When imported into Operations Manager, they enable the agent to monitor the health of an application, generate alerts when something of significance goes wrong in the application, and take actions in the application and its supporting infrastructure to further diagnose the application or restore it to a healthy state. Without an application, operating-system, or device-specific management pack, Operations Manager 2007 is unaware of those entities and is unable to monitor them.

Optional Server Roles and Components

These additional server roles extend the functionality of a management group. Most of these components are installed separately from the required core components, but some can be installed at the same time as the core components. For complete details on installing Operations Manager 2007 components, see the Operations Manager 2007 Deployment Guide.

Management Server

A management server is used primarily for receiving configurations and management packs from the RMS and distributing them to the agents that report to the management server. It does not perform any of the special functions of the RMS. A management server can be promoted to the RMS role if the RMS fails, as long as it was present in the management group prior to the RMS failure. Multiple management servers are installed in a management group to provide extra capacity for agent management. In addition to providing scalability, introducing additional management servers in a management group allows for agents to fail over and start reporting their data to another management server if communication with their primary management server is lost.

The management server can also be used for remote monitoring purposes (such as URL monitoring and cross-platform monitoring). One additional role for a management server is to host the Audit Collection Service (ACS) Collector role. The ACS Collector can be installed only on a management server or gateway server. See the "Audit Collection Service (ACS)" section later in this document for additional information about Audit Collection Services. Other roles include the AEM file share role, which is also explained later in this document.

The management server makes heavy use of the CPU for data collection activities, and it also makes heavy use of disk for UNIX and Linux data queues.

Gateway Server

Operations Manager 2007 requires that agents and management servers authenticate each other and establish an encrypted communication channel before they exchange information. Kerberos is the default authentication protocol. When the agent and the management server are in the same Active Directory forest or in forests with forest trust, mutual authentication occurs automatically. This is because Kerberos is the default authentication protocol in Active Directory.

When agents and management servers are not within the same Kerberos trust boundary (that is, not in the same Active Directory forest or in forests with forest trust), certificate-based authentication mechanisms must be used. In this situation, a certificate must be issued and maintained for those agents and the management servers to which they report. In addition, if there is a firewall between the agents and the management server, either the firewall rules must permit each computer that hosts an agent to communicate directly through it over an encrypted channel or the Operations Manager communication port must be opened inbound.

An Operations Manager 2007 gateway server can be used to drastically reduce the administrative overhead required to maintain communication between agents and management servers that are separated by a trust boundary. The gateway server acts as a proxy for agent communications. The gateway server is placed within the trust boundary of the agents (which can be a domain), and all the agents communicate with it. Then the gateway server, through the use of its computer certificate, performs mutual authentication with the management server and forwards the agent-to-management server and management server-to-agent communications along. This then requires only one certificate for the management server and one for the gateway. In the firewall scenario, only the gateway server and the management server need to be authorized to communicate with each other.

Multiple gateway servers can be installed in a management group for the purposes of scalability and failover. Should an agent lose communication with its gateway server, it can then fail over to a different gateway server that is in the same management group and within the agent's trust boundary.

Likewise, gateway servers can be configured to fail over between management servers in a management group. This configuration then provides fully redundant communication channels for agents that lie outside a management server's trust boundary.

The gateway server participates in the following activities:

 All data communication between untrusted agents and management servers – gateway servers proxy communications between management servers and agents. They also serve as a concentration point for the same communications. This data consists of configuration data and management packs that are sent to the agent, and it consists of discovery and monitoring data that is sent to the management server. All this data is queued on the gateway servers local disk. Because this places a significant load on the gateway server disk, be sure to provide plenty of fast disk.

Web Console Server

The Web console server provides an interface to the management group that is accessible via a Web browser. It does not have the full functionality of the Operations console, however, and provides access to only the Monitoring, Favorite Reports, and My Workspace views. The Web console provides access to all the monitoring data and tasks that are actions that can be run against monitored computers from the Operations console. Access to data in the Web console has the same restrictions as access to content in the Operations console.

Management Pack Authoring Console

The Operations Manager 2007 authoring console is a stand-alone application that provides richer management pack authoring functionality than what is provided by the Operations console authoring space. Using the authoring console, you can create new management packs, view and modify existing management packs, verify the integrity of management packs, and import and export management packs to and from management groups. The Operations Manager 2007 authoring console can be downloaded here: <http://go.microsoft.com/fwlink/?LinkId=136356>.

Reporting Data Warehouse

The Reporting Data Warehouse stores monitoring and alerting data for historical purposes. The management servers write their data to the Data Warehouse at the same time it is written to the OperationsManager database, so the reports generated always contain the most up-to-date data. The Data Warehouse automatically aggregates performance data on an hourly and daily basis. This allows long-term trending reports to be run much faster than they would be otherwise, and far less data needs to be retained to support long-term trend reporting.

The Reporting Data Warehouse can receive data from multiple management groups, thereby allowing for an aggregated view of data in your reports.

Reporting Server

Operations Manager Reporting Server is installed into an instance of Microsoft SQL 2005 Reporting Services SP1 or later or Microsoft SQL Server 2008 SP1 Reporting Services. It is responsible for building and presenting the reports from data queried from the Reporting Data Warehouse. All reports are accessed in the Operations console, so access to reports is controlled via role-based security.

Audit Collection Services

Audit Collection Services (ACS) is a high-performance, secure solution that collects and stores events from the Security Event Log on monitored computers. Events are stored in a separate database, the ACS database (discussed later in this document), in Microsoft SQL Server 2005 SP1 or later and Microsoft SQL Server 2008 SP1. ACS collects all events written to the Security Event Log on computers that the ACS Forwarder is enabled on. Events are forwarded from monitored computers to the ACS Collector, which runs on a management server, which then processes them and writes them to the ACS database. The events are transmitted in an encrypted, near real-time fashion from the forwarders to the collector. A separate component, ACS Reporting, is then used to generate reports from the stored ACS data.

A key to using ACS effectively is the development of a sound Windows Audit Group Policy that is implemented as a domain Group Policy. For details on Windows Audit Group Policy and implementing ACS, see [Managing Audit Collection Services in Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkID=144374) http://go.microsoft.com/fwlink/?LinkID=144374 .

ACS Forwarder

The ACS Forwarder is embedded in the Operations Manager 2007 agent, so no separate deployment or configuration is required. The ACS Forwarder appears as the Audit Forwarder service and is disabled by default. The ACS Forwarder on an individual computer or on groups of computers is enabled via a task in the Operations console.

ACS Collector Server

The main purpose of the ACS Collector server is to collect, filter, and pre-process all the Windows security log events for insertion into the database. Because the ACS collects all security events in near real-time, vast amounts of data enters the system from the forwarders. Not all of this information will be of interest to your company, as defined in your company's Windows Audit Group Policy. The filtering mechanism at the collector allows you to specify which events you want written to the ACS database for long-term storage.

The ACS Collector server has a separate installation program from the Operations Manager servers, agents, or reporting components. It can be installed only on an existing management server or RMS if you have not installed any additional management servers. One ACS Collector server can support hundreds to thousands of servers, depending on the server role and Windows Audit Group Policy, and tens of thousands of workstations. However, there is a one-to-one relationship between the ACS Collector server and the ACS Database (which is discussed in the next section). If for scalability or control reasons your company requires additional ACS Collectors, you will need one ACS Database per ACS Collector.

ACS Database

After the data has been pre-processed by the ACS Collector server, it is written to its ACS Database, which is just a database created on a Microsoft SQL Server 2005 SP1 or SP2 instance. Because it is a standard SQL database, it can be clustered for high-availability. To accommodate the one-to-one relationship between collectors and databases, you can create, via named instances, multiple ACS Databases on a single SQL Server 2005 server as long as it can support the additional load. For more information about sizing and capacity planning for ACS, see that section later in this guide.

ACS Reporting

The ACS Reporting server is also a separately installed component. A number of preconfigured reports are available. Installation of ACS Reporting requires an existing instance of SQL Server 2005 SP1 or later Reporting Services or Microsoft SQL Server 2008 Reporting Services. This can be a stand-alone instance, or you can install ACS Reporting along with Operations Manager 2007 Reporting with one tradeoff.

If you install ACS Reporting into the same Reporting Services instance as Operations Manager 2007 Reporting, ACS Reporting is fully integrated with Operations Manager Reporting. This results in reduced administrative overhead, because anyone who has been assigned to the Operations Manager Reporting role will have access to the ACS reports. Some companies might not find this to be a desirable configuration, and they might elect to install ACS Reporting into its own instance of SQL Server Reporting. In this case, you must define your own security groups and roles, resulting in higher administrative overhead but extremely tight control over access to ACS data.

