

Operations Manager 2007 R2 Operations Administrator’s Guide

Microsoft Corporation

Published: September 2009

Author

Chris Fox, John Downing, Anat Kerry, Liza Poggemeyer, Scott Butler

Feedback

Send suggestions and comments about this document to [momdocs@microsoft.com](mailto:momdocs@microsoft.com?subject=Administrators%20Guide). Please include the guide name and published date with your feedback.

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 release of this guide contains the following updates and additions:   * The title of the guide was changed from “Operations Guide” to “Administrator’s Guide” to reflect the focus of the content. * Configuration information, including configuring notifications, was moved to the Deployment and Configuration Guide. * Information for deploying agents to UNIX-based and Linux-based systems was added. * New and updated procedures for backup and restore were added to reflect updated supported software configurations. |
| September 2009 | Added detailed examples for using the MOMAgent.msi command to deploy agents. |

Contents

[Operations Manager 2007 R2 Operations Administrator's Guide 7](#_Toc240345572)

[Introduction to the Operations Manager Operations Administrator's Guide 7](#_Toc240345573)

[Understanding the Operations console 7](#_Toc240345574)

[Navigate the Operations console 9](#_Toc240345575)

[View data in the Operations console 10](#_Toc240345576)

[Start Monitoring 13](#_Toc240345577)

[Deploying Agents in Operations Manager 2007 13](#_Toc240345578)

[Deploying Windows Agents 14](#_Toc240345579)

[Use the Discovery Wizard to Deploy Agents 15](#_Toc240345580)

[Use the Agent Setup Wizard 18](#_Toc240345581)

[Use the Command Line to Deploy Agents 20](#_Toc240345582)

[MOMAgent.msi command examples 22](#_Toc240345583)

[Use Active Directory to Assign Computers 24](#_Toc240345584)

[Process Manual Agent Installations in Operations Manager 2007 27](#_Toc240345585)

[Deploying UNIX or Linux Agents 30](#_Toc240345586)

[Configuring a Cross Platform Run As Account 31](#_Toc240345587)

[Importing Cross Platform Management Packs 33](#_Toc240345588)

[Using the Discovery Wizard to Discover Systems and Deploy Cross Platform Agents 34](#_Toc240345589)

[Manually Installing Cross Platform Agents 35](#_Toc240345590)

[Discovering Systems after Manual Deployment 36](#_Toc240345591)

[Viewing System Monitors 37](#_Toc240345592)

[Uninstalling Cross Platform Management Packs and Agents 37](#_Toc240345593)

[Working with Agents 39](#_Toc240345594)

[Understanding Agent States 40](#_Toc240345595)

[Heartbeat and Heartbeat Failure Settings in Operations Manager 2007 40](#_Toc240345596)

[Configure an Agent to Report to Multiple Management Groups 45](#_Toc240345597)

[Use Agentless Monitoring 45](#_Toc240345598)

[Investigating and Resolving Alerts 48](#_Toc240345599)

[Investigate Alerts 49](#_Toc240345600)

[Investigate Alert Storms 51](#_Toc240345601)

[Resolve a Heartbeat Alert 52](#_Toc240345602)

[Configuring the Customer Experience Improvement Program (CEIP) in Operations Manager 2007 53](#_Toc240345603)

[Configuring Operational Data Reports in Operations Manager 2007 54](#_Toc240345604)

[Configure Client Monitoring in Operations Manager 2007 55](#_Toc240345605)

[Configuring Error Reporting in Operations Manager 2007 59](#_Toc240345606)

[Maintenance and Best Practices for Operations Manager 61](#_Toc240345607)

[Managing Gateway Servers in Operations Manager 2007 62](#_Toc240345608)

[Managing Reporting in Operations Manager 2007 69](#_Toc240345609)

[Managing Web Console Servers in Operations Manager 2007 73](#_Toc240345610)

[Managing Connected Management Groups in Operations Manager 2007 75](#_Toc240345611)

[Managing Audit Collection Services in Operations Manager 2007 78](#_Toc240345612)

[Using the Operations Manager Command Shell 87](#_Toc240345613)

[Changing Passwords for Operations Manager Accounts 90](#_Toc240345614)

[Identifying the Root Management Server in Operations Manager 2007 90](#_Toc240345615)

[Scheduling Maintenance and Monitoring 91](#_Toc240345616)

[How to Configure Grooming Settings for the Operations Manager 2007 Database in Operations Manager 2007 93](#_Toc240345617)

[Backing Up and Restoring Operations Manager 2007 Components 93](#_Toc240345618)

[Complete and Incremental Backups in Operations Manager 2007 94](#_Toc240345619)

[Backup File Naming Conventions in Operations Manager 2007 95](#_Toc240345620)

[What to Back Up in Operations Manager 2007 96](#_Toc240345621)

[How to Schedule Backups of Operations Manager Databases 96](#_Toc240345622)

[How to Back Up the Root Management Server Encryption Key 98](#_Toc240345623)

[How to Back Up the IIS 6.0 Metabase 100](#_Toc240345624)

[How to Back Up an IIS 7 Configuration 101](#_Toc240345625)

[How to Back Up Custom Management Packs 101](#_Toc240345626)

[Recommended Backup Schedule in Operations Manager 2007 102](#_Toc240345627)

[Failure and Restore in Operations Manager 2007 103](#_Toc240345628)

[Impact of Failure in Operations Manager 2007 104](#_Toc240345629)

[Failure Recovery Scenarios for the Root Management Server 108](#_Toc240345630)

[High-Level Restore Guidelines in Operations Manager 2007 109](#_Toc240345631)

[How to Restore Operations Manager 2007 Databases 113](#_Toc240345632)

[How to Restore the IIS 6.0 Metabase Backup in Operations Manager 2007 114](#_Toc240345633)

[How to Restore an IIS 7 Configuration 114](#_Toc240345634)

[How to Restore the Root Management Server Encryption Key in Operations Manager 2007 115](#_Toc240345635)

[Making Updates to an Operations Manager 2007 Deployment 116](#_Toc240345636)

[How to Move the OperationsManager Database in Operations Manager 2007 116](#_Toc240345637)

[How to Move the OperationsManagerDW Database in Operations Manager 2007 122](#_Toc240345638)

[How to Move the OperationsManagerAC Database in Operations Manager 2007 127](#_Toc240345639)

[How to Promote a Management Server to a Root Management Server Role in Operations Manager 2007 128](#_Toc240345640)

[How to Remove a Management Server From a Computer in Operations Manager 2007 132](#_Toc240345641)

[How to Move the Operations Manager Reporting Server in Operations Manager 2007 135](#_Toc240345642)

[Appendix A - Cross Platform Operating System Package Dependencies 138](#_Toc240345643)

Operations Manager 2007 R2 Operations Administrator's Guide

The Microsoft System Center Operations Manager 2007 R2 Administrator’s Guide is a comprehensive resource that can be used to understand and use your Operations Manager 2007 implementation to your best advantage. It follows the Operations Manager 2007 Deployment and Configuration Guide in order of usage during an Operations Manager implementation project. It teaches the Operations Manager administrator what to do after successfully deploying a management group for the first time.

Introduction to the Operations Manager Operations Administrator's Guide

You can use the Operations Administrator’s guide in one of two ways:

 If you are coming to this guide having just deployed a management group for the first time, you should start at the beginning and read through the guide sequentially.

 If you are already familiar with administering an Operations Manager 2007 management group, just go ahead to the section that you need.

The “Start Monitoring” section tells you how to start monitoring your environment. This section provides information about deploying agents, managing agents, and working with alerts. With these tasks completed, your Operations Manager 2007 implementation will be monitoring your applications and computers and providing you with actionable alerts, performance data, and other information from your environment.

The “Maintenance and Best Practices for Operations Manager” section describes ongoing tasks. This section can be used as a reference by all Operations Manager administrators for understanding general management group administration scenarios; it includes the procedures needed to support those scenarios. The information in this section includes content related to administering management servers, administering management groups, performing basic backup and restore procedures, and administering gateway servers.

Understanding the Operations console

The Operations console is the primary tool used for managing your Operations Manager 2007 deployment. In the Operations console, you view and interact with alerts and monitoring data, manage and edit unsealed management packs, generate and view reports, administer management group settings, and build a workspace that is customized to your needs.

Note

If you are accessing the Operations console by using Terminal Services (or another remote access program) to connect to a computer with the Operations console installed, the performance of the Operations console might suffer, depending on network latency, network bandwidth and the amount of data fetched by the console.

The Operations console is made up of the following parts:

Toolbar

|  |
| --- |
| Provides access to the menus, search, find, and scope features, and actions. Note that the tools you see might differ depending on the level of access you have. |

Navigation pane

|  |
| --- |
| Displays the aspects of your Operations Manager implementation, including all currently discovered objects. You can use the navigation tree to drill into your environment. When you select an item in the tree, details of that item are displayed in the Results pane. |

Navigation buttons

|  |
| --- |
| Enable you to move through the monitoring and administration views in the Operations console. The buttons that you have access to depends on the security role you are signed in as. A member of the Administrator group can access all the buttons; an Operator can access all the buttons except Administration.  There are five areas:   Monitoring   Authoring   Reporting   Administration   My Workspace |

Actions pane

|  |
| --- |
| Displays links to any actions you can take on a selected object (such as viewing the properties of the object), additional resources you can use to get more information (links to online information), and links to the product help. The links displayed in the Actions pane are context-specific and reflect your current scope, view, and selected object. |

Results pane

|  |
| --- |
| Displays the results from navigation using the navigation tree or from a search or find action. The Results pane also shows any textual feedback from actions. |

Details pane

|  |
| --- |
| Displays more detailed information about the selected item in the Results pane. |

Navigate the Operations console

To view the portion of the navigation tree that you want, select the appropriate navigation button, such as Administration or Monitoring. Which navigation buttons are available to you depends on which Operations Manager 2007 components have been installed (such as Reporting) and the role for which you are logged in (Administrators see all navigation buttons; operators see only Monitoring). Each navigation button opens a different view. The navigation tree in the Operations console is context-sensitive based on the view that you are using. For example, when you are working in the Administration view, the navigation tree shows different functions for administration (such as configuring user security), while when in the Monitoring view, the navigation tree displays monitoring functions (such as viewing alerts).

The following sections provide details about each of the views and what you can do in those views.

Monitoring view

In the Monitoring view, you can quickly find the monitoring data you need, such as alerts, performance data, and diagram views. The view displays different aspects of the monitoring data that is collected by Operations Manager 2007. Each item in the Monitoring navigation tree is either a view type or a folder that contains more views.

The views listed under the Monitoring view display aspects of your entire environment, such as current active alerts. The folders listed in the navigation tree are either features of Operations Manager, such as Agentless Exception Monitoring and synthetic transactions, or containers for views defined within a management pack. The feature folders are created when Operations Manager is installed. The folders are named after imported management packs and contain views from those management packs.

You cannot delete the folders or views that are created when Operations Manager is installed or when Management Packs are imported. However, you can personalize the display of these views by using the Personalize View option in the Monitoring pane. Also, you can hide any of the folders by clicking Show or hide views, located just above the navigation buttons, and making your selections by clearing the appropriate check boxes in the Show or hide views window.

The Find, Search, and Scope buttons on the Operations console can make it easier to access the monitoring data within the Monitoring view. For information about using Find, Search, and Scope, see Viewing data in the Operations Console.