Proxy Agent

Operations Manager 2007 has the ability to monitor network devices, via SNMP v2, computers that are not running a Windows operating system, and computers without agents. In these cases, another computer that has an agent installed is actually performing the monitoring remotely. The computer that is performing the remote monitoring is called a proxy agent. The agent that is acting as a proxy for monitoring other devices is a standard Operations Manager agent. It is merely configured differently by selecting the Allow this agent to act as a proxy and discover managed objects and other computers option in the agent properties. Then you configure the agentless managed device to designate the proxy agent it is to use. For more information about agent deployment and management of devices, please see the Operations Manager 2007 Operations Guide.

Operations Manager 2007 Command Shell

In 2006, Microsoft introduced the Windows PowerShell command-line interface for use on its Windows Server 2003, Windows Server 2008, Windows XP, and Vista operating systems. This interface was developed for use by system administrators for automating tasks. The interface includes an interactive prompt and a scripting environment that can be used independently or in combination. The objects that you interact with in PowerShell are called "command-lets" and are binary native commands in Windows PowerShell. Windows PowerShell commands are designed to deal with objects—structured information that is more than just a string of characters appearing on the screen. Command output always carries along extra information that you can use if you need it.

The Operations Manager 2007 Command Shell is a grouping of 203 individual command-lets that have been specifically developed for automating Operations Manager 2007 administrative tasks. The Command Shell can be installed on any computer that will have the Operations console installed.

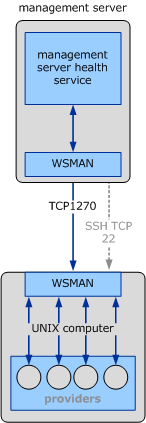
Features

Features are present by default and only require configuration to make use of them. The ability to configure and use features as you please in Operations Manager 2007 is a hallmark of its flexibility.

Cross-Platform Monitoring (UNIX-based or Linux-based Computers)

Operations Manager 2007 R2 management servers and gateway servers can monitor UNIX and Linux computers. For a complete list of UNIX-based and Linux-based operating systems that can be monitored, please see the Supported Configuration guide at <http://go.microsoft.com/fwlink/?LinkId=144400>.

In cross-platform monitoring, the system center management service on the management server or gateway server runs all the monitoring intelligence. The monitoring system center management service communicates with the monitored computer through a WSMAN layer that is on both the management server and the computer being monitored. It is a prerequisite that the WSMAN layer be installed on the monitored computer. Communication between the WSMAN layers occurs over TCP port 1270 and always originates from the management server or gateway server. In some cases, such as when the WSMAN layer is not present on the monitored computer or it has failed, the communication can occur to SSH TCP 22. SSH can be used for installing the WSMAN layer or performing diagnostics.



Agentless Exception Monitoring

In Windows operating systems, when an application error occurs, the Watson service can capture the error and forward the information about the error to Microsoft to determine the root cause of the problem. Typically, each computer does this individually. Because error monitoring and reporting is occurring on an individual basis, IT administrators do not have any visibility into these exceptions across their organization.

When the Agentless Exception Monitoring feature is enabled, all the exceptions can be forwarded to a management server in your management group and aggregated. Because they are then concentrated in a single place, your company can use this data for analyzing and diagnosing desktop and server application issues as they are occurring throughout your company. If you choose, you can also configure the management server to forward the exception-monitoring information to Microsoft for crash analysis.

Connector Framework

The Connector Framework is an application programming interface (API) that exposes Operations Manager functionality for the purposes of integrating with other management products or other technologies, such as trouble-ticketing systems. It enables the development of connectors that can bidirectionally exchange information with Operations Manager. The Connector Framework interacts primarily with the System Center Data Access service on the RMS. For more information about developing applications that use the Operations Manager 2007 Connector Framework, see the [Operations Manager 2007 SDK](http://go.microsoft.com/fwlink/?LinkId=126913).

URL Monitoring

Operations Manager 2007 provides the ability to monitor URL availability from a watcher node (another health service running on a different computer. Management servers that perform this function will have a heavy load placed on their CPU resources and then disk resources. If you are going to monitor more than 1000 URLs, you should create a dedicated management group for this purpose.

Concepts

In planning your topology, you must understand the concept of role-based security as implemented in Operations Manager.

Role- Based Security

Role-based security is used to control the objects that you can see and what actions you can take on those objects. A role is made up of two parts. The first part is a scope that contains the objects that can be accessed or seen. For example, a scope can be defined as containing nothing but domain controllers or SQL servers. The second part is a profile. Each profile defines actions that can be taken on objects that can be seen. Out of the box, Operations Manager 2007 provides the following five profiles:

 Administrator profile—This profile has full privileges to Operations Manager.

 Advanced Operator profile—This profile has the limited ability to tweak the monitoring configuration by configuring overrides on rules and monitors.

 Author profile—This profile has the ability to author the monitoring configuration elements, such as rules, tasks, monitors, and views.

 Operator profile—This profile has the ability to access Alerts, Views, and Tasks.

 Read-Only Operator profile—This profile allows read-only access to Alerts and Views.

 Report Operator profile—This profile allows read access to Operations Manager reports.

Operations Manager also contains five predefined roles, each of which is globally scoped. For example, the Operations Manager Administrator role uses the Administrator profile and is globally scoped, meaning that it can see and manipulate all objects in Operations Manager. There are matching predefined roles for each of the profiles listed above.

In addition to the predefined roles, you can create new roles based on the Advanced Operator, Author, Operator, and Read-Only Operator profiles. When creating a new role, after you have selected the profile that you want to use, you then create the scope of objects that the role will have access to. In this fashion, you can create a role that uses the Operator profile and is scoped only to Microsoft Exchange Servers for your Exchange administrators. When you then assign the Exchange administrators to the role (either by membership in an Active Directory Group or by individual account), they are able to open the Operations console, but they only see the Exchange servers and are allowed to take action only on the Exchange-related Alerts, Views, and Tasks.

Role-based security is applied no matter how you access Operations Manager functionality, whether it is through the Web console or the Command Shell. For more information about roles and role-based security, see the Operations Manager 2007 Security Guide.

Identifying Requirements for Operations Manager 2007

Identifying your company's requirements is the next step in your Operations Manager design process. The requirements can be divided into three categories: business requirements, IT requirements, and optimization requirements or goals. The requirements gathering step is the single most important step in developing your Operations Manager 2007 design. By having a thorough understanding of the requirements, you can then build a solution that is aligned with those expectations. If the project deliverable is not aligned with expectations, the project might not succeed.

To make sure that you have an accurate understanding of the requirements, you have to talk to different groups of people. To start with, you must understand the expectations of the key stakeholders and sponsors. If they expect Operations Manager to be able to do something that it can't, now is your opportunity to educate them and set expectations appropriately. You must also work with the groups that will use or consume data from Operations Manager. This means not only the helpdesk and application administration teams but also their management, who will likely be consuming the reports from Operations Manager and who will want to know the status of their application at a single glance.

After you have completed the requirements gathering, compile the data and then publish it in a public way for all the interested parties to see. This provides another opportunity to clarify capabilities. To further ensure agreement on the requirements, you can choose to have the project sponsors and key stakeholders sign off on them.

Business Requirements

The business owners that you need to work with are not just the top-level executives who are sponsoring your Operations Manager project; they are the managers and directors who are responsible for the business processes that make your company money. They might not be particularly interested in Operations Manager as a product, but they are very interested in the level of service that IT is providing to support their mission-critical applications.

When you are having your discussions with people in these roles, their interests will likely center on four areas:

 Ongoing service from IT

 Performance information about their application

 Regulatory compliance

 Return on IT costs

Ongoing Service from IT

What business owners primarily want from IT is to make sure that their application is up and running. If it is not, they must know immediately. They will want to know the impact of the outage on their business process and its expected duration. Understanding their business process is key to meeting their needs. In your conversations with them, make sure you understand these points:

 What are the applications they use to perform operations that affect their core business? Knowing this identifies which applications you must provide end-to-end service monitoring for.

 What are the components of those applications? Knowing this helps you build a distributed application model that you will monitor.

 Does the application have a critical component that runs on workstations or other clients? Knowing this will help you plan your client monitoring strategy.

 Have them describe a complete transaction in their application. Operations Manager 2007 can use synthetic transactions to regularly test an application, as well as provide monitoring data of the end-user experience with the application.

Performance Information

When you are discussing what the business owners need to know about application performance information, it is important to distinguish between business process performance and application performance. Business process performance (or metrics) are provided by business intelligence applications, usually in the form of reports and balanced scorecards, and are not part of this conversation. The expectations that you must understand here are those relating to application performance. Make sure you understand and discuss these points:

 What application performance information are they receiving today? What would they like to receive? Knowing this will help you with role planning (profiles and scopes).

 How are they receiving application performance information today? How would they like to receive it? Knowing this helps you decide how to provide access to the performance information. For example, do they need an Operations console with Read-Only Operator and Reports access scoped to their application, or would the Web console suffice?

Regulatory Compliance

Regulatory compliance is a critical issue with business process owners now and into the future. The business process owners look to IT to participate in the company's plans to achieve compliancy and to stay compliant. Be sure to cover these points:

 Does the business process fall under regulation? If it does, what do the regulations state? Knowing this will help with your Audit Collection Service (ACS) planning and role planning.