Authoring view

In the Authoring view, you can display monitoring settings from currently imported management packs. You can click any node under the Management Pack Objects node to view the monitoring settings that apply to the corresponding node. For example, if you click Rules, the Details pane displays a list of all the rules that are from currently imported management packs. Rules, like all other management pack objects, are listed by the type of object to which the rule applies. Each object type is listed in ascending alphabetical order. Each monitoring object in the Details pane includes information, such as the management pack that contains the setting and if it is currently enabled or disabled. Most settings included in the automatically imported management packs are enabled, by default.

You can also use the Authoring view to create and configure additional monitors, distributed applications, and groups.

See the [Management Pack Authoring Guide](http://go.microsoft.com/fwlink/?LinkID=82637) (http://go.microsoft.com/fwlink/?LinkID=82637) for detailed information about how to create a management pack for a product (which can be an application, a service, or a device).

Reporting view

In the Reporting view, you access the Reporting function in Operations Manager. You can use the Reporting function to create reports based on the data collected by Operations Manager. Reports present data that has been aggregated, is from specific time intervals and from specific sources, and can provide a longitudinal view of information from your monitoring environment. For example, you can create a report that shows the amount of time it takes between an alert being raised to its being written in the Operations Manager database. This report can help you identify any network delays and isolate trouble spots. Based on the data in this report, you can then take corrective action.

The Reporting view is only available if you have installed the Reporting components and have been granted access to them. For information about installing and deploying the Reporting feature, see the Operations Manager Deployment Guide. You can also find additional information about using the Reporting interface in the Report Authoring Guide and the Operations Manager Help.

Administration view

In the Administration view, you can deploy and configure all aspects of the monitoring environment. For example, if you want to set up notifications (messages that are sent when alerts occur), you do that through the Administration view. You also perform most administration aspects of Operations Manager through this view: You can configure and manage management groups and users, set up user security through user roles, and manage connectors (non-Microsoft devices that provide monitoring data to Operations Manager 2007).

My Workspace view

Use the My Workspace view to create and save custom workspaces and searches. This enables you to customize your working environment so that it shows only those items that you are interested in.

View data in the Operations console

Operations Manager 2007, with the appropriate management packs imported will provide you with a comprehensive view of what is going on with your monitored applications, hardware, and processes. This can result in a very large volume of data being displayed in the Operations console. Learning how to quickly locate the data you need is essential to efficient interaction with the console. You can use the Scope, Find, and Search buttons on the Operations console toolbar to filter your view of monitoring data so that you can find the exact monitoring object or group of objects that you need. You can also filter your data based on the number of hours or days you would like to show.

The Scope, Search, Find, and Time tools apply a temporary filter to the data you are viewing in the console. While you can locate a specific object using Search or Find, you can also use Scope or Time to display a set of objects that meet a set of criteria. The following table shows the differences between the different filtering options:

|  |  |
| --- | --- |
| Filter | When to use |
| Scope | Use to limit the data in a view to only those objects that meet your criteria. This scope remains in place until you clear it. |
| Search | Use to display a list of objects that meet your criteria. You can then act on those objects; however, when you navigate away from this list, the filter is removed, and any view will show all objects (not just those from your search criteria). |
| Find | Use to display a known single object. |
| Time | Use to limit the data displayed to only that data (such as alerts) that has been generated within a defined time frame. |

If you need to view the same set of monitoring data, you can personalize a view so that the same filters are always applied to the data when you open that view in the console. You can also save a search for later use.

Changing the scope

Changing the scope of the monitoring view enables you to view only those objects that meet a certain criteria, such as management servers. For example, if you want to view only those computers in your environment that are running Windows XP, you can apply a scope that uses “Windows XP” as the criteria; no other computers are displayed.

Note that the scope used within the Operations console is different from that used for security roles. In a security sense, the term “scope” applies to the realm of responsibility (such as being responsible for all computers in the Northwest running Microsoft Exchange). A security role is made up of the scope plus a profile.

To change the scope

|  |
| --- |
| 1. In the Operations console, click the Monitoring button to display the objects in your monitoring environment.  2. Click the Scope button on the Operations Manager toolbar. If this button is not available, check to make sure that you have an object, not a folder, selected in the Monitoring pane.  3. The Change View Scope dialog box displays a list of existing groups and distributed applications. If the list is too long, you can find a specific group or distributed application by entering a word or phrase in the Look for box. Once you make a selection, click OK.  Now only the objects that meet the scope criteria are shown in the Results pane. |

Using Find and Search

Use the Find button when the list of objects in the Results pane is too long to quickly pick out a particular object. Use the Search button if you want to find all objects that meet a certain criteria.

To use the Find button to locate an object within a list

|  |
| --- |
| 1. In the Operations console, click the Monitoring button.  2. Click to select a view that is available in the Monitoring pane. This displays a list of objects.  3. Check to see if a Look for box is at the top of the Results pane. If there is no Look for box, click the Find button on the Operations Manager toolbar. In Look for, type a word, such as the name of an object, that you want to find in the list, and then click Find.  The object that you are looking for is displayed.  4. Click Clear to go back to the original list of objects. |

To use the Search feature to create a list of objects

|  |
| --- |
| 1. In the Operations console, click the Monitoring button.  2. Click the Search button in the Operations Manager toolbar.  3. In the Search window, type the word or phrase that describes the set of objects you want to find. A list of objects that meet your criteria displays. The list is sorted by object type. |

Changing the time criteria

Changing the time criteria of the monitoring view enables you to view only those objects that meet a certain criteria, such as “Last 12 hours.” When you change the time criteria, you limit what is displayed to only what has happened in that time period. For example, if you want to view the last week of data, you can change the time criteria to Last 1 week.

To change the time criteria

|  |
| --- |
| 1. In the Operations console, click the Monitoring button to display the objects in your monitoring environment.  2. Click the Calendar button on the Operations Manager toolbar. If this button is not available, check to make sure that you have an object, not a folder, selected in the Monitoring pane.  3. Select the proper time criteria you are interested in. |

Now only the objects that meet the time criteria are shown in the Results pane.

Start Monitoring

This section describes the process for deploying agents, working with management packs, and working with alerts. After these tasks are complete, your management group automatically deploys the correct management packs to the correct computers and monitoring will begin.

Also, this section describes the configuration of the Customer Experience Improvement Program (CEIP), client monitoring options, and error reporting.

Deploying Agents in Operations Manager 2007

To begin monitoring your environment, you need to decide what applications and devices you want to monitor. Then you can identify the computers that support those applications.

Monitoring Windows-Based Systems

Microsoft System Center Operations Manager 2007 provides two methods for monitoring Windows-based computers: agent-managed monitoring or agentless-managed monitoring.

 Agent-Managed Monitoring

Agent-managed computers have an Operations Manager service installed. This service, which appears as HealthService in the Services list in Computer Management is the Operations Manager agent. Monitoring computers via agents allows access to all Operations Manager options and functionality; therefore, the vast majority of monitoring is performed this way. Agents also play a role in agentless management.

 Agentless-Managed Monitoring

Windows-based computers where an agent cannot be installed can be monitored agentlessly. You can manage an agentless-managed computer by setting up communications between a management group, a proxy agent, and the agentless-managed computer. You can also monitor network devices and systems that are not running Windows through the use of agentless monitoring.

For more information about deploying and using Operations Manager agents on Windows-based systems, see [Deploying Windows Agents](#zedf0ac74d84b40f2b0126eb063d7fea2).

Monitoring UNIX-based or Linux-based Systems

System Center Operations Manager 2007 enables IT professionals to monitor system health and events on computers running UNIX and Linux operating systems, including the following:

 File systems and network interfaces

 Critical system processes (for example, syslog, cron, and others)

 Key configurations (for example, resolution of host name, or the correct configuration of Web Services Management components)

 Core system attributes (for example, the health of system memory and processors)

 Physical and logical disk space, swap space, and system memory

 Performance degradation caused by applications or processes

System Center Operations Manager 2007 supports monitoring for the following UNIX and Linux operating systems:

 AIX 5.3 (Power), 6.1 (Power)

 HP-UX 11iv2 (PA-RISC & IA64), and 11iv3 (PA-RISC, and IA64)

 Red Hat Enterprise Server 4 (x86 and x64) and 5 (x86 and x64)

 Solaris 8 (SPARC), 9 (SPARC), and 10 (SPARC & x86 versions later than 120012-14)

 SUSE Linux Enterprise Server 9 (x86) and 10 SP1 (x86 and x64)

For more information about deploying and using Operations Manager Agents on UNIX-based or Linux-based systems, see [Deploying UNIX or Linux Agents](#z161277a1b7904f29bca5baaebc1cfb07).

Administering Agents

After you have installed and configured agents on computers you want to monitor, Operations Manager 2007 has several tools and procedures available for you to use to administer the agents that you have deployed.

For more information about administering agents, see [Working with Agents](#zd95565a622ef410291089f6f2cc1d8e0).

Deploying Windows Agents

The first step in monitoring your environment is to deploy agents. Your network architecture will greatly influence which monitoring options you use and how you plan the deployment of your agents. Be aware of whether you are managing systems on the other side of a firewall from your management group, or are managing systems that don’t participate in a Kerberos trust with the management group.

Note

If you add or delete a new virtual server on a cluster after a Microsoft System Center Operations Manager 2007 agent is installed, the agent will not recognize the changes and new virtual servers will not be reported. For the agent to recognize the virtual server, you must restart the System Center Management service on the node where the virtual server is active.

You can use any of the following methods to deploy agents:

 The Discovery Wizard (through the Operations console)

 The Agent Setup Wizard

 The MOMAgent.msi program, from the command line

 Active Directory, to assign agents to a management group

The following sections provide detailed steps for each of these methods.

The following tasks are described in this topic:

|  |  |
| --- | --- |
| Task | Where to find information |
| Discover systems | [Use the Discovery Wizard to Deploy Agents](#z3187910250d8421eb48ffb067ee32f02) |
| Deploy agents using the Setup wizard | [Use the Agent Setup Wizard](#zc36665ef9ab3407bb0a3fa79eb7de835) |
| Deploy agents from the command | [Use the Command Line to Deploy Agents](#z7108fb6850c34fca919b922703f128d3) |
| Assign agents using Active Directory | [Use Active Directory to Assign Computers](#zd6a76739a332439885c31f8f3581665d) |
| Manage newly installed agents | [Process Manual Agent Installations in Operations Manager 2007](#z5bcdc135a84a4e6a99872242f32c877b) |

Use the Discovery Wizard to Deploy Agents

You can use the Operations console to search your environment for manageable objects and then deploy an agent to any object that you want to monitor. The process of searching your environment is called “discovery.” One of the advantages of using discovery is that it lists all manageable objects, including any that you might not be aware of.

The Discovery Wizard does not show systems that the management group is already monitoring. If you are doing a phased rollout of your management group, you can run the wizard to add new systems to the group. Also, after your initial deployment, you can use the Discovery Wizard to add newly installed computers to be managed.

When agents are pushed out to computers, Microsoft System Center Operations Manager 2007 sends credentials that have local administrator rights for that computer; this is required to install the agent. Sending credentials could raise security concerns. Consult the [Operations Manager 2007 Security Guide](http://go.microsoft.com/fwlink/?LinkId=64017) (http://go.microsoft.com/fwlink/?LinkId=64017) for information to help you address any security issues before you use the Discovery Wizard.

If the Discovery Wizard is not right for your needs (for example, if you have a set list of computers to which you want to deploy agents), you have the option of manually installing agents on systems to be managed. Agents can also be embedded in the host image of the monitored computer.

Use the following procedure to discover Windows-based computers and to deploy the Operations Manager 2007 agent to them from the Operations console.

To deploy the Operations Manager 2007 agent to Windows-based computers from the Operations console

|  |
| --- |
| 1. Log in to the Operations console with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 management group.  2. Click the Administration button.  3. At the bottom of the navigation pane, click Discovery Wizard.  4. On the Introduction page, click Next. The Introduction page does not appear if the Computer and Device Management Wizard has been run before and Do not show this page again was selected.  5. On the Auto or Advanced? page, do the following:  a. Select either Automatic computer discovery or Advanced discovery. If you select Automatic computer discovery, click Next, and then go to step 7. If you select Advanced discovery, continue with the following steps.  Note  Automatic computer discovery scans for Windows-based computers in the domain that the root management server is in. Advanced discovery allows you to specify criteria for the computers that the wizard will return, such as computer names starting with NY.  b. In the Computer & Device Types list, select Servers & Clients, Server Only, or Clients Only.  c. In the Management Server list, click the management server or gateway server to discover the computers. When multiple management servers are in a management group, the agents are automatically configured to use secondary management servers if their root management server is unavailable.  d. If you selected Servers & Clients, you can select the Verify discovered computers can be contacted check box. This is likely to increase the success rate of agent deployment, but discovery can take longer.  Note  If the Active Directory catalog does not contain the NetBIOS names for computers in a domain, select Verify discovered computers can be contacted. Otherwise, the Browse, or Type In option will fail to find computers. This affects computers in the same domain as the root management server, in another domain with a full trust relationship, and in untrusted domains using a gateway server.  e. Click Next.  Note  The wizard can return approximately 4000 computers if Verify discovered computers can be contacted is selected, and it can return 10,000 computers if this option is not selected. Automatic computer discovery verifies that discovered computers can be contacted. A computer that is already managed by the management group is not returned.  6. On the Discovery Method page, you can locate the computers that you want to manage by either scanning or browsing Active Directory Domain Services or typing the computer names.  If you want to scan, do the following:  a. If it is not already selected, select Scan Active Directory and then click Configure.  b. In the Find Computers dialog box, type the criteria that you want to use for discovering computers and then click OK.  c. In the Domain list, click the domain of the computers that you want to discover.  If you want to browse Active Directory or type the computer names, do the following:   Select Browse for, or type-in computer names, click Browse, specify the names of the computers that you want to manage, and then click OK.   In the Browse for, or type-in computer names box, type the computer names, separated by a semi-colon, comma, or a new line [ENTER]. You can use NetBIOS computer names or fully qualified domain names (FQDN).  7. Click Next, and on the Administrator Account page, do one of the following:   Select Use selected Management Server Action Account if it is not already selected.   Select Other user account, type the User name and Password, and then select the Domain from the list. If the user name is not a domain account, select This is a local computer account, not a domain account.  Important  The account must have administrative privileges on the targeted computers. If This is a local computer account, not a domain account is selected, the Management Server Action Account will be used to perform discovery. For more information about Operations Manager 2007 accounts, see the [Operations Manager 2007 Security Guide](http://go.microsoft.com/fwlink/?LinkId=64017) (http://go.microsoft.com/fwlink/?LinkId=64017).  8. Click Discover to display the Discovery Progress page. The time it takes discovery to finish depends on many factors, such as the criteria specified and the configuration of the IT environment.  Note  Computers that are already managed by the management group will not be returned by the wizard.  9. On the Select Objects to Manage page, do the following:  a. Select the computers that you want to be agent-managed computers.  b. In the Management Mode list, click Agent and then click Next.  Note  Computer Discovery shows virtual nodes of clusters. Do not select any virtual nodes to be managed.  10. On the Summary page, do the following:  a. Leave the Agent installation directory set to the default of %ProgramFiles%\System Center Operations Manager 2007 or type an installation path.  Important  If a different Agent installation directory is specified, the root of the path must exist on the targeted computer or the agent installation fails. Subdirectories, such as OM2007\Agent, are created if they do not exist.  b. Leave Agent Action Account set to the default, Local System, or select Other and type the User name, Password, and Domain. The Agent Action Account is the default account that the agent will use to perform actions. For more information about Operations Manager 2007 accounts, see the [Operations Manager 2007 Security Guide](http://go.microsoft.com/fwlink/?LinkId=64017) (http://go.microsoft.com/fwlink/?LinkId=64017).  c. Click Finish.  11. In the Agent Management Task Status dialog box, the Status for each selected computer changes from Queued to Success; the computers are ready to be managed.  Note  If the task fails for a computer, click the targeted computer. The reason for the failure is displayed in the Task Output text box.  12. Click Close. |

Use the Agent Setup Wizard

Use the following procedure to deploy the Microsoft System Center Operations Manager 2007 agent with the MOMAgent.msi setup wizard.

Before you use the setup wizard, ensure the following conditions are met:

 Each agent that is installed with the wizard must be approved by a management group. For more information, see [Process Manual Agent Installations in Operations Manager 2007](#z5bcdc135a84a4e6a99872242f32c877b).

 If an agent is manually deployed to a domain controller and an Active Directory management pack is later deployed, errors might occur during deployment of the management pack. To prevent errors from occurring before deploying the Active Directory management pack, or to recover from errors that might have already occurred, you need to deploy the Active Directory management pack helper object by deploying the file Oomads.msi on the affected domain controller. The file Oomads.msi is on the computer that is hosting the agent at C:\Program Files\System Center Operations Manager 2007\HelperObjects. For more information, see the section "Agent-Managed Domain Controllers" in the topic [Process Manual Agent Installations in Operations Manager 2007](#z5bcdc135a84a4e6a99872242f32c877b)

To deploy the Operations Manager 2007 agent with the Agent Setup Wizard

|  |
| --- |
| 1. Use local administrator privileges to log on to the computer where you want to install the agent.  2. On the Operations Manager 2007 installation media, double-click the SetupOM.exe file.  3. On the Start page, select Install Operations Manager 2007 Agent.  4. On the Welcome page, click Next.  5. On the Destination Folder page, leave the installation folder set to the default, or click Change and type a path, and then click Next.  6. On the Management Group Configuration page, do one of the following:   Leave the Specify Management Group information check box selected, and then click Next.   Clear the Specify Management Group information check box if management group information has been published to Active Directory Domain Services, and then click Next.  Note  Step 7 is bypassed by the Agent Setup Wizard if the Specify Management Group information check box is cleared.  7. On the Management Group Configuration page, do the following:  a. Type the name of the management group in the Management Group Name field and the server name in the Management Server field.  Note  To use a gateway server, enter the gateway server name in the Management Server text box. For more information about gateway servers, see the [Operations Manager 2007 Security Guide](http://go.microsoft.com/fwlink/?LinkId=64017) (http://go.microsoft.com/fwlink/?LinkId=64017).  b. Type in a value for Management Server Port, or leave the default 5273.  c. Click Next.  8. When the Agent Action Account page appears, leave it set to the default of Local System, or select Domain or Local Computer Account; type the User Account, Password, and Domain or local computer; and then click Next.  Note  For information about Operations Manager 2007 accounts, see the [Operations Manager 2007 Security Guide](http://go.microsoft.com/fwlink/?LinkId=64017) (http://go.microsoft.com/fwlink/?LinkId=64017).  9. On the Ready to Install page, review the settings and then click Install to display the Installing System Center Operations Manager Agent page.  10. When the Completing the System Center Operations Manager Agent Setup Wizard page appears, click Finish. |

Use the Command Line to Deploy Agents

You can use the MOMAgent.msi executable to deploy agents from the command line. Deploying agents from the command line is also referred to as a manual install.

Before you begin deployment, ensure the following conditions have been met:

 The account that is used to run MOMAgent.msi must have administrative privileges on the targeted computers.

 A management group (or single management server) must be configured to accept agents installed with MOMAgent.msi or they will be automatically rejected and therefore not display in the Operations console. For more information, see [Process Manual Agent Installations in Operations Manager 2007](#z5bcdc135a84a4e6a99872242f32c877b). If the management group or server is configured to accept manually installed agents after the agents have been manually installed, the agents will display in the console after approximately one hour.

 If an agent is manually deployed to a domain controller and an Active Directory management pack is later deployed, errors might occur during deployment of the management pack. To prevent errors from occurring before deploying the Active Directory management pack or to recover from errors that might have already occurred, you need to deploy the Active Directory management pack helper object by deploying the file Oomads.msi on the affected domain controller. The file Oomads.msi is on the computer that is hosting the agent at C:\Program Files\System Center Operations Manager 2007\HelperObjects. For more information, see the section "Agent-Managed Domain Controllers" in the topic [Process Manual Agent Installations in Operations Manager 2007](#z5bcdc135a84a4e6a99872242f32c877b)

 Each agent that is installed with MOMAgent.msi must be approved for a management group. For more information, see [Process Manual Agent Installations in Operations Manager 2007](#z5bcdc135a84a4e6a99872242f32c877b).

MOMAgent.msi can be found in the Microsoft System Center Operations Manager 2007 installation media and the management server installation directory.

Use the following procedure to deploy an agent. For examples of ways in which you can customize the MOMAgent.msi command, see [MOMAgent.msi command examples](#z0f5eb03f5b944e109fde594bc50c02cf).

To deploy the Operations Manager 2007 agent from the command line

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Log on to the computer where you want to install the agent by using an account with local administrator privileges.  2. Open a command window.  3. Run the following command:  %WinDir%\System32\msiexec.exe /i \\path\Directory\MOMAgent.msi /qn USE\_SETTINGS\_FROM\_AD={0|1} MANAGEMENT\_GROUP=MGname MANAGEMENT\_SERVER\_DNS=MSname SECURE\_PORT=PortNumber ACTIONS\_USE\_COMPUTER\_ACCOUNT={0|1} ACTIONSUSER=UserName ACTIONSDOMAIN=DomainName ACTIONSPASSWORD=Password  where:   |  |  | | --- | --- | | USE\_SETTINGS\_FROM\_AD=[0|1] | Indicates whether the management group settings properties will be set on the command line. Use 0 if you want to set the properties at the command line. Otherwise, if you use 1, the management group settings are taken from Active Directory. | | MANAGEMENT\_GROUP=MGname | Specifies the management group that will manage the computer. | | MANAGEMENT\_SERVER\_DNS=MSname | Specifies the fully qualified domain name for the management server . To use a gateway server, enter the gateway server FQDN as MANAGEMENT\_SERVER\_DNS .  Important  If the computer's DNS and Active Directory names differ, the MANAGEMENT\_SERVER\_AD\_NAME property also needs to be set to the fully qualified Active Directory Domain Services name. | | SECURE\_PORT=PortNumber | Sets the health service port number. | | ACTIONS\_USE\_COMPUTER\_ACCOUNT={0|1} | Indicates whether to use a specified user account (0) or the Local System account (1). | | ACTIONSUSER=UserName | Sets the Agent Action account to UserName . This parameter is required if you specified ACTIONS\_USE\_COMPUTER\_ACCOUNT=0. | | ACTIONSDOMAIN= DomainName | Sets the domain for the Agent Action account identified with the ACTIONSUSER parameter. . | | ACTIONSPASSWORD= Password | The password for the user identified with the ACTIONSUSER parameter. | |

MOMAgent.msi command examples

The following examples show different ways in which you can use the MOMAgent command. You can use this command to perform new installations of agents, upgrade agents from previous releases of Operations Manager 2007, or change the configuration of an agent (such as the management group or management server associated with the agent).