 What sort of data is the business process owner looking to IT to provide and for what time frames? This will help with reporting planning and data-retention planning.

Return on IT Costs

Either through direct charge backs or through an indirect overhead charge, the business owners are paying for IT services, and like all good business owners, they want to know what they are getting for their payments. You can use Operations Manager Reporting as a vehicle for providing these answers, but you need to know what it is the business owner finds value in. Be sure to cover these points:

 What do they see as the most valuable services that IT provides to them? Knowing this helps with report planning.

 Are they aware of what they are getting for their IT overhead now? Knowing this, you might choose to assemble different reports that demonstrate the services provided to the business owner that are outside of their application.

IT Requirements

The IT requirements are going to drive the topology of Operations Manager and its supporting infrastructure. The two main factors that will shape your IT requirements are your optimization goals and the IT environment that Operations Manager will exist in. You will gather these requirements from IT sponsors, key stakeholders, and consumers of Operations Manager data. These conversations should consist of broad, open-ended questions on your part. Start by asking how Operations Manager should be used in the environment and what the implementation should be optimized for. Be sure to cover the following points.

Optimization Goals

Optimization goals are aspects of your Operations Manager implementation that must be met by the design. They are exemplified by statements such as the following:

 Availability/Recoverability--Operations Manager must be available with minimal outages. Knowing this helps you with your high availability and backup/recovery planning.

 Cost--Operations Manager must be implemented as economically as possible. Knowing and operating within the budgetary constraints is critical to the success of the project.

 Performance--For example, Operations Manager must report data from the environment in no more than 1 minute and console access must occur in no more than 10 seconds after the console is launched. Knowing this helps with the hardware planning.

 Scope--Operations Manager must provide a single view of the entire environment. Knowing this helps you with planning the number of management groups that will be needed and the relationships between them.

 Administration--Operations Manager administration must be restricted (or available) to certain groups. Knowing this helps you plan security groups, roles, access, and potentially the number of management groups that you will implement.

 Location of Access Points--Operations Manager data must be accessible only from within the company's intranet, or it must be available internally and externally. Knowing this helps you plan where Operations consoles and Web consoles will be made available.

 Integration--Operations Manager must integrate with the existing trouble ticketing system or other enterprise-monitoring product. Knowing this helps you plan where Operations Manager and its features will fit in your environment and the role it will play. It also helps you decide if third-party connectors or connectors developed in house will be necessary.

Inventory of Current Environment

Getting an accurate inventory of your current environment helps you in two regards. First, it tells you about what Operations Manager will be monitoring, and second, it tells you the restrictions or boundaries it must operate within. Be sure to include the following points:

 Scale--The approximate number of devices that will be monitored.

 Management packs needed--The applications that will be monitored.

 Type of devices that support the applications—This list includes Windows computers, network devices, and UNIX or Linux-based computers.

 Topology--The physical and network location of the devices that will be monitored.

 Topology and console distribution--The physical and network location of the people who will use Operations Manager data.

 Certificate and gateway server needs--Your environment's Active Directory Trust boundaries.

 Current Management and Helpdesk products--All other products that are used to perform monitoring, alerting, and reporting.

 Topology and gateway planning--Firewalls and wide area network (WAN) links that define network boundaries.

 Topology and role planning--IT administrative boundaries for monitored devices and applications.

 Topology and localization--Language and geopolitical boundaries that your environment spans.

Inventory Current Procedures

In one way or another, all environments are monitored and managed. The techniques and technologies used to accomplish this vary in levels of sophistication and maturity. Following the Infrastructure Optimization Model, all environments can be described by using four categories: Basic, Standardized, Rationalized, and Dynamic. See [the Infrastructure Optimization Assessment](http://go.microsoft.com/fwlink/?LinkId=112191) for more information about these four categories and a self-evaluation tool to provide an estimate as to where your process and environment lie.

To plan how the capabilities of Operations Manager 2007 will be used, you must understand the procedures that are used to monitor and manage your environment now. This will help you plan how alert information is responded to and who responds to it. It will help you plan how notifications are sent out and who receives them. It will help you plan out administrative control of management groups and data security.

Following are the main questions to ask in this phase:

 How does my organization perform monitoring today?

 How does my organization act on information provided by the monitoring process/system?

Also be sure to cover these points:

 Who normally responds to issues or alerts that are raised by automated systems or helpdesk? Knowing this will help determine who needs direct access to the Operations console and what data the console should contain.

 Does the help desk usually resolve server issues, or are issues passed to the server support teams?

 Does the company have a manned Network Operations Center or other manned monitoring system in place? If yes, how many people and how many consoles are in continuous use? This helps determine where management groups can be placed so that they will receive adequate support.

 How many locations other than datacenters will have agents deployed to them, and where are they on the network?

 What are the available bandwidth statistics between the sites where managed devices are and the sites where the management servers are?

 How is security logging performed currently?

 How are desktop or client applications monitored currently?

 How is monitoring performed for UNIX-based or Linux-based computers and network devices?

Mapping Requirements to a Design for Operations Manager 2007

Mapping Requirements to a Design

In the previous section, you completed the following three tasks:

 You gathered the business requirements, which help you plan which features of Operations Manager to implement.

 You gathered the IT requirements, which help you plan the management group topology.

 You inventoried how your company currently performs monitoring, which helps you plan how to configure Operations Manager.

This section guides you through the design decisions that map all the information and knowledge that has been collected to an actual design. This will be done by applying best practices for sizing and capacity planning for server roles and components. This includes Audit Collection Services (ACS), management servers, RMS, agentless exception monitoring (AEM), gateway servers, collective client monitoring.

Management Group Design

All Operations Manager 2007 implementations consist of at least one management group, and given the scalability of Operations Manager 2007, for some implementations, a single management group might be all that is needed. Depending on the requirements of the company, additional management groups might be needed immediately or might be added over time. The process of distributing Operations Manager services among multiple management groups is called partitioning.

This section addresses the general criteria that would necessitate multiple management groups. Planning the composition of individual management groups, such as determining the sizing of servers and distribution of Operations Manager roles among servers in a management group, is covered in the "Management Group Composition" section.

One Management Group

Approach your Operations Manager management group planning with the same mindset as you have with Active Directory domain planning: start with one management group, and add on as necessary. A single Operations Manager 2007 R2 management group can scale along the following recommended limits:

 3,000 agents reporting to a management server.

 Most scalability, redundancy, and disaster recovery requirements can be met by using from three to five management servers in a management group.

 50 Operations consoles open simultaneously.

 1,500 agents reporting to a gateway server.

 25,000 Application Error Monitoring (AEM) machines reporting to a dedicated management server.

 100,000 AEM machines reporting to a dedicated management group.

 2,500 Collective Monitoring agents reporting to a management server.

 10,000 Collective Monitoring agents reporting to a management group.

 6000 total agents and UNIX or Linux computers per management group with 50 open consoles

 10,000 total agents and UNIX or Linux computers per management group with 25 open consoles

 500 UNIX or Linux computers monitored per dedicated management server.

 100 UNIX or Linux computers monitored per dedicated gateway

 3000 URLS can be monitored per dedicated management server

 12,000 URLs can be monitored per dedicated management group

 50 URLs can be monitored per agent

Click this link for the recommended limits for [Operations Manager 2007 SP1](http://go.microsoft.com/fwlink/?LinkId=152381).

When you consider these limits in conjunction with the security scopes offered through the use of Operations Manager roles to control access to data in the Operations console, a single management group is very scalable and will suffice in many situations.

Multiple Management Groups and Partitioning

As scalable as a management group is, if your requirements include any of the following scenarios, you will need more than one management group:

 Production and Pre-Production Functionality—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 it is migrated into the production environment. In addition, some companies employ a staging environment for servers where newly built servers are placed for a burn-in period prior to being placed into production. The pre-production management group can be used to monitor the staging environment to ensure the health of servers prior to production rollout.

 Dedicated ACS Functionality—If your requirements include the need to collect the Windows Audit Security log events, you will be implementing the Audit Collection Service (ACS). It might be beneficial to implement a management group that exclusively supports the ACS function if your company's security requirements mandate that the ACS function be controlled and administered by a separate administrative group other than that which administers the rest of the production environment.

 Disaster Recovery Functionality—In Operations Manager 2007, all interactions with the OperationsManager database are recorded in transaction logs prior to being committed to the database. Those transaction logs can be sent to another Microsoft SQL Server 2005 SP1 or higher or Microsoft SQL Server 2008 SP1 server and committed to a copy of the OperationsManager database there. This technique is called log shipping. The failover location must contain the failover SQL Server that receives the shipped logs and at least one management server that is a member of the source management group. If it is necessary to execute a failover, you must edit the registry on the management server in the failover location to point it to the failover SQL Server and restart the System Center Management Service. Then promote the failover management server to the RMS role. To complete the failover and return the management group to full functionality you then change the registry on all the remaining management servers in the management group to point to the failover SQL server and restart the System Center Management Service on each management server.