Agent installation using a specific Action Account

The following example shows a fresh installation of an agent and uses a specific Action Account.

msiexec.exe /i \\path\Directory\MOMAgent.msi /qn /l\*v %temp% MOMAgentinstall.log USE\_SETTINGS\_FROM\_AD=0 MANAGEMENT\_GROUP=<MG\_Name> MANAGEMENT\_SERVER\_DNS=<MSDNSName> ACTIONS\_USE\_COMPUTER\_ACCOUNT=0 ACTIONSUSER=<AccountUser> ACTIONSDOMAIN=<AccountDomain> ACTIONSPASSWORD=<AccountPassword> USE\_MANUALLY\_SPECIFIED\_SETTINGS=1 SET\_ACTIONS\_ACCOUNT=1

Agent installation using the Local System account

The following example shows a fresh installation of an agent and uses the Local System for the Action Account.

msiexec.exe /i \\path\Directory\MOMAgent.msi /qn /l\*v %temp%\MOMAgentinstall.log USE\_SETTINGS\_FROM\_AD=0 MANAGEMENT\_GROUP=<MG\_Name> MANAGEMENT\_SERVER\_DNS=<MSDNSName> ACTIONS\_USE\_COMPUTER\_ACCOUNT=1 USE\_MANUALLY\_SPECIFIED\_SETTINGS=1 SET\_ACTIONS\_ACCOUNT=1

Agent installation with Active Directory integration and using a specific Action Account

The following example installs an agent by using Active Directory and a specific Action Account.

msiexec /i \\path\Directory\MOMAgent.msi  /qn /l\*v %temp%mominst.NoGroupSpecified.log USE\_SETTINGS\_FROM\_AD=1 USE\_MANUALLY\_SPECIFIED\_SETTINGS=0 ACTIONS\_USE\_COMPUTER\_ACCOUNT=0 ACTIONSUSER=<AccountUser> ACTIONSDOMAIN=<AccountDomain> ACTIONSPASSWORD=<AccountPassword>  SET\_ACTIONS\_ACCOUNT=1

Agent installation with Active Directory integration and using the Local System account

The following example installs an agent by using Active Directory and the Local system account for the Action Account.

msiexec /i \\path\Directory\MOMAgent.msi  /qn /l\*v %temp%\ mominst.NoGroupSpecified.log USE\_SETTINGS\_FROM\_AD=1 ACTIONS\_USE\_COMPUTER\_ACCOUNT=1 USE\_MANUALLY\_SPECIFIED\_SETTINGS=0 SET\_ACTIONS\_ACCOUNT=1

Agent upgrade from a previous release of Operations Manager 2007 SP1

The following example upgrades an agent.

msiexec /i \\path\Directory\MOMAgent.msi SET\_ACTIONS\_ACCOUNT=0 /qn /l\*v %temp%\MOMAgentUpgrade.log

Change the name of the management server associated with the agent

The following example changes the name of the management server.

MsiExec.exe /i \\path\Directory\MOMAgent.msi /norestart /qn /l\*v %temp%\MOMAgentReinstall.log MANAGEMENT\_GROUP= <SameManagementGroup>  MANAGEMENT\_GROUP\_OPERATION=ModifyConfigGroup MANAGEMENT\_SERVER\_DNS=<NewManagementServerName>  REINSTALL=ALL

Add a new management group

The following example adds a new management group to an agent. This is also referred to as “multi-homing.”

MsiExec.exe /i \\path\Directory\MOMAgent.msi /norestart /qn /l\*v %temp%\MOMAgentAdd.log MANAGEMENT\_GROUP=<NewManagementGroup> MANAGEMENT\_GROUP\_OPERATION=AddConfigGroup MANAGEMENT\_SERVER\_DNS=<NewManagementServerName> REINSTALL=ALL

Note:

Note

If the agent was installed as Active Directory-enabled, then the configuration is set by Active Directory.

Remove a management group

The following example removes a management group from the agent.

MsiExec.exe /i \\path\Directory\MOMAgent.msi  /norestart /qn /l\*v %temp%\MOMRemove.log MANAGEMENT\_GROUP=<OldManagementGroup> MANAGEMENT\_GROUP\_OPERATION=RemoveConfigGroup MANAGEMENT\_SERVER\_DNS=<OldManagementServerName> REINSTALL=ALL

Note

If this is the last management group assigned to this agent, the agent will also be uninstalled.

If the agent was installed as Active Directory-enabled, then the configuration is set by Active Directory.

Remove an old management group or management server and redirect to a new management group or management server

The following example removes an existing management group or server and adds a new management group or server to the agent.

First, add the new management group or management server:

MsiExec.exe /i \\path\Directory\MOMAgent.msi /norestart /qn /l\*v %temp%\MOMAgentAdd.log MANAGEMENT\_GROUP=<NewManagementGroup> MANAGEMENT\_GROUP\_OPERATION=AddConfigGroup MANAGEMENT\_SERVER\_DNS=<NewManagementServerName> REINSTALL=ALL

Next, remove the old management group or management server:

MsiExec.exe /i \\path\Directory\MOMAgent.msi  /norestart /qn /l\*v %temp%\MOMRemove.log MANAGEMENT\_GROUP=<OldManagementGroup> MANAGEMENT\_GROUP\_OPERATION=RemoveConfigGroup MANAGEMENT\_SERVER\_DNS=<OldManagementServerName> REINSTALL=ALL

Note

Make sure to add the new management group first before removing the old one.  If you remove the old management group first and it’s the last management group assigned to the agent, the agent will be uninstalled.

If the agent was installed as Active Directory-enabled, then the configuration is set by Active Directory.

Use Active Directory to Assign Computers

You can use Active Directory Domain Services to assign agent-managed computers to management groups. To assign computers to management groups by using Active Directory Domain Services:

 The functional level of Active Directory Domain Services domains must be Windows 2000 native, Windows Server 2003, or Windows Server 2008.

 Agent-managed computers and the root management server must be in the same domain or in two-way trusted domains.

Note

Regardless of whether Active Directory Domain Services is used to assign computers to a management group, agent-managed computers and their root management server and secondary management server must be in the same domain or in two-way trusted domains, or a gateway server must be used. For more information about gateway servers, see the [Operations Manager 2007 Security Guide](http://go.microsoft.com/fwlink/?LinkId=64017) (http://go.microsoft.com/fwlink/?LinkId=64017).

Configuring agents to get their management group information from Active Directory Domain Services is also helpful if your organization uses images to deploy computers. For example, add the Operations Manager 2007 agent to the Microsoft SQL Server image and configure the agent to get its management group information from Active Directory. When you initialize a new server running SQL Server from an image, the server is automatically configured to be managed by the appropriate Microsoft System Center Operations Manager 2007 management group and to download the applicable management packs.

When Active Directory Domain Services assigns computers to Operations Manager 2007 management groups, the following phrases are used:

1. A domain administrator uses MOMADAdmin.exe to create an Active Directory Domain Services container for an Operations Manager 2007 management group in the domains of the computers it will manage. The Active Directory Domain Services security group that is specified when you are running MOMADAdmin.exe is granted read and delete child permissions to the container. By creating a container this way, Operations Manager administrators are given the necessary permission to add management servers to the container and assign computers to them, without needing to be domain administrators.

2. An Operations Manager administrator assigns computers to the root management server and secondary management server. For more information, see [How to Use Active Directory to Assign Computers to Operations Manager 2007 Management Servers](#z1) in the next section.

3. The Operations Manager 2007 agent is deployed to the computers that you want, and it is configured to get its management group information from Active Directory by using MOMAgent.msi. See [Use the Command Line to Deploy Agents](#z7108fb6850c34fca919b922703f128d3) for information.

Note

Active Directory Integration is disabled for agents that were installed from the Operations console. By default, Active Directory Integration is enabled for agents installed manually by using MOMAgent.msi. To disable Active Directory Integration for manual installations, use the command-line parameter USE\_SETTINGS\_FROM\_AD=0 as it is explained in [Use the Command Line to Deploy Agents](#z7108fb6850c34fca919b922703f128d3).

How to Use Active Directory to Assign Computers to Operations Manager 2007 Management Servers

The Operations Manager 2007 Agent Assignment and Failover Wizard creates an agent assignment rule that uses Active Directory Domain Services to assign computers to a management group and assign the computers' primary management server and secondary management servers. Use the following procedures to start and use the wizard.

Note

The Agent Assignment and Failover Wizard does not deploy the agent. You must deploy the agent to the computers by using MOMAgent.msi.

Changing the agent assignment rule can result in computers no longer being assigned to, and therefore monitored by, the management group. The state of these computers will change to critical, because the computers no longer send heartbeats to the management group. These computers can be deleted from the management group and, if the computer is not assigned to other management groups, the Operations Manager 2007 agent can be uninstalled.

To start the Operations Manager 2007 Agent Assignment and Failover Wizard

|  |
| --- |
| 1. Log on to the Operations console with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 management group.  2. Click the Administration button.  3. In the Administration pane, expand Administration, expand Device Management, and then click Management Servers.  4. In the Management Servers pane, right-click the management server or gateway server to be Primary Management Server for the computers that are returned by the rules you will create in the following procedure, and then click Properties.  5. In the Management Server Properties dialog box, click the Agent Management tab, and then click Add to start the Agent Assignment and Failover Wizard. |

To use the Operations Manager 2007 Agent Assignment and Failover Wizard to assign computers to a management group

|  |
| --- |
| 1. In the Agent Assignment and Failover Wizard, on the Introduction page, click Next.  Note  The Introduction page does not appear if the wizard has been run and Do not show this page again was selected.  2. On the Domain page, do the following:  Note  To assign computers from multiple domains to a management group, run the Agent Assignment and Failover Wizard for each domain.   Select the domain of the computers from the Domain name drop-down list. The management server must be able to resolve the domain name.  Important  The management server and the computers that you want to manage must be in two-way trusted domains.   Set Select Run As Profile to the Run As profile associated with the Run As account that was provided when MOMADAdmin.exe was run for the domain. The default account that is used to perform agent assignment is the computer account for the root management server, also referred to as the Active Directory Based Agent Assignment Account. If this was not the account that was used to run MOMADAdmin.exe, select Use a different account to perform agent assignment in the specified domain, and then select or create the account from the Select Run As Profile drop-down list.  Note  For more information about Run As Profiles and Run As Accounts, see the [Operations Manager 2007 Security Guide](http://go.microsoft.com/fwlink/?LinkId=64017).  3. On the Inclusion Criteria page, either type the LDAP query for assigning computers to this management server in the text box and then click Next, or click Configure. If you click Configure, do the following:  a. In the Find Computers dialog box, type the criteria that you want to use for assigning computers to this management server.  b. Click OK, and then click Next.  Note  The following LDAP query returns computers with a name starting with MsgOps, (&(sAMAccountType=805306369)(objectCategory=computer)(cn=MsgOps\*)) For more information about LDAP queries, see [Creating a Query Filter](http://go.microsoft.com/fwlink/?LinkId=73366) available in the Microsoft Developer Network Library (http://go.microsoft.com/fwlink/?LinkId=73366).  4. On the Exclusion Rule page, type the fully qualified domain name (FQDN) of computers that you explicitly want to prevent from being managed by this management server, and then click Next.  Important  You must separate the computer FQDNs that you type with a semicolon, colon, or a new line (CTRL+ENTER).  5. On the Agent Failover page, either select Automatically manage failover and click Create or select Manually configure failover. If you select Manually configure failover, do the following:  a. Clear the check boxes of the management servers to which you do not want the agents to fail over.  b. Click Create.  Note  With the Manually configure failover option, you must run the wizard again if you subsequently add a management server to the management group and want the agents to fail over to the new management server.  6. In the Management Server Properties dialog box, click OK.  Note  It can take up to one hour for the agent assignment setting to propagate in Active Directory Domain Services. |

Process Manual Agent Installations in Operations Manager 2007

Manual installation of an agent refers to the process of running MOMAgent.msi locally on a computer that is to host a Microsoft System Center Operations Manager 2007 agent. When it is installed, the agent attempts to join the specified management group by contacting a specified management server. You can use security settings at both the management group and the management server level to configure how requests from manually installed agents are processed.

The following three options are available to process manually installed agents.

|  |  |
| --- | --- |
| Option | Action |
| Reject new manual agent installations | Designates that all requests from a manually installed agent will be denied by Operations Manager 2007. This is the most secure setting and is selected by default. |
| Review new manual agent installations in pending management view | Designates that all requests from a manually installed agent will be directed to the Pending Management node before being allowed to join the management group. An administrator must first review the request and manually approve the agents' request. |
| Auto-approve new manually installed agents | This option is available only if Review new manual agent installations in pending management view has been selected. This setting causes Operations Manager 2007 to automatically allow any manually installed agent to join the management group. This is the least secure option. |

Important

A management group or management server must be configured to accept agents that are installed with MOMAgent.msi or they will be automatically rejected and therefore not displayed in the Operations console. If a management group is configured to accept manually installed agents, the agents will display in the console approximately one hour after they are installed.

The following procedures show you how to configure security settings for manual agent installations.

How to Configure Security for Manual Agent Installations for the Management Group

Use the following procedure to configure a management group to accept or deny agents that are installed manually.

To configure manual agent installations settings for a management group

|  |
| --- |
| 1. Log on to the Operations console with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 management group.  2. Click the Administration button.  3. In the Administration pane, expand Administration, and then click Settings.  4. In the Settings pane, expand Type: Server, right-click Security, and then click Properties.  5. In the Global Management Server Settings - Security dialog box, on the General tab, do one of the following:   To maintain a higher level of security, select Reject new manual agent installations, and then click OK.   To configure for manual agent installation, click Review new manual agent installations in pending management view, and then click OK. For more information about manual agent installations, see the [How to Approve a Pending Agent Installation](#z2) section later in this topic.   Optionally, select Auto-approve new manually installed agents. |

How to Override Manual Agent Settings on a Management Server

Use the following procedure to override the Management group Manual Agent Installs setting and configure the setting for a specific management server.

To override the manual agent installs setting for a management server

|  |
| --- |
| 1. Log on to the Operations console with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 management group.  2. Click the Administration button.  3. In the Administration pane, expand Administration, expand Device Management, and then click Management Servers.  4. In the results pane, right-click the management server that you want to view the properties of, and then click Properties.  5. In the Management Server Properties dialog box, click the Security tab.  6. On the Security tab, do the following:   To maintain a higher level of security, select Reject new manual agent installations, and then click OK.   To configure for manual agent installation, click Review new manual agent installations in pending management view, and then click OK.   Optionally, select Auto-approve new manually installed agents.  7. Click OK. |

How to Approve a Pending Agent Installation

Use the following procedure to approve an Operations Manager 2007 agent installed for a management group with MOMAgent.msi. This procedure is not needed if the management group has been configured to automatically approve manually installed agents.

Tip

In Microsoft Operations Manager 2005, the Pending Management window displayed both agents that were in the process of being installed and those that were in the process of being uninstalled. In Operations Manager 2007, only those agents that are in the process of being installed are displayed in this window.

To approve a pending agent installation

|  |
| --- |
| 1. In the Operations console, click Administration.  2. Click Administration, expand Administration, expand Device Management, and then click Pending Management.  3. In the Pending Management pane, select computers in Type: Manual Agent Install.  4. Right-click the computers, and then click Approve.  5. In the Manual Agent Install dialog box, click Approve. The computers now appear in the Agent Managed node and are ready to be managed.  Note  Rejected agents remain in Pending Management until the agent is uninstalled for the management group. |

Deploying UNIX or Linux Agents

System Architecture

Microsoft System Center Operations Manager 2007 Cross Platform uses Web Services Management (WS-Man) 1.1, a Web services-based protocol that enables remote computer management over HTTP and HTTPS, including hardware management and policy-based event forwarding. WS-Man enables secure and efficient data transfers by requiring authentication and using HTTPS as the transport, and it is required for all communication between Operations Manager 2007 and UNIX or Linux systems.

Important

You should install WS-Man prior to installing Operations Manager 2007 R2. You receive a warning from Operations Manager 2007 R2 if WS-Man is not installed, but you can proceed, and install WS-Man later.

Upgrading Operations Manager 2007 Cross Platform Extensions to Operations Manager 2007 R2 is not supported in this release. You must uninstall previous versions of Operations Manager 2007 Cross Platform.

Required package dependencies for each operating system are shown in [Appendix A - Cross Platform Operating System Package Dependencies](#za412358fee2e4e4cb2257063b7d45d1f).

Install [WS-Management (WS-Man) 1.1](http://go.microsoft.com/fwlink/?LinkId=103610), available from the Microsoft Download Center (http://go.microsoft.com/fwlink/?LinkId=103610).

Steps for Monitoring Cross Platform Computers

This topic demonstrates how to import management packs, discover non-Windows servers, install the suitable operating system agents on those servers, deploy monitors, and generate reports based on the data collected from the cross platform systems.

|  |  |
| --- | --- |
| Step | Reference |
| [Configuring a Cross Platform Run As Account](#z48a23b42cc4f42afb3cdb5619b7f292c) | Create Run-As accounts and profiles to monitor systems. |
| [Importing Cross Platform Management Packs](#z320a0d9b7dae4fa79fa624bab302567a) | Import the management packs that are used to install monitoring agents on monitored computers. |
| [Using the Discovery Wizard to Discover Systems and Deploy Cross Platform Agents](#z660b5f11b64448fd93891ca96a23fd4f) | Use the Discovery Wizard to allow Operations Manager to detect non-Windows-based computers and to install agents that enable monitoring of these computers. |
| [Manually Installing Cross Platform Agents](#z83754a0008ab4ebaa3372ee8ef1c5de5) | Install the agents manually when the computers are not detected by the Discovery Wizard. |
| [Viewing System Monitors](#zb658f30be7dd47bdb045288c9fd10043) | Create system monitors to view and troubleshoot alerts, state changes, and other significant issues on non-Windows-based computers. |

Configuring a Cross Platform Run As Account

In Microsoft System Center Operations Manager 2007 R2, Run As profiles and Run As accounts are used to provide credentials that have the necessary privileges that the default Action account might not have for running rules, tasks, and monitors. To monitor UNIX and Linux computers, you must configure both the UNIX Action account profile and the UNIX Privileged account profile. You must go through the “To configure run as for cross platform” procedure below once for each profile.

To configure Run As for cross platform

|  |
| --- |
| 1. Open the Operations console with an account that is a member of the Operations Manager 2007 R2 Administrators profile.  2. Select the Administration view.  3. In the navigation pane under Run As Configuration, select Profiles.  4. In the results pane, double-click the UNIX Action Account, or UNIX Privileged Account profile to open the Run As Profile Properties – UNIX Action Account or Run As Profile Properties – UNIX Privileged Account dialog box.  5. Select the Associations tab. Notice that the Selected Targets box is empty. Click Cancel to close the window.  6. In the navigation pane under Run As Configuration, select Accounts.  7. Right-click in the results pane, and then select Create Run As Account from the context menu to start the Create Run As Account wizard.  8. If the Introduction page appears, click Next.  9. On the General page, select Basic Authentication from the Run As Account Type list. Notice that there are other options to choose from. The option you select depends on the type of account and authentication that you need. For information on which account type to select, refer to the management pack guide for the management pack that contains the profile that you are configuring.  10. In the Display Name box, enter a name to identify the UNIX Action Account or UNIX Privileged Account credentials. For this exercise, enter Step by Step Run As UNIX Action Account or Step by Step Run As UNIX Privileged Account, and then click Next.  11. On the Basic Run As Account page, enter appropriate values in the Account Name, Password, and Confirm Password boxes, and then click Create. This creates the Step by Step Run As UNIX Action Account or Step by Step Run As UNIX Privileged Account object and maps it to the actual UNIX account credentials that will be used for non-privileged or privileged interaction with the UNIX-based computers that you will be monitoring. Click Close to close the Create Run As Account wizard.  12. In the Accounts pane, double-click the account you just created.  13. In the Run As Account Properties dialog box, select the Distribution tab and choose the Distribute credentials to selected computers option.  14. Click Add to open the Computer Search dialog box.  15. From the Option list, choose Show management servers, and then click Search.  16. In the Available items text box, choose the management server that these credentials will be distributed to, and then click Add.  17. Click OK to close the Computer Search dialog box.  18. Click OK to close the Run As Account Properties dialog box.  19. In the navigation pane under Run As Configuration, select Profiles.  20. In the results pane, right-click the UNIX Action Account or UNIX Privileged Account profile, and select properties from the context menu to open the Run As Profile Properties – UNIX Action Account or Run As Profile Properties – UNIX Privileged Account dialog box. Select the Associations tab.  21. Click Add, and then select Class from the list to open the Class Search dialog box.  22. In the Filter by: box, enter UNIX, and then click Search. The UNIX Computer Group appears in the Available items box.  23. Select UNIX Computer, and then click Add. The Unix Computer will appear in the Selected objects box. Click OK to close the Class Search dialog box.  24. In the Run As Profile Properties – UNIX Action Account dialog box, select Step by Step Run As UNIX Action Account or Step by Step Run As UNIX Privileged Account from the drop-down list in the Account column of the Selected Targets text box. Click OK to complete the creation of the association. |

Importing Cross Platform Management Packs

This topic describes how you can use the Import Management Packs Wizard to import and install cross-platform management packs.