 Increased Capacity—Operations Manager 2007 has no built-in limits regarding the number of agents that a single management group can support. Depending on the hardware that you use and the monitoring load (more management packs deployed means a higher monitoring load) on the management group, you might need multiple management groups in order to maintain acceptable performance.

 Consolidated Views—When multiple management groups are used to monitor an environment, a mechanism is needed to provide a consolidated view of the monitoring and alerting data from them. This can be accomplished by deploying an additional management group (which might or might not have any monitoring responsibilities) that has access to all the data in all other management groups. These management groups are then said to be connected. The management group that is used to provide a consolidated view of the data is called the Local Management Group, and the others that provide data to it are called Connected Management Groups.

 Installed Languages—All servers that have an Operations Manager server role installed on them must be installed in the same language. That is to say that you cannot install the RMS using the English version of Operations Manager 2007 and then deploy the Operations console using the Japanese version. If the monitoring needs to span multiple languages, additional management groups will be needed for each language of the operators.

 Security and Administrative—Partitioning management groups for security and administrative reasons is very similar in concept to the delegation of administrative authority over Active Directory Organizational Units or Domains to different administrative groups. Your company might include multiple IT groups, each with their own area of responsibility. The area might be a certain geographical area or business division. For example, in the case of a holding company, it can be one of the subsidiary companies. Where this type of full delegation of administrative authority from the centralized IT group exists, it might be useful to implement management group structures in each of the areas. Then they can be configured as Connected management groups to a Local management group that resides in the centralized IT data center.

The preceding scenarios should give you a clear picture of how many management groups you will need in your Operations Manager infrastructure. The next section covers the distribution of server roles within a management group and the sizing requirements for those systems.

Management Group Composition

There are few limitations on the arrangement of Operations Manager server components in a management group. They can all be installed on the same server (except the gateway server role), or they can be distributed across multiple servers in various combinations. Some roles can be installed into a Cluster service (formerly known as MSCS) failover cluster for high availability, and multiple management servers can be installed to allow agents to fail over between them. You should choose how to distribute Operations Manager server components and what types of servers will be used based on your IT requirements and optimization goals.

Server Role Compatibility

An Operations Manager 2007 management group can provide a multitude of services. These services can be distributed to specific servers, thereby classifying a server into a specific role. Not all server roles and services can coexist. The following table lists the compatibilities and dependencies and notes whether the role can be installed on a failover cluster:

|  |  |  |  |
| --- | --- | --- | --- |
| Server role | Compatible with other roles | Requirements | Can be placed in a quorum failover cluster |
| Operational database | Yes | SQL | Yes |
| Audit Collection Services (ACS) database | Yes | SQL | Yes |
| Reporting Data Warehouse database | Yes | SQL | Yes |
| Reporting | Yes | Dedicated SQL Server Reporting Services instance; not on a domain controller | No |
| root management server | Yes | Not compatible with management server or gateway server role | Yes |
| management server | Yes | Not compatible with root management server | No |
| Administrator console | Yes | Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008 | N/A |
| ACS collector | Yes | Can be combined with gateway server and audit database | No |
| gateway server | Yes | Can be combined with ACS collector only; must be a domain member | No |
| Web console server | Yes |  | N/A |
| agent | Yes | Automatically deployed to root management server and management server in a management group | N/A |

All the recommendations made here are based on these assumptions:

 The disk subsystem figures are based on drives that can sustain 125 random I/O operations per second per drive. Many drives can sustain higher I/O rates, and this might reduce the number of drives required in your configuration.

 In management groups that have management servers deployed in addition to the RMS, all agents should use the management servers as their primary and secondary management servers and no agents should be using the RMS as their primary or secondary management server.

 The Agentless Exception Monitoring guidance assumes that there are approximately one to two crashes per machine per week, with an average CAB file size of 500 KB.

 Collective Client Monitoring includes only out-of-the-box client-specific management packs, including the Windows Vista, Windows XP, and Information Worker Management Packs.

 All connectivity between agents and servers is at 100 Mbps or better.

Availability

The need for high availability for the databases, the RMS, management servers, and gateway servers can be addressed by building redundancy into the management group.

 Database—All databases used in Operations Manager 2007 require Microsoft SQL Server 2005 SP1 or higher or Microsoft SQL Server 2008 SP1 or higher, which can be installed into a MSCS quorum node failover configuration.

Note

For more information on Cluster services, refer to the Windows Server 2003 and Windows Server 2008 online help.

 RMS—The System Center Data Access service and System Center Management Configuration service run only on the RMS, and this makes them a single point of failure in the management group. Given the critical role that the RMS plays, if your requirements include high availability, the RMS should also be installed into its own two-node failover cluster. For complete details on how to cluster the RMS, see the Operations Manager 2007 Deployment Guide.

 Management servers—In Operations Manager, agents in a management group can report to any management server in that group. Therefore, having more than one management server available provides redundant paths for agent/server communication. The best practice then is to deploy one or two management servers in addition to the RMS and to use the Agent Assignment and Failover Wizard to assign the agents to the management servers and to exclude the RMS from handling agents.

 Gateway servers—Gateway servers serve as a communications intermediary between management servers and agents that lie outside the Kerberos trust boundary of the management servers. Agents can fail over between gateway servers just as they can between management servers if communications with the primary server of either one is lost. Likewise, gateway servers can be configured to fail over between management servers, providing a fully redundant set of pathways from the agents to the management servers. See the Operations Manager 2007 Deployment Guide for procedures on how to deploy this configuration.

Cost

The more distributed the management group server roles are, the more resources will be needed to support that configuration. This includes hardware, environment, licensing, operations, and maintenance overhead. Designing with cost control as the optimization goal moves you in the direction of a single-server implementation or minimal role distribution; this in turn reduces redundancy and, potentially, performance.

Performance

With performance as an optimization goal, you will be better served, with a more distributed configuration and higher-end hardware. Commensurately, cost will rise.

Console Distribution and Location of Access Points

The Operations console communicates directly with the RMS and, when the Reporting component is installed, with the Reporting server. Planning the location of the RMS and the database servers, then, in relationship to the Operations console is critical to performance. Be sure to keep these components in close network proximity to each other.

Recommended Component Distribution and Platform Sizing

The following tables present recommendations for component distribution and platform sizing for Operations Manager 2007 R2. Click this link for recommendations on component distribution and platform sizing for [Operations Manager 2007 SP1](http://go.microsoft.com/fwlink/?LinkId=152381). In these tables, DB is a SQL database server, DW is a SQL database server, RS is the Reporting server, RMS is the root management server, and MS is a management server. Basic ACS design and planning is presented later in this paper.

Note

For additional information on sizing Operations Manager infrastructure, see the [Operations Manager 2007 R2 Sizing Helper](http://go.microsoft.com/fwlink/?LinkID=200081) at http://go.microsoft.com/fwlink/?LinkID=200081

Single Server, All-in-One Scenario

|  |  |
| --- | --- |
| # of Monitored Devices | Server Roles and Config |
| 15 to 250 Windows computers, 200 UNIX or Linux computers | DB, DW, RS, RMS;  4-disk RAID 0+1, 8 GB RAM, quad processors |

Multiple Server, Small Scenario

|  |  |  |
| --- | --- | --- |
| # of Monitored Devices | Server Roles and Config | Server Roles and Config |
| 250 to 500 Windows computers, 500 UNIX or Linux computers | DB, DW, RS;  4-disk RAID 0+1, 4 GB RAM, dual processors | RMS;  2-disk RAID 1, 4 GB RAM, dual processors |

Multiple Servers, Medium Scenario

To allow for redundancy, you can deploy multiple management servers, each with the described minimum configuration. To provide high availability for the database and RMS servers, you can deploy them into a cluster, with each node having the described minimum configuration plus connections to an externally shared disk for cluster resources.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # of Monitored Devices | Server Role and Config | Server Role and Config | Server Role and Config | Server Role and Config |
| 500 to 750 Windows computers, 500 UNIX or Linux computers | DB;  4-disk RAID 0+1, 4 GB RAM, dual processors | MS;  2-disk RAID 1, 4 GB RAM, dual processors | DW, RS;  4-disk RAID 0+1 (data), 2-disk RAID 1 (logs), 4 GB RAM, dual processors | RMS;  2-disk RAID 1, 8 GB RAM, dual processors |