To import the cross-platform management packs from the local system

|  |
| --- |
| 1. Open the Operations console with an account that is a member of the Operations Manager 2007 R2 Administrators profile.  2. Select the Administration view.  3. In the navigation pane, right-click Management Packs, and click Import Management Packs in the context menu to open the Import Management Packs Wizard.  4. In the Management Pack Wizard, click Add, and then click Add from disk to open the Select Management Pack to Import page.  5. On the Select Management Pack to Import page, in the list of management packs, select the management pack for the operating system that you want to monitor, and then click Open.  6. The management packs that you selected for import are added to the Import list box. An icon next to each management pack in the list indicates the status of the selection, as follows:   A green check indicates that the management pack can be imported.   A red error icon indicates that the management pack is dependent on other management packs that are not in the Import list and not available from the disk.  Note  Click the Error link under the Status column to see which dependent management packs are missing. Return to the Select Management Pack to Import page to select the dependent management packs.  7. When all selected management packs have a green check in their status field, click Install.  8. The Import Management Packs dialog box shows the installation progress for each management pack. Each management pack is downloaded to a temporary directory, imported to Operations Manager, and then deleted from the temporary directory. If there is a problem at any stage of the import process, you can select the management pack in the Import list box to view the status details.  9. Click Close to close the Imports Management Packs Wizard. |

Using the Discovery Wizard to Discover Systems and Deploy Cross Platform Agents

After the management packs have been imported, follow the steps in this section to launch the Discovery Wizard to discover available UNIX and Linux-based computers and deploy the agents.

To discover and deploy agents

|  |
| --- |
| 1. Open the Operations console with an account that is a member of the Operations Manager 2007 R2 Administrator profile.  2. Select the Administration view.  3. At the bottom of the navigation pane, select the Discovery Wizard link.  4. In the Computer and Device Management Wizard, select Discovery Type, choose Unix/Linux Discovery Wizard, and then click Next.  5. On the Discovery Method page, click Add to specify criteria for discovering UNIX-based systems and Linux-based systems on your network.  6. On the Define discovery criteria page, type the credentials and necessary information to locate the computer you want to discover, and then click OK.  7. On the Discovery Method page, click Add to add more computers to the Discovery Scope list. You can also click Edit or Remove to modify or delete computers from the Discovery Scope list.  8. In the Discovery Scope column, select the computer that you want to find.  9. In the Management Server list, select the management server that will monitor the agents.  10. Select Enable SSH based discovery if you want to push the agent installation instead of having the discovered system pull the agent from the management server.  Caution  Using SSH-based discovery is potentially dangerous because there is no way to check the SSH-key of the remote host. The discovery process sends the user name and password to the remote system. Only use SSH based discovery with systems that you know are running and trusted.  11. Click Discover to initiate system discovery.  12. If there is an invalid certificate on the discovered system or systems, the Certificate status page appears. Select the systems that you want new certificates issued to, and then click Sign.  Caution  Issuing a certificate for an unknown system can be potentially dangerous. Issue certificates only for systems that you know and trust. For more information about certificates and security, see the [Operations Manager 2007 R2 Security Guide](http://go.microsoft.com/fwlink/?LinkId=64017) (http://go.microsoft.com/fwlink/?LinkId=64017).  13. On the Discovery results page, in the Select the systems you want to manage: list, select the check box for the system or systems that you want to manage, or click Select All to include all discovered systems.  14. If there are systems listed in the Select the systems you want to manage list on the Discovery results page that the wizard was unable to discover, you can click Details to get information about why the discovery failed. Correct the problem and repeat the discovery step.  15. After you have selected the systems you want to manage, click Next to start the deployment, and to close the Discovery results page.  16. On the Deployment complete page, the Computer and Device Management Wizard displays the agent deployment status in the Status menu.  17. Click Done to close the wizard. |

Manually Installing Cross Platform Agents

Automatic System Discovery might not detect some UNIX and Linux systems due to firewalls or security issues. For example, if the UNIX or Linux root password is not available to the Microsoft System Center Operations Manager 2007 administrator, an error might result. Use the following procedures to manually install agents to UNIX and Linux systems. After agents are successfully deployed, rerun the Discovery Wizard from the Operations console to discover these systems.

To install the agent on Red Hat Enterprise Linux and SUSE Linux Enterprise Server

|  |
| --- |
| 1. Transfer the agent (scx-<version>-<os>-<arch>.rpm) to the Linux server.  scx-<version>-<os>-<arch>.rpm  2. To install the package, type  rpm -i scx-<version>-<os>-<arch>.rpm  3. To verify that the package is installed, type  rpm -q scx  4. To verify that the Microsoft SCX CIM Server is running, type  service scx-cmid status |

To install the agent on Solaris

|  |
| --- |
| 1. Transfer the agent (scx-<version>-<os>-<arch>.pkg.Z) to the Solaris server.  scx-<version>-<os>-<arch>.pkg.Z  2. Run the following command:  uncompress scx-<version>-<os>-<arch>.pkg.Z  3. To install the package, type  pkgadd -d scx-<version>-<os>-<arch>.pkg MSFTscx  4. To verify that the package is installed, type  pkginfo –l MSFTscx  5. To verify that the Microsoft SCX CIM Server is running, type  svcs scx-cimd |

To install the agent on HP-UX

|  |
| --- |
| 1. Transfer the agent (scx-<version>-<os>-<arch>.gz) to the HP server:  cp scx-<version>-<os>-<arch>.gz  2. To unzip the package, type  gzip –d scx-<version>-<os>-<arch>.gz  3. To install the package, type  swinstall –s /path/scx-<version>-<os>-<arch> scx  4. To verify that the package is installed, type  swlist scx  5. To verify that the Microsoft SCX CIM Server is running, type  ps –ef|grep scx  Look for the following process in the list:  scxcimserver |

To install the agent on AIX

|  |
| --- |
| 1. Transfer the agent (scx-<version>-<os>-<arch>.gz) to the AIX server:  cp scx-<version>-<os>-<arch>.gz  2. To unzip the package, type  gzip –d scx-<version>-<os>-<arch>.gz  3. To install the package, type  /usr/sbin/installp -a -d scx-<version>-<os>-<arch> scx  4. To verify that the package is installed, type  swlist scx  5. To verify that the Microsoft SCX CIM Server is running, type  ps –ef|grep scx  Look for the following process in the list:  scxcimserver |

Discovering Systems after Manual Deployment

After you have manually deployed agents to UNIX-based systems and Linux-based systems, they still need to be discovered by Operations Manager 2007 R2.

Follow the steps in the [Using the Discovery Wizard to Discover Systems and Deploy Cross Platform Agents](#z660b5f11b64448fd93891ca96a23fd4f) section of this guide to discover these UNIX-based systems and Linux-based systems, and pay attention to the following points.

 Because you identified the UNIX-based systems and Linux-based systems and deployed agents to them, you do not need to check Enable SSH based discovery.

 The manual deployment process issued an unsigned certificate to the system that the agent was deployed to. Because the certificate was unsigned, the Discovery wizard displays the Certificate status page, which allows you to issue a signed certificate as part of the discovery process.

Viewing System Monitors

You can use the Health Explorer in Microsoft System Center Operations Manager 2007 R2 to view and troubleshoot alerts, state changes, and other significant issues when you are monitoring computers on your network. Health Explorer organizes information in the following categories:

 Availability

 Configuration

 Performance

 Security

To view system monitors

|  |
| --- |
| 1. Open the Operations console with an account that is a member of the Operations Manager 2007 R2 Administrators profile.  2. Select the Monitoring view.  3. Expand the Cross Platform Servers folder.  4. Expand the folder for the server type that you want.  5. Click the Server State icon for the server type that you want.  6. In the results pane, double-click the green or red icon in the State column to open the Health Explorer dialog box.  7. Expand any of the monitoring categories to view the health state of that monitor. |

Uninstalling Cross Platform Management Packs and Agents

When you no longer need a management pack, you can delete it by using the Operations console. When you delete a management pack, all the settings and thresholds that are associated with it are removed from Microsoft System Center Operations Manager 2007 R2. The associated .mp or .xml file is not deleted from the hard disk of the management server. You can delete a management pack only if you have first deleted dependent management packs.

There are three ways to uninstall the cross platform management packs and agents.

1. Delete selected UNIX or Linux system management packs from the Operations Manager 2007 R2 console.

2. Delete an agent from Operations Manager 2007 R2, and uninstall the agent from the monitored computer. It will be uninstalled first from the UNIX or Linux computer.

3. Delete the agent from Operations Manager without uninstalling it on the UNIX or Linux host.

Use the following procedures to uninstall agents.

To delete a UNIX or Linux system management pack from the Operations console

|  |
| --- |
| 1. Open the Operations console with an account that is a member of the Operations Manager 2007 R2 Administrators profile.  2. Select the Administration view.  3. In the navigation pane, click Management Packs.  4. In the Management Packs pane, right-click the pack you want to remove.  5. Click Delete from the context menu. |

To delete a UNIX or Linux system agent from Operations Manager 2007 R2 and the monitored computer

|  |
| --- |
| 6. 0. 1. Open the Operations console with an account that is a member of the Operations Manager 2007 R2 Administrators profile.  2. Select the Administration view.  3. In the navigation pane, click UNIX/Linux Servers.  4. In the UNIX/Linux Servers pane, right-click the monitored computer agent you want to delete.  5. Select Uninstall from the context menu. |

Delete an agent from Operations Manager without uninstalling it on the UNIX or Linux host

|  |
| --- |
| 1. Open the Operations console with an account that is a member of the Operations Manager 2007 R2 Administrators profile.  2. Select the Administration view.  3. In the navigation pane, click UNIX/Linux Servers.  4. In the UNIX/Linux Servers pane, right-click the monitored computer agent you want to remove.  5. Select Delete from the context menu. |

After the UNIX or Linux computer has been deleted from the list of monitored computers, you must log on to the monitored computer and manually uninstall the agent. Use the following procedures to manually uninstall agents from UNIX and Linux computers.

To uninstall the agent from Red Hat enterprise Linux and SUSE Linux enterprise servers:

|  |
| --- |
| 1. Log on as the root user, and uninstall the agent by typing  rpm –e scx  2. To verify that the package is uninstalled, type  rpm –q scx |

To uninstall the agent from Solaris computers

|  |
| --- |
| 1. Log on as the root user, and uninstall the agent by typing  pkgrm MSFTscx  2. To verify that the package is uninstalled, type  pkginfo –I MSFTscx |

To uninstall the agent from HP-UX

|  |
| --- |
| 1. Log on as the root user, and uninstall the agent by typing  swremove scx  2. To verify that the package is uninstalled, type  swlist scx |

To uninstall the agent from IBM AIX

|  |
| --- |
| 1. Log on as the root user, and uninstall the agent by typing  installp –u scx  2. To verify that the package is uninstalled, type  lslpp –L scx.rte |

Working with Agents

After you have installed agents on the managed Windows-based computers in your environment and configured Microsoft System Center Operations Manager 2007 to manage them, Operations Manager begins collecting monitoring data as soon as you import management packs (as discussed in the “How to Import a Management Pack in Operations Manager 2007” topic in the [Operations Manager 2007 R2 User’s Guide](http://go.microsoft.com/fwlink/?LinkId=150555) (http://go.microsoft.com/fwlink/?LinkId=150555). Aside from managing the data collected, there are a number of administrative tasks regarding agents. The following sections discuss those tasks.

|  |  |
| --- | --- |
| Task | Where to find information |
| Check agent status. | [Understanding Agent States](#z4e2c561d48b04710884da3ff244fb30a) |
| Change heartbeat settings. | [Heartbeat and Heartbeat Failure Settings in Operations Manager 2007](#z5cfa1c3f1ed8443b9ea363825b839fce) |
| Set up an agent to report to more than one management server. | [Configure an Agent to Report to Multiple Management Groups](#zb659927e00a1457693464ed56394796d) |
| Monitor a resource without an agent. | [Use Agentless Monitoring](#zf4d6489ba2af4dd297447123490fb64f) |

Understanding Agent States

You can view the state (or health) of an agent in the Agent Health State view. The agent state is relayed by the Health Service Watcher, which monitors the status of agents. You can get more information about the state of an agent by going to the Health Service Watcher view.