Multiple Servers, Large Scenario

To allow for redundancy, you can deploy multiple management servers, each with the described minimum configuration. To provide high availability for the database and RMS servers, you can deploy them into a cluster, with each node having the described minimum configuration plus connections to an externally shared disk for cluster resources.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # of Monitored Devices | Server Role and Config | Server Role and Config | Server Role and Config | Server Role and Config | Server Role and Config |
| 750 to 1000 Windows computers, Unix or Linux computers | DB;  4-disk RAID 0+1 (data), 2-disk RAID 1 (logs), 8 GB RAM, dual processors | DW;  4-disk RAID 0+1 (data), 2-disk RAID 1 (logs), 8 GB RAM, dual processors. Note: a RAID 5 configuration with similar performance can be used to fulfill the DW storage needs. | RS;  2-disk RAID 1, 4 GB RAM, dual processors | RMS;  2-disk RAID 1, 8 GB RAM, dual processors | MS;  2 disk RAID 1, 4 GB RAM, quad processors |

Multiple Server, Enterprise

To allow for redundancy, you can deploy multiple management servers, each with the described minimum configuration. To provide high availability for the database and RMS servers, you can deploy them into a cluster, with each node having the described minimum configuration plus connections to an externally shared disk for cluster resources.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # of Monitored Devices | Server Role and Config | Server Role and Config | Server Role and Config | Server Role and Config | Server Role and Config |
| 1,000 to 3,000 Windows computers, 500 UNIX or Linux computers | DB;  8-disk RAID 0+1 (data), 2-disk RAID 1 (logs), 8 GB RAM, quad processors | DW;  8-disk RAID 0+1 (data), 2-disk RAID 1 (logs), 8 GB RAM, quad processors | RS;  2-disk RAID 1, 4 GB RAM  quad processors | RMS;  4-disk RAID 0+1, 12 GB RAM, 64-bit quad processors | MS;  4-disk RAID 0+1, 8 GB RAM, quad processors |
| 3,000 to 6,000 Windows computers, UNIX or Linux computers | DB;  14-disk RAID 0+1 (data), 2-disk RAID 1 (logs), 16 GB RAM, quad processors | DW;  14-disk RAID 0+1 (data), 2-disk RAID 1 (logs), 16 GB RAM, quad dual processors. Note a RAID 5 configuration with similar performance can be used to meet the DW storage needs. | RS;  2-disk RAID 1, 4 GB RAM, quad processors | RMS;  4-disk RAID 0+1, 16 GB RAM, quad processors | MS;  2-disk RAID 0+1, 8 GB RAM, quad processors |

Component Guidelines and Best Practices

In addition to the sizing guidance just given, there are additional considerations and best practices when planning for each of the Operations Manager server components.

Root Management Server Guidelines and Best Practices

On the RMS, the most critical resources are RAM and CPU, as many of the operations that the RMS performs are memory intensive and thus suffer from excessive paging. Factors that influence RMS load include the following:

 Number of agents in the management group—Because the RMS must compute the configuration for all agents in the management group, increasing the number of agents increases the amount of memory required on the RMS, regardless of the volume of operations data the agents send.

 Rate of instance space changes—The instance space is the data that Operations Manager maintains to describe all the monitored computers, services, and applications in the management group. Whenever this data changes frequently, additional resources are needed on the RMS to compute configuration updates for the affected agents. The rate of instance space changes increases as you import additional management packs into your management group. Adding new agents to the management group also temporarily increases the rate of instance space changes.

 Number of concurrent Operations consoles and other SDK clients—Examples of other SDK clients include the Web console and many third-party tools that interface with Operations Manager. Because the SDK Service is hosted on the RMS, each additional connection uses memory and CPU.

Some best practices around sizing RMS include the following:

 Use 64-bit hardware and operating system—Using 64-bit hardware enables you to easily increase memory beyond 4 GB. Even if your current deployment does not require more than 4 GB of RAM, using 64-bit hardware gives you room for growth if the requirements change in the future.

 Limit the number or eliminate agents reporting to the RMS—In management groups with smaller agent counts, it’s typically fine to have agents report directly to the RMS. This reduces the overall cost of the hardware required for your installation. However, as the number of agents increases, you should consider restricting any agents from directly reporting to the RMS. Moving the agent workload to other management servers reduces the hardware requirements for the RMS and generally results in better performance and reliability from the management group.

 Ensure high bandwidth network connectivity to the OperationsManager database and the Data Warehouse—The RMS frequently communicates with the Operations Database and Data Warehouse. In general, these SQL connections consume more bandwidth and are more sensitive to network latency than connections between agents and the RMS. Therefore, you should generally ensure that the RMS, OperationsManager database, and Data Warehouse database are on the same local area network.

Operations Database Guidelines and Best Practices

As with all database applications, the Operations database performance is most affected by the performance of the disk subsystem. Because all Operations Manager data must flow through the OperationsManager database, the faster the disk the better the performance. CPU and memory affect performance as well. Factors that influence the load on the OperationsManager database include the following:

Note

To calculate the OperationsManager database size, use the [Operations Manager 2007 R2 Sizing Helper Tool](http://go.microsoft.com/fwlink/?LinkID=200081) at http://go.microsoft.com/fwlink/?LinkID=200081

 The rate of data collection—The RMS frequently communicates with the Operations Database and Data Warehouse. In general, these SQL connections consume more bandwidth and are more sensitive to network latency than connections between agents and the RMS. Therefore, you should generally ensure that the RMS, OperationsManager database, and Data Warehouse database are on the same local area network.

 The rate of instance space changes—The instance space is the data that Operations Manager maintains to describe all the monitored computers, services, and applications in the management group. Updating this data in the OperationsManager database is costly relative to writing new operational data to the database. Additionally, when instance space data changes, the RMS makes additional queries to the OperationsManager database to compute configuration and group changes. The rate of instance space changes increases as you import additional management packs into your management group. Adding new agents to the management group also temporarily increases the rate of instance space changes.

 Concurrent Operations console and other SDK clients—Each open instance of the Operations console reads data from the OperationsManager database. Querying this data consumes potentially large amounts of disk activity as well as CPU and RAM. Consoles displaying large amounts of operational data in the Events View, State View, Alerts View, and Performance Data View tend to put the largest load on the database. To achieve maximum scalability, consider scoping views to include only necessary data.

Following are some best practices for sizing the OperationsManager database server:

 Choose an appropriate disk subsystem—The disk subsystem for the OperationsManager database is the most critical component for overall management group scalability and performance. The disk volume for the database should typically be RAID 0+1 with an appropriate number of spindles. RAID 5 is typically an inappropriate choice for this component because it optimizes storage space at the cost of performance. Because the primary factor in choosing a disk subsystem for the OperationsManager database is performance rather than overall storage space, RAID 0+1 is more appropriate. When your scalability needs do not exceed the throughput of a single drive, RAID 1 is often an appropriate choice because it provides fault tolerance without a performance penalty.

 The placement of data files and transaction logs—For lower-scale deployments, it is often most cost-effective to combine the SQL data file and transaction logs on a single physical volume because the amount of activity generated by the transaction log isn’t very high. However, as the number of agents increases, you should consider placing the SQL data file and transaction log on separate physical volumes. This allows the transaction log volume to perform reads and writes more efficiently. This is because the workload will consist of mostly sequential writes. A single two-spindle RAID 1 volume is capable of handling very high volumes of sequential writes and should be sufficient for almost all deployments, even at a very high scale.

 Use 64-bit hardware and operating system—The OperationsManager database often benefits from large amounts of RAM, and this can be a cost-effective way of reducing the amount of disk activity performed on this server. Using 64-bit hardware enables you to easily increase memory beyond 4 GB. Even if your current deployment does not require more than 4 GB of RAM, using 64-bit hardware gives you room for growth if your requirements change in the future.

 Use a battery-backed write-caching disk controller—Testing has shown that the workload on the OperationsManager Database benefits from write caching on disk controllers. When configuring read caching vs. write caching on disk controllers, allocating 100 percent of the cache to write caching is recommended. When using write-caching disk controllers with any database system, it is important to ensure they have a proper battery backup system to prevent data loss in the event of an outage.

Data Warehouse Guidelines and Best Practices

In Operations Manager 2007, data is written to the Data Warehouse in near real time. This makes the load on it similar to the load on the OperationsManager database machine. Because it is a SQL Server, the disk subsystem is the most critical to overall performance, followed by memory and CPU. Operations Manager Reporting Services also places a slightly different load on the Data Warehouse server. Factors that affect the load on the Data Warehouse include the following:

 Rate of data insertion—To allow for more efficient reporting, the Data Warehouse computes and stores aggregated data in addition to a limited amount of raw data. Doing this extra work means that operational data collection to the Data Warehouse can be slightly more costly than to the OperationsManager database. This additional cost is typically balanced out by the reduced cost of processing discovery data on the Data Warehouse as opposed to processing it on the OperationsManager database.

 Numbers of concurrent reporting users—Because reports frequently summarize large volumes of data, each reporting user can put a significant load on the system. Both the number of reports run at the same time and the type of reports being run affect overall capacity needs. Generally, reports that query large date ranges or large numbers of objects demand more system resources.

Following are some best practices when sizing the Data Warehouse server:

 Choose an appropriate disk subsystem—Because the Data Warehouse is now an integral part of the overall data flow through the management group, choosing an appropriate disk subsystem for the Data Warehouse is very important. As with the OperationsManager database, RAID 0+1 is often the best choice. In general, the disk subsystem for the Data Warehouse should be similar to the disk subsystem for the OperationsManager database.

 Placement of the data files and the transaction logs—As with the OperationsManager database, separating SQL data and transaction logs is often an appropriate choice as you scale up the number of agents. If both the OperationsManager database and Data Warehouse are located on the same physical machine and you want to separate data and transaction logs, you must put the transaction logs for the OperationsManager database on a separate physical volume from the Data Warehouse to see any benefit. The data files for the OperationsManager database and Data Warehouse can share the same physical volume, as long as it is appropriately sized.

 Use 64-bit hardware and operating system—The Data Warehouse often benefits from large amounts of RAM, and this can be a cost-effective way of reducing the amount of disk activity performed on this server. Using 64-bit hardware enables you to easily increase memory beyond 4 GB. Even if your current deployment does not require more than 4 GB of RAM, using 64-bit hardware gives you room for growth if your requirements change in the future.

 Use dedicated server hardware for the Data Warehouse—Although lower-scale deployments can often consolidate the OperationsManager database and Data Warehouse onto the same physical machine, it is advantageous to separate them as the number of agents increases and, consequently, the volume of incoming operational data increases as well. You will also see better reporting performance if the Data Warehouse and Reporting servers are separated.

 Use a battery-backed write-caching disk controller—Testing has shown that the workload on the Data Warehouse benefits from write caching on disk controllers. When configuring read caching versus write caching on disk controllers, allocating 100 percent of the cache to write caching is recommended. When using write-caching disk controllers with any database system, it is important to ensure they have a proper battery backup system to prevent data loss in the event of an outage.

Management Server Guidelines and Best Practices

The largest portion of the load on a management server is from the collection of operational data and the insertion of that data into the OperationsManager and Data Warehouse databases. It is important to note that management servers perform these operations directly without depending on the RMS. Management servers perform most of the data queuing in memory rather than depending on a slower disk, thereby increasing performance. The most important resource for management servers is the CPU, but testing has shown that they typically do not require high-end hardware. Factors that affect load on a management server include the following:

 Rate of operational data collection—Because operations data collection is the primary activity performed by a management server, this rate has the biggest impact on overall server utilization. However, testing has shown that management servers can typically sustain high rates of operational data processing with low to moderate utilization. The primary factor affecting the rate of operational data collection is which management packs are deployed in the management group.

Following are some best practices when sizing a management server:

 Do not oversize management server hardware.—For most scenarios, using a standard utility server is sufficient for the work performed by a management server. Following the hardware guidelines in this document should be sufficient for most workloads.

 Do not exceed an agent-to-management-server ratio of about 3,000 to 1—Actual server performance will vary based on the volume of operations data collected, but testing has shown that management servers typically do not have issues supporting 2,000 agents each with a relatively high volume of operational data coming in. Having 2,000 agents per management server is a guideline based on test experience and not a hard limit. You might find that a management server in your environment is able to support a higher or lower number of agents.

 To maximize the UNIX or Linux computer-to-management-server ratio (500:1), use dedicated management servers for cross-platform monitoring.

 Use the minimum number of management servers per management group to satisfy redundancy requirements—The main reason for deploying multiple management servers should be to provide for redundancy and disaster recovery rather than scalability. Based on testing, most deployments will not need more than three to five management servers to satisfy these needs.

Gateway Server Guidelines and Best Practices

Gateway servers relay communications between management servers and agents that lie on opposite sides of Kerberos trust boundaries from each other. The gateway server uses certificate-based authentication to perform mutual authentication with the management server, and it does so using a single connection rather than multiple connections as would be required between the agents and the management server. This makes managing certificate-based authentication to untrusted domains easier and more manageable. Factors that affect load on a gateway server include the following:

 Rate of operations data collection—The primary factor that influences the load on a gateway is the rate of operations data collection. This rate is a function of the number of agents reporting to the gateway and the management packs deployed within the management group.

Following are some best practices when sizing a gateway server:

 Gateway servers can be beneficial in managing bandwidth utilization—From a performance perspective, gateways are recommended as a tool to optimize bandwidth utilization in low-bandwidth environments as it performs a level of compression on all communications with the management server.

 Do not exceed an agent-to-Gateway-Server ratio of about 1,500 to 1—Testing has shown that having more than 1,000 agents per gateway can adversely affect the ability to recover in the event of a sustained (multi-hour) outage that causes a gateway to be unable to communicate with the management server. If you need more agents than this to be reporting to a gateway, consider using multiple gateway servers. If you want to exceed 1,500 agents per gateway, it is highly recommended that you test your system to ensure that the gateway is able to quickly empty its queue after a sustained outage between the gateway and the management server if gateway recovery time is a concern in your environment.

 For large numbers of gateways and gateway connected agents, use a dedicated management server—Having all gateways connect to a single management server with no other agents connected to it can speed recovery time in the event of a sustained outage.

Application Error Monitoring Guidelines and Best Practices

The management server used for AEM receives the data from the Error Reporting Client and stores it to a file share. If that file share is local, this will affect the management server.

Following are some best practices when planning for AEM:

 Disk storage for the files hare can be local or on a Network Attached Storage (NAS) or storage area network (SAN) device.

 The disk used for AEM should be separate from the disk used for the Data Warehouse or OperationsManager databases.

 If the storage is set up on a Distributed File System (DFS), DFS replication should be disabled.

 A gateway server should not be used as an AEM collector.

|  |  |
| --- | --- |
| # of Monitored Devices | management server for AEM file share |
| 0 to 10,000 | 200 GB of disk as 2 drives RAID 1, 4 GB RAM, dual processors |
| 10,000 to 25,000 | 500 GB of disk as 2 drives RAID 1, 8 GB RAM, quad processors |

URL Monitoring Guidelines and Best Practices

URL monitoring can be performed by the Health Service of an agent or a management server. If you are monitoring more than 1000 URLs from a management server, you should increase the Health Service Version Store page size from the default of 5120 pages to 10240 pages. This is done in the HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\HealthService\Parameters\Persistence Version\Store Maximum. A management server that is performing URL monitoring will have a heavy load placed on its CPU and disk resources, and it is recommended to use a battery backed cache controller.

Collective Client Monitoring Guidelines and Best Practices

Collective Health Monitoring is performed by gathering event and performance data from many machines and aggregating the data based on groups of systems for reporting and analysis. For example, individual memory performance data is gathered from Windows XP and Windows Vista clients on different types of hardware. Collective Health Monitoring aggregates this data and provides reports based on memory performance for specific groups of systems, such as by operating system or by hardware vendor. This makes analysis of overall performance easier than the alternative of digging through long lists of individual system performance reports. Collective monitoring mode also enables alerting and monitoring at a collective, rather than an individual, level.

Collective Client monitoring management packs include the following: Information Worker, Windows Client, Windows XP, Windows Vista, Network Address Protocol, and other client-focused management packs.

Each client that is monitored by an agent typically generates summary events periodically, and these events are used to calculate the collective health of the client population. Alerting on the individual agent is disabled, and hence, there will not be any alerts data generated by the agents running on the clients.

Depending on the number of management packs deployed and agent traffic, each management server can manage up to 3,000 to 4,000 agent-managed clients.

When planning the rollout of collective monitoring clients, the agents should be approved in batches of no more than 1,000 at a time to allow the agents to get synchronized with the latest configuration.

Designing Audit Collection Services

This section provides high-level guidance to help you get started with planning your ACS implementation.

ACS is not a stand-alone solution. ACS can be hosted only in an existing management group because its agent is integrated and installed with the Operations Manager agent, and the ACS Collector can be installed only on a management server or gateway server. The remaining components, the ACS database and ACS Reporting, can be installed on the same SQL Server 2005 server or instance as the rest of the OperationsManager database and reporting components as well. However, for performance, capacity, and security reasons, you will probably choose to install these on dedicated hardware.

Design Decisions

There are four fundamental design decisions to make when planning your ACS implementation. As you make these decisions, keep in mind that there is a one-to-one relationship between the ACS Collector server and its ACS database. An ACS database can have only one ACS Collector feeding data to it at a time, and every ACS Collector needs its own ACS database. It is possible to have multiple ACS Collector/Database pairs in a management group; however, there are no procedures available out of the box for integrating the data from multiple ACS databases into a single database.

The first decision that must be made is whether or not to deploy a management group that is exclusively used to support ACS or to deploy ACS into a management group that also provides health monitoring and alerting services. Here are the characteristics of these two ACS deployment scenarios.

 ACS hosted in a production management group scenario:

 Scaled usage of ACS—Given that ACS collects every security event from the systems that ACS Forwarders are enabled on, the use of ACS can generate a huge amount of data. Unless you are using dedicated hardware for the ACS Collector and Database roles, processing this data might negatively affect the performance of the hosting management group, particularly in the database layer.