An agent can have one of the following states:

|  |  |
| --- | --- |
| State | Description |
| Healthy – green check mark | The agent is running normally. |
| Critical – red check mark | There is a problem on the agent. |
| Unknown – gray agent. The check mark and agent name are grayed out. | The health service watcher on the root management server (RMS) that is watching the health service on the monitored computer is not receiving heartbeats from the agent anymore.  It had been receiving them previously (and it was reported as healthy), but now it is not. This also means that the management servers are no longer receiving any information from the agent at all.  The computer running the agent might be down, or there might be connectivity issues. You can find more information on the Health Service Watcher view. |
| Unknown – green circle with no check mark | The status of the discovered item is unknown. There is no monitor available for this specific discovered item. |

Heartbeat and Heartbeat Failure Settings in Operations Manager 2007

An agent sends a packet of data to its management server on a periodic basis; by default, once every 60 seconds. This packet of data is called the heartbeat. By default, a management server can tolerate three missed heartbeats. If the management server registers four missed heartbeats, an alert will be generated against the health service on the agent computer indicating it is no longer available. The management server then attempts to diagnose the problem by pinging the agent computer. If the ping is unsuccessful, another alert is generated, indicating that the computer is no longer reachable.

If the management server and the agent are separated by a slow connection, it might be normal for three minutes to pass without the management server receiving a heartbeat. To prevent unnecessary alerts, you can increase the number of missed heartbeats that a management server will tolerate.

It is also possible that you might be monitoring critical applications in your environment and service-level agreements might not allow waiting three minutes before alerts are generated. In this situation, you can decrease the heartbeat interval, thus increasing how often an agent sends a heartbeat.

There are two settings you can adjust that relate to the heartbeat: the heartbeat interval and the number of missed heartbeats. Heartbeat interval refers to how often an agent sends a heartbeat. Number of missed heartbeats refers to how many heartbeats a management server will tolerate before running a diagnostic ping. Heartbeat interval and number of missed heartbeats can be configured at a global level and thus affect every agent and management server in the management group. In addition, the number of missed heartbeats can be overridden at the management server level and heartbeat interval can be overridden at the agent level.

In addition to using these options for failure settings, you also have the option of disabling heartbeat monitoring for all agents or for the following specified agents:

 That connect to the network intermittently.

 That connect to the network over poor connections or use dial-up connections.

 On systems that are frequently restarted.

Global Heartbeat Settings

The following heartbeat settings are set at a global level and affect all management servers and agents in the management group.

How to Globally Change the Heartbeat Interval

The following procedure shows how to change the heartbeat interval at the global level. Changes made in this procedure affect all the agents in the management group.

To configure agent heartbeat interval settings

|  |
| --- |
| 1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Microsoft System Center Operations Manager 2007 management group.  2. In the Operations console, click the Administration button.  3. In the Administration pane, expand Administration, and then click Settings.  4. In the Settings pane, expand Type: Agent, right-click Heartbeat, and then click Properties.  5. In the Global Agent Settings - Heartbeat dialog box, on the General tab, enter a value in the Heartbeat interval box to specify how often an agent generates a heartbeat, and then click OK.  Note  The maximum value is 86,400 seconds (1 day). The minimum value is 5 seconds. |

How to Globally Change the Number of Missed Heartbeats a Management Server Will Tolerate

The following procedure shows how to change the number of missed heartbeats at the global level. Changes made in this procedure affect all the management servers in the management group.

To change the number of missed heartbeats a management server will tolerate

|  |
| --- |
| 1. Log on to the Operations console with an account that is a member of the Administrators role for the Operations Manager 2007 management group.  2. Click the Administration button.  3. In the Administration pane, expand Administration, and then click Settings.  4. In the Settings pane, expand Type: Server, right-click Heartbeat, and then click Properties.  5. In the Global Management Server Settings - Heartbeat dialog box, on the General tab, in the Number of missing heartbeats allowed, enter or select the number of missing heartbeats the management server will allow before it starts to ping the agent.  Note  The maximum value allowed for the number of missing heartbeats is 100. The minimum value allowed is 1. |

Management Server- Heartbeat Settings and Agent-Specific Heartbeat Settings

The following heartbeat settings can be configured on a per-management server basis.

How to Override the Heartbeat Interval

Use the following procedure to override the agent heartbeat interval settings for a specific agent.

To override the heartbeat interval setting

|  |
| --- |
| 1. Log on to the Operations console with an account that is a member of the Administrators role for the Operations Manager 2007 management group.  2. Click the Administration button.  3. In the Administration pane, expand Administration, expand Device Management, and then click Agent Managed.  4. In the results pane, right-click the object that you want to view the properties of, and then click Properties.  5. In the Agent Properties dialog box, select Override global server settings.  6. Change the Heartbeat interval. The maximum value allowed for the heartbeat interval is 86,400 seconds (1 day). The minimum value allowed is 5 seconds.  7. Click OK. |

How to Override the Number of Missed Heartbeats a Management Server Will Tolerate

Use the following procedure to override the management group heartbeat failure setting and configure the number of missed heartbeats a specific management server will allow for an agent before it changes the state of the respective computer.

To override the number of missed heartbeats

|  |
| --- |
| 1. Log on to the Operations console with an account that is a member of the Administrators role for the Operations Manager 2007 management group.  2. Click the Administration button.  3. In the Administration pane, expand Administration, expand Device Management, and then click Management Servers.  4. In the Management Server Properties dialog box, click the Heartbeat tab.  5. On the Heartbeat tab, do the following:  a. Select Override global server settings.  b. Change the Number of missing heartbeats to the number that you want.  6. Click OK. |

Disabling Heartbeat Monitoring

You can disable heartbeat monitoring for all agents or for specified agents.

To disable monitoring for all agents

|  |
| --- |
| 1. Click Authoring to open the Authoring area.  2. Expand Management Pack Objects, and then click Monitors.  3. Find and right-click the Health Service Heartbeat Failure monitor for Health Service Watcher (Agent).  Note  You can also use Find Now to find the monitor.  4. On the shortcut menu, point to Overrides, point to Disable the Monitor, and then click For all objects of the type: Health Service Watcher (Agent).  5. Expand Management Pack Objects, and then click Rules.  6. Find and right-click Heartbeat Failure - Success under Health Service Watcher Group (Agent).  7. On the shortcut menu, point to Overrides, point to Disable the Rule, and then click For all objects of the type: Health Service Watcher (Agent).  8. Repeat steps 6 and 7 to disable the rules Heartbeat Failure - Warning and Heartbeat Failure - Error. |

To disable monitoring for a subset of managed systems, create a group by using the Create Group Wizard. For instance, to disable monitoring for the systems Server01.contoso.com, Server78.contoso.com, and Server99.contoso.com, create a group called Heartbeat Monitor Disabled Agents containing members of the type Health Service Watcher Group (Agent) and add the systems to that group.

For information about creating groups, see [How to Create Groups in Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkID=101188).

To disable monitoring for a group of agents

|  |
| --- |
| 1. Click Authoring to open the Authoring area.  2. Expand Management Pack Objects, and then click Monitors.  3. Find and right-click the Health Service Heartbeat Failure monitor for Health Service Watcher (Agent).  4. Click Authoring to open the Authoring area.  5. Expand Management Pack Objects and click Monitors.  6. Right-click the Health Service Heartbeat Failure monitor for Health Service Watcher (Agent).  Note  Use Find Now, if necessary, to find the monitor.  7. On the shortcut menu, point to Overrides, point to Disable the Monitor and then click For all objects of the type: Health Service Watcher (Agent).  8. In the Select Object dialog box, click the group to be used (in this example, Heartbeat Monitor Disabled Agents), and then click OK.  9. Expand Management Pack Objects, and then click Rules.  10. Find and right-click Heartbeat Failure - Success under Health Services Watcher Group (Agent).  11. Right-click, point to Overrides, point to Disable the Rule, and then click For a group.  12. In the Select Object dialog box, click the group to be used (in this example, Heartbeat Monitor Disabled Agents), and then click OK.  13. Click Yes to confirm.  14. Repeat steps 7 through 13 to disable the rules Heartbeat Failure-Warning and Heartbeat Failure - Error. |

Configure an Agent to Report to Multiple Management Groups

Use the following procedure to make an Operations Manager 2007 agent a member of multiple management groups, also referred to as multihoming. For example, an agent can be configured to report Active Directory data to the Networking Management Group and Exchange data to the Messaging Management Group. An agent can be a member of up to four management groups.

You do not need to use the same deployment method for all of the management groups.

You can also use Active Directory Domain Services to assign agents to management groups. For more information, see How to Use Active Directory to Assign Computers to an Operations Manager 2007 Management Group.

Note

It might take one day or longer for the discovered instances of the agent to be made part of the new management group. They will be added after the next discovery interval.

To make an Operations Manager 2007 agent a member of multiple management groups

|  |
| --- |
|  Do one of the following:  a. Run the Discovery Wizard from the Operations Manager 2007 Operations console that is connected to the new management group, select the desired computers, and deploy the agent to them. For more information, see How to Deploy the Operations Manager 2007 Agent to Windows-Based Computers from the Operations Console.  b. Run the MOMAgent.msi on the desired computers, and modify the installation by adding a new management group. For more information, see How to Deploy the Operations Manager 2007 Agent Using the Agent Setup Wizard. |

See Also

Use Agentless Monitoring

Microsoft Windows-based systems in which an agent cannot be installed can be managed without an agent. This is called agentless management.

Note

Not all management packs support agentless management, so make sure agentless management will serve your needs before using it. In particular, the Active Directory management pack and the Microsoft Exchange Server 2003 management pack do not support agentless management.

Agentless management of computers is different from Agentless Exception Monitoring. Though they are similar in name, Agentless Exception Monitoring is used to aggregate, view, and report on error reports that are sent by the Windows Error Reporting service.

The Discovery Wizard can find and set up systems for agentless management. The process is almost the same as for deploying. You do, however, have to select a proxy for each agentless-managed system. A proxy is a system with an agent that is used to monitor an agentless system. A management group can serve as a proxy, but this takes up system resources. A best practice is using an agent-managed system as a proxy. This system must be set up for management before running the Discovery Wizard to establish agentless management.

Note

If a proxy is removed from management, its agentless systems are no longer managed.

Both the agentless-managed system and its proxy need to have access to the managing server through any firewalls. For more information about interacting with firewalls, see the [Operations Manager 2007 Security Guide](http://go.microsoft.com/fwlink/?LinkId=64017) (http://go.microsoft.com/fwlink/?LinkId=64017).

Note

When you are monitoring virtual servers on a cluster, you must deploy agents to the cluster nodes, configure them to be managed as a proxy and then monitor the virtual servers as you would monitor an agentless-managed computer.