 Separate administration and security is not required—Because ACS is hosted in a management group, people with administrative control in the management group will have administrative rights in ACS. If the business, regulator/audit, and IT requirements mandate that ACS be under nonproduction IT control, deploying ACS into a production management group scenario is not an option.

 ACS hosted on a dedicated management group scenario:

 Separate administration and security is required—If there is a separate administrative group that is responsible for audit and security controls at your company, hosting ACS on a dedicated management group administered by the audit/security group is recommended.

The second decision that must be made is whether or not to deploy ACS Reporting into the same SQL Server 2005 Reporting Services instance as the Operations Manager 2007 Reporting component. Here are the characteristics of these two scenarios.

 ACS reporting integrated with Operations Manager Reporting:

 Single console for all reports—When ACS Reporting is installed with Operations Manager Reporting, the ACS reports are accessed via the Operations Manager Operations console.

 Common security model—When Operations Manager 2007 Reporting is installed into SQL Server 2005 Reporting Services, it overwrites the default security model, replacing it with the Operations Manager role-based security model. ACS Reporting is compatible with this model. All users who have been assigned the Report Operator role will have access to the ACS Reports as long as they also have the necessary permissions on the ACS database.

Note

If Operations Manager Reporting is later uninstalled, the original SRS security model must be restored manually using the ResetSRS.exe utility found on the installation media in the SupportTools directory.

 ACS reporting installed on a dedicated SQL Server Reporting Services instance:

 Separate console for ACS and Operations Manager reports—When installed on a dedicated SRS instance, the ACS Reports are accessed via the SRS Web site that is created for it at installation. This provides greater flexibility in configuring the folder structure and in using SRS Report designer.

 Separate security model—A consequence of using a dedicated SRS instance is that you can create security roles as needed to meet the business and IT requirements to control access to the ACS reports. Note that the necessary permissions must still be granted on the ACS database.

The third design decision that must be made is how many ACS Collector/Database pairs to deploy to support your environment. The rate that a single ACS Collector/Database pair can support an ongoing event collection and insertion is not an absolute number. This rate is dependent upon the performance of the storage subsystem that the database server is attached to. For example a low-end SAN solution can typically support up to 2,500 to 3,000 security events per second. Independent of this the ACS Collector has been observed supporting bursts of 20,000 security events per second. Following are factors that affect the number of security events generated per second:

 Audit Policy Configuration—The more aggressive the audit policy, the greater the number of Security events that are generated from audited machines

 The role of the machine that the ACS forwarder is enabled on, given the default Audit Policy, Domain Controller will generate the most security events. Member servers will generate the next highest amount, and workstations will generate the least.

|  |  |
| --- | --- |
| Machine Role | Approximate Number of Unfiltered Security Events per Second generated under high load |
| Windows Server 2003 Domain Controller | 40 events per second |
| Windows Server 2003 Member Server | 2 events per second |
| Workstation | 0.2 events per second |

 Using the numbers in the preceding table, a single, high-end ACS Collector/Database pair can support up to 150 Domain Controllers, 3,000 Member Servers, or 20,000 Workstations (with the appropriate ACS Collector filter applied).

 The amount of user activity on the network—If your network is used by high-end users conducting a large number of transactions, as is experienced, for example, at Microsoft, more events will be generated. If your network users conduct relatively few transactions, such as might be the case at a retail kiosk or in a warehouse scenario, you should expect fewer security events.

 The ACS Collector Filter configuration—ACS collects all security events from a monitored machine's security event log. Out of all the events collected, you might be interested in only a smaller subset. ACS provides the ability to filter out the undesired events, allowing only the desired ones to be processed by the Collector and then inserted into the ACS database. As the amount of filtering increases, fewer events will be processed and inserted into the ACS database.

The last design decision that must be made is the version of SQL Server 2005 or SQL Server 2008 to use for the ACS database. ACS supports the use of SQL Server 2005 Standard edition and SQL Server 2005 Enterprise edition or SQL Server 2008 Standard or Enterprise editions. Which version is used has an impact on how the system will behave during the daily database maintenance window. During the maintenance window, database partitions whose time stamps lie outside the data retention schedule (with 14 days being a typical configuration for data retention) are dropped from the database. If SQL Server Standard edition is used, Security event insertion halts and events queue up on the ACS Collector until maintenance is completed. If SQL Server Enterprise edition is used, insertion of processed Security events continues, but at only 30 percent to 40 percent of the regular rate. This is one reason why you should carefully pick the timeframe for daily database maintenance, selecting a time when there is the least amount of user and application activity on the network.

Sizing Audit Collection Services

This section helps you size ACS hardware components before you deploy them by determining how many disks, ACS collectors, and ACS databases are needed.

Important

To effectively size ACS, you must determine the number of disks required for ACS disk I/O and you must determine the ACS database size. The processes of calculating these values are detailed in the "Sizing ACS" section. Each ACS collector must have its own ACS database. The rate of data insertion to the database, which is dictated by the performance of the storage subsystem, determines the capacity of a single ACS collector. The more disks that a single disk array can support, the better it can perform.

Tip

ACS supports the use of SQL Server 2005 Standard Edition and SQL Server 2005 Enterprise Edition; however, the edition you use affects how the system performs during the daily database maintenance window. During the maintenance window, database partitions with time stamps outside of the default 14-day data retention schedule are dropped from the database. If SQL Server 2005 Standard Edition is used, Security event insertion halts and events queue in the ACS Collector until maintenance is completed. If SQL Server 2005 Enterprise Edition is used, Security event insertion continues, but at only at 30 to 40 percent of the regular rate. Therefore, you should carefully pick the timeframe for daily database maintenance, selecting a time when there is the least amount of user and application activity on the network.

Sizing ACS

The number of ACS collectors and the sizing of the ACS database and the sizing of the disk subsystem for the database are entirely dictated by the volume of security events that get forwarded to it as measured in events per second. You perform ACS sizing calculations to find out three things:

1. The number of ACS Collectors you will need

2. How much space you will need to allot for the database

3. How many disks you will need to support the expected throughput on the database

Ideally, you could determine the number of security events generated by computers in your organization by installing a pilot ACS collector to measure the incoming event rate. If you have a pilot ACS collector, you can monitor the ACS Collector\Incoming Event per Sec performance monitor counter. However, if you do not have a pilot ACS collector, you can use the sizing guidelines and script sample that follow to produce similar results.

Use the following procedure to measure the number of events per second for all computers in your organization by using the Events Generated Per Second Script. After you determine the number of events, you use it this number to calculate the number of disks required to handle I/O and the total ACS database size as described in the subsequent sections.

To estimate the number of events per second for all computers

|  |
| --- |
| 1. Identify groups of computers that perform similar functions; for example, domain controllers, member servers, and desktop computers.  2. Count the number of computers in each group for all computers in your organization.  3. Run the script sample contained in the Events Generated Per Second Script section over a 48-hour period on at least one computer in each group to record data. The computer you run the script on represents all computers included in its group.  4. Record the data in a spreadsheet for consolidation and analysis.  5. Based on the data you collect, identify when peak usage occurs.  6. For each computer you collect data from, determine how many events occur per second during peak usage and then multiply it by the number of computers in the represented group. Repeat this step for each group.  7. Add the values together from the previous step to determine the number of events per second for all computers in your organization.  You will use the total value to calculate the number of disk required to handle I/O and to calculate the total ACS database size in the following sections. |

Calculating the number of disks required to handle I/O During testing at Microsoft, the estimated average number of logical disk I/O per event for ACS database logs was 1.384 and the ACS database was 0.138. However, these values may differ slightly depending on the environment. This assumed that the disk revolutions per minute (RPM) has a 1:1 ratio with the logical disk I/O and that a RAID 0+1 configuration is used.

You can use the following formulas to calculate the number of disks required to handle I/O.

For the log drives:

[Average number of disk I/O per event for transaction log] \* [Events per second for all computers] / [disk RPM] \* 60 sec/minute = [number of required drives] \* 2 (for RAID 1)

Values for the preceding variables are described in the following table.

|  |  |
| --- | --- |
| Variable | Value |
| Average number of logical disk I/O per event (for the transaction log file) | 1.384 |
| Estimated events per second for all computers | Estimated by using the script and the To estimate the number of events per second for all computers procedure |
| Disk RPM | Varies, determined by disk device |

For the database drives:

[Average number of disk I/O per event for database file] \* [Events per second for all computers] / [drive RPM] \* 60 sec/minute = [number of required drives] \* [2 for RAID 1]

Values for the preceding variables are described in the following table.

|  |  |
| --- | --- |
| Variable | Value |
| Average number of logical disk I/O per event (for the database file) | 0.138 |
| Estimated events per second for all computers | Estimated by using the script and the To estimate the number of events per second for all computers procedure |
| Disk RPM | Varies, determined by disk device |

If the number of disks required to handle I/O for events exceeds the number of disks you can have in a disk array, you will need to divide the events into multiple collectors.

Calculating the total ACS Database size  
To determine the total ACS database size, use the following formula:

[Events per second for all computers] \* [0.4 KB, which is the size of event] \* 60 sec \*60 min \* 24 hr /1024 MB /1024 GB /1024 TB \* [retention period, which is days to keep in database] = total size of database

Audit Collection Service Guidelines and Best Practices

The overall performance of the ACS system is most affected by the performance of the ACS database and its disk subsystem. Given that many thousands of events per second will be inserted continuously, with potential peaks of tens of thousands per second, this is easy to see. It is not uncommon with a large number of monitored devices, including domain controllers, to accumulate more than a terabyte of data in a 14-day time span in the ACS database. Following are some best practices for ACS:

 Use 64-bit hardware and operating system for the Collector and SQL Server, along with a high-performance SAN solution.

 Separate the database files from the transaction logs.

 Use dedicated hardware to host ACS if warranted.

 Use tight filters to reduce the number of noise Security events that get inserted into the database.

 Plan your Windows Audit policy carefully so that only relevant events are logged on monitored systems.

 Enable the ACS Forwarder only on necessary systems.

 Configure Security Event logs with sufficient space so that if communication is lost with the ACS Collector, the Security Event log file will not wrap on itself and overwrite previous events, resulting in a loss of event data.

Developing an Operations Manager 2007 Implementation Plan

Developing an Implementation Plan

At this point in the design process, you should have several documents:

 A listing of the goals of your Operations Manager 2007 implementation project

 A summary of the business, regulatory, and IT requirements

 A reliable inventory of your current production environment

 A reliable description of the processes used to perform monitoring currently

 A listing of the Operations Manager 2007 services that will be implemented and the components necessary to support those services

 A detailed diagram of your planned management groups and how they will be placed in your environment

 A detailed plan of how Operations Manager will be integrated with your current monitoring processes

 Hardware specifications for the servers in the planned management groups

The last deliverable that this guide will assist you in developing is an implementation plan.

Lab Testing

An implementation plan is simply a moderately detailed listing of the steps necessary to move the monitoring environment from wherever it is now, referred to as the "start state," to where you want it to be, referred to as the "desired end state." There is only one way to develop an implementation plan properly and that is through lab testing. The goal of lab testing as part of implementation plan development is to validate configuration and procedures, not to prove out scalability, as it is usually cost prohibitive to fully model the production environment with all its complexity and load in a lab setting.

Start your lab design by identifying the critical components in your production environment that support the monitoring environment, such as Active Directory and DNS. Also identify components Operations Manager will interact with, such as applications, servers, and workstations.

Secure hardware that will host the start state lab environment. Because you are not testing for scale, consider using Microsoft Virtual Server to host these components as virtual machines. Using Virtual Server has the added advantage of providing the ability to quickly reset the test environment to a clean start state after a testing run. Build the critical components infrastructure and other start state components in this environment. Exercise due diligence here to ensure that the lab environment resembles the production environment as closely as possible. The closer it is in terms of configuration, services, and data, the more valid the subsequent testing will be.

Next, get the hardware that will be used to support the production implementation of your management groups and get it up and running in the lab setting. This gives you the opportunity to confirm that all the hardware is present and working properly. Then compile a rough list of the steps that will be used to perform the Operations Manager deployment. This completes the preparatory steps.

Now you should perform the implementation in the lab, step by step, updating the procedures as you progress. You should expect to encounter issues during this process. The goal here is to identify as many issues that block the implementation as possible and to develop solutions or procedures to work around the issues. You should expect to repeat this process many times, getting a bit further each time and resetting the lab to the start state as necessary.

Once you are able to get successfully through the implementation from start state to desired end state, you can be sure that you have a reliable and truly useful implementation plan.

Appendix A

ACS Sizing Example

This appendix is a sample walkthrough of generating a sizing estimate for a hypothetical ACS installation. In this example we assume that the following information has been collected without any event log filters applied:

The number of security events from a Windows Server domain controller (one of twenty domain controllers in the environment) was sampled using the Events Generated Per Second script over a 2 day period. The server generated an average of 900,000 events in a given 24 hour period. Peak event generation occurred between 7:30 A.M. and 10:00 A.M. (150 minutes) when 360,000 events were recorded. [20]\*[360,000] / [150 min] / [60 sec] = 800 events per second for all servers.

The number of disks needed to support the logs was determined by using the disk RPM (assuming 15,000 RPM), logical disk I/O, and the number of events that occurred per second values and placing them in the following equation:

1.384\*800\*60/15000=~5 drives \*2 (for RAID 1)=10 drives

The number of disks needed to support the databases was determined by using the disk RPM (assuming 15,000 RPM), logical disk I/O, and the number of events that occurred per second values and placing them in the following equation:

0.138\*800\*60/15000=~1 drive \*2 (for RAID 1)=2 drives

The maximum number of disk drives that the disk array controller can support is 8 drives per array. Therefore, you will need two collectors and two audit databases. The 20 Windows Server domain controllers will be divided evenly among the two collectors.

The amount of storage to allocate for each database is estimated by taking the size of an average event collected (0.4 KB), the number of events collected per second, and the duration to store data values and placing them in the following equation:

900,000\*20\*0.4KB=6.87GB of data collected per day

Assuming you want to store data for 14 days, you need 96 GB of total storage space, which is 48 GB per audit database.

Events Generated Per Second Script The Microsoft Visual Basic script shown in this section counts and displays the number of security events generated every second in the local security log for a computer. For best results, you should run this script locally on the computer where you are recording security events. However, you can run the script on a remote computer when you use the target computer name as an argument. You can generate script results by directing the results to a .csv file. To stop the script, press CTRL+C. Afterward, you can open the .csv file in Microsoft Excel to perform calculations on the results.

Usage

CScript /nologo SecurityEventPerSecond.vbs >>NumOfEvtsGenPerSec.csv

Or

CScript /nologo SecurityEventPerSecond.vbs <RemoteComputerName> >>NumOfEvtsGenPerSec.csv

Sample

' \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

' Copyright (c)2007-2008, Microsoft Corporation, All Rights Reserved

'

' SecurityEventPerSecond.vbs

'

' Written by: Joseph Chan (Microsoft Operations Manager Program Manager)

'

' This is a sample script that counts and displays the

' number of security events generated every second in the local

' security event log

'

' This script takes one parameter "Computer". You can specify a

' remote computer. If no computer name is specified then it will

' count events on the local computer.

'

' This script does not stop until you stop it manually (Ctrl+C)

' You should always run this script by using CScript.exe

' If you use WScript, you will need to

' use Task Manager to stop the WScript process

'

' \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

On Error Resume Next

Set objArgs = WScript.Arguments

If objArgs.Count >= 1 Then

computer = objArgs(0)

Else

computer = "."

End If

Dim currentTime

currentTime = DateAdd("s", 0, Now) 'time = 0 seconds from now

Do While True

WScript.Sleep(1000)

GetEventCount computer, currentTime

currentTime = DateAdd("s", 1, currentTime) 'time = 0 seconds from now

Loop

Sub GetEventCount (strComputer, currentTime)

On Error Resume Next

Err.Clear

Dim objWMI, objItem, colLoggedEvents, nextSec, dateTimeCriteria, timeGeneratedField

count = 0

Set dateTimeCriteria = CreateObject("WbemScripting.SWbemDateTime")

dateTimeCriteria.SetVarDate(currentTime)

strCurrent = "'" & dateTimeCriteria.Value & "'"

Set nextSec = CreateObject("WbemScripting.SWbemDateTime")

nextSec.SetVarDate(DateAdd("s", 1, currentTime))

strNext = "'" & nextSec.Value & "'"

Set timeGeneratedField = CreateObject("WbemScripting.SWbemDateTime")

Set objWMI = GetObject("winmgmts:" \_

& "{impersonationLevel=impersonate,(Security)}!\\" \_

& strComputer & "\root\cimv2")

If Err.Number > 0 then

WScript.Echo " Error: [" & Err.Number & "] " & Err.Description

Exit Sub

End If

Set colLoggedEvents = objWMI.ExecQuery \_

("Select \* from Win32\_NTLogEvent Where Logfile ='Security' AND TimeGenerated >= " & strCurrent & " AND TimeGenerated < " & strNext)

If Err.Number > 0 then

WScript.Echo " Error: [" & Err.Number & "] " & Err.Description

Exit Sub

End If

For Each objItem in colLoggedEvents

'timeGeneratedField.Value = objItem.TimeGenerated

'WScript.Echo " " & timeGeneratedField.GetVarDate & ", " & objItem.EventCode & ", " & objItem.SourceName & ", " & objItem.User

count = count +1

Next

If Err.Number > 0 then

WScript.Echo " Error: [" & Err.Number & "] " & Err.Description

Exit Sub

End If

WScript.Echo currentTime & ", " & count

End Sub