To configure an agent-managed computer as a proxy for agentless-managed computers

|  |
| --- |
| 1. In the Agent Properties dialog box, click the Security tab.  2. On the Security tab, select Allow this agent to act as a proxy and discover managed objects on other computers, and then click OK. |

To discover Windows-based computers and configure Operations Manager 2007 to manage them as agentless-managed computers

|  |
| --- |
| 1. Log on to the Operations console with an account that is a member of the Operations Manager Administrators role for the Microsoft System Center Operations Manager 2007 management group.  2. Click Administration.  3. At the bottom of the navigation pane, click Discovery Wizard.  4. On the Introduction page, click Next. The Introduction page will be skipped if the Computer and Device Management Wizard has been run before and Do not show this page again was selected.  5. On the Auto or Advanced? page, do one of the following:  a. Select either Automatic computer discovery or Advanced discovery. If you select Automatic computer discovery, click Next, and then go to step 6. If you select Advanced discovery, continue with the following steps.  Note  Automatic computer discovery scans for Windows-based computers in the domain where the root management server is installed. You can use advanced discovery to specify criteria for the computers the wizard will return, such as computer names starting with NY.  b. In the Computer & Device Types list, select Servers & Clients, Servers Only, or Clients Only.  c. In the Management Server list, click the management server or gateway server to discover the computers.  Note  For more information about gateway servers, see the [Operations Manager 2007 Security Guide](http://go.microsoft.com/fwlink/?LinkId=64017) (http://go.microsoft.com/fwlink/?LinkId=64017).  d. If you selected Servers & Clients, you can select the Verify discovered computers can be contacted check box. This is likely to increase the success rate of agent deployment, but discovery can take longer.  e. Click Next.  Note  The wizard can return approximately 4000 computers if Verify discovered computers can be contacted is selected, and it can return 10,000 computers if it is not selected. Automatic computer discovery verifies that discovered computers can be contacted. A computer that is already managed by the management group is not returned.  6. On the Discovery Method page, you can locate the computers that you want to manage by either scanning or browsing Active Directory or by typing the computer names.  If you want to scan, do the following:  a. Select Scan Active Directory, if it is not already selected, and then click Configure.  b. In the Find Computers dialog box, type the criteria that you want to use for discovering computers, and then click OK.  c. In the Domain list, click the domain of the computers that you want to discover.  If you want to browse Active Directory or type the computer names, do the following:   Select Browse for, or type-in computer names, click Browse, specify the names of the computers that you want to manage, and then click OK.   In the Browse for, or type-in computer names box, type the computer names, separated by a semi-colon, comma, or new line [ENTER].  7. Click Next, and then on the Administrator Account page, do one of the following:   Select Use selected Management Server Action Account, if it is not already selected, and then click Discover.   Select Other user account, type the User name and Password, and then select the Domain from the list. If the user name is not a domain account, select This is a local computer account, not a domain account.  Important  The account must have administrative privileges on the targeted computers. If This is a local computer account, not a domain account is selected, the Management Server Action Account will be used to perform discovery. For more information about Operations Manager 2007 accounts, see the [Operations Manager 2007 Security Guide](http://go.microsoft.com/fwlink/?LinkId=64017) (http://go.microsoft.com/fwlink/?LinkId=64017).  8. Click Discover to display the Discovery Progress page. The time it takes discovery to finish depends on many factors, such as the criteria that are specified and the configuration of the IT environment.  9. On the Select Objects to Manage page, do the following:  a. Select the computers you want to manage as agentless-managed computers.  b. In the Management Mode list, click Agentless.  c. Click Change, select the Proxy Agent that you want to use, click OK, and then click Next.  Important  An agentless-managed computer places greater resource requirements on the management server than an agent-managed computer. Therefore, an agent-managed computer that is configured as a proxy is recommended for managing agentless-managed computers.  10. On the Summary page, click Finish. The computers will appear in the Agentless Managed node of the Administration pane in the Operations console, and they are ready to be managed. |

Investigating and Resolving Alerts

Microsoft System Center Operations Manager 2007 displays alerts in the Operations console and the Web console as specified by monitors and rules. Any alert is an indication of an issue that has occurred somewhere in your environment. Individual alerts can pertain to individual monitored devices, such as a malfunctioning hard drive on a computer, or to an issue with a distributed application, such as Microsoft Exchange or Active Directory.

When you are addressing issues with alerts, you must consider the following:

 The severity of the alert.

 The number of times the alert has occurred.

 The importance to your organization of the application or device that the alert refers to.

 Knowing this information will allow you to prioritize the order in which alerts will be investigated and resolve the underlying issues.

The following topics provide detailed information about resolving alerts:

 [Investigate Alerts](#z1ea0affd1186482caac30b5243054dd4)

 [Investigate Alert Storms](#za54350fde6434df4883699cbbe9b5aa7)

 [Resolve a Heartbeat Alert](#z75627937d3ef4b6a9f4abae2db3050d7)

Investigate Alerts

You can review and investigate alerts in the Monitoring pane of the Operations console or the Web console. The Web console displays the same alert information as the Operations console, but it provides fewer tools to deal with the alert because it does not support the Tasks feature.

To view an alert

|  |
| --- |
| 1. In the Operations console, click Monitoring.  2. In the Monitoring pane, expand Monitoring, and then click Active Alerts.  3. In the Active Alerts pane, click the alert to highlight it. |

Microsoft System Center Operations Manager 2007 displays the Alert Details in the details pane at the bottom of the screen. Details include which monitor is involved and information about the alert and what can cause it.

The Actions pane on the right of the screen contains links to tools and scripts that can be used to diagnose and resolve the alert. Click Actions on the toolbar to display the Actions pane if the pane is not visible. The Actions pane includes links to the settings of the monitor, Operations Manager Health Explorer, controls for Maintenance Mode, tasks for the monitor, and additional resources and help.

Using Health Explorer

Use Health Explorer to find out what monitor is reacting and to review knowledge about the monitor and possible causes for actions related to it. Click the alert to highlight it. The Health Explorer link under Alert Actions becomes active.

By default, when the Health Explorer window opens, all monitors in a failed state are expanded. If a monitor contains other monitors, as in the case of a roll-up monitor, Health Explorer shows all monitors in a hierarchical layout, displaying monitoring data for all dependent services and applications. To view more information about any dependent monitor, you can right-click that monitor, and then click Monitor Properties to open another Health Explorer window.

For more information about Health Explorer, see Operations Manager 2007 Help.

Using Tasks

In the Actions pane on the right of the screen, the Operations console provides tasks to troubleshoot individual alerts.

Note

If the Actions pane is not displayed, click Actions to display it.

Click an alert to highlight it to see tasks for that alert. Click a task to run the task.

Different alerts, which are raised by different monitors, offer different tasks for investigating and resolving the alert. For some examples of using tasks, see the [Resolve a Heartbeat Alert](#z75627937d3ef4b6a9f4abae2db3050d7) section of this guide.

Closing Alerts

Monitors can be configured to automatically close alerts that have been resolved. You also have the option of manually closing an alert.

To view an alert

|  |
| --- |
| 1. In the Operations console, click Monitoring.  2. In the Monitoring pane, expand Monitoring, and then click Active Alerts.  3. In the Active Alerts pane, right-click the alert, and then click Close Alert.  Note  Select multiple alerts by pressing and holding down the CTRL key when clicking alerts. |

Using Monitor Properties

After you investigate the cause of an alert, you can improve the process of dealing with similar alerts.

You can record knowledge about the alert in the Company Knowledge tab. You can view and edit company knowledge by highlighting an alert, clicking View or edit the settings of the monitor, and then clicking the Company Knowledge tab.

You can also create tasks to diagnose and recover from alerts. Diagnostic and recovery tasks can run automatically when an alert is created. You can manage diagnostic and recovery tasks by highlighting an alert, clicking View or edit the settings of the monitor, and then clicking the Diagnostic and Recovery tab.

Overriding a Monitor

You can use overrides to refine the settings of a monitoring object in Operations Manager 2007. As you fine-tune your monitors, many useless alerts will be avoided.

To override a monitor

|  |
| --- |
| 1. In the Operations console, click the Authoring button.  2. In the Authoring pane, expand Management Pack Objects and then click Monitors.  3. In the details pane, expand an object type completely, and then click a monitor.  4. On the Operations Manager toolbar, click Overrides, and then point to Override the Monitor. You can choose to override this monitor for objects of a specific type or for all objects within a group. After you choose which group of object type to override, the Override Properties dialog box opens, enabling you to view the default settings contained in this monitor. You can then choose whether to override each individual setting contained in the monitor.  Note  If the Overrides button is not available, make sure you have selected a monitor and not a container object in the Monitors pane.  5. Select each setting that you want to override. When you complete your changes, click OK. |

Investigate Alert Storms

A large and sudden increase in the number of alerts is called an alert storm. An alert storm can be a symptom of massive changes of some kind within your management group, such as the catastrophic failure of networks. An alert storm can also be a symptom of configuration issues within Microsoft System Center Operations Manager 2007.

Installing new or updated management packs can give rise to an alert storm. Monitors in a management pack begin working as soon as the management pack has been imported. Use best practices in importing management packs to minimize alert storms.

Finding Alert Storms

For general, real-time monitoring of alerts, use the Active Alerts view. Make sure Scope is not active and hiding alerts.

Check for large numbers of alerts when your network undergoes changes. Monitor closely when you install a new management pack.

Operations Manager 2007 offers reports that can be useful in identifying alert storms. From an Operations console with access to a reporting server, look at the Microsoft Generic Report Library. The reports Most Common Alerts and Most Common Events help identify high-volume alerts.

Modifying Monitors and Rules

If you are getting a large number of alerts that do not point to issues in your managed systems, you need to modify the monitors or rules that create those alerts.

View active alert details in the Monitoring pane. Alert Details specifies the monitor or rule for an alert.

Modify the monitor using overrides. The procedure for overriding rules is the same as for monitors. See how your overrides affect the amount of alerts and continue to fine-tune the monitors as necessary.

About Suppressed Alerts

Rules offer the option of suppressing duplicate alerts. A suppressed alert is not displayed in the Operations console.

Operations Manager 2007 suppresses only duplicate alerts as defined by the alert suppression criteria. Fields stated in the suppression criteria must be identical for the alert to be considered a duplicate and suppressed. An alert must be created by the same rule and be unresolved to be considered a duplicate.

Resolve a Heartbeat Alert

The Health Service sends a heartbeat to a management server to verify that the system is still responding. When a specified number of heartbeats fail to arrive, Microsoft System Center Operations Manager 2007 displays an alert.

This section shows how to investigate a Health Service Heartbeat Failure alert as an example. Different alerts have different causes and different resolutions.

If you want to walk through these procedures, you can cause this alert by disabling the System Center Management service on a test system.

To cause a Health Service heartbeat failure for testing

|  |
| --- |
| 1. On a system with an agent installed, open Control Panel.  2. Double-click Administrative Tools.  3. Double-click Services.  4. Right-click the System Center Management service, and then click Stop.  Note  Use this same procedure, selecting Start in step 4, when you are done testing. |

How to Investigate Agent Heartbeat Issues

The Monitoring pane displays active alerts. Looking at an alert provides information and tools to investigate with.

To investigate an active alert

|  |
| --- |
| 1. Open the Operations console.  2. Click Monitoring.  3. If necessary, in the Monitoring pane, click Monitoring to expand it.  4. Click Active Alerts to view the Health Service Heartbeat Alert.  Note  Depending on the heartbeat interval and the number of missing heartbeats, a few minutes might be required to see the alert.  5. Click the alert to highlight it and read the information in the Alert Details area. The Alert Details area provides information about the alert, including a description and knowledge about the cause and resolution. |

How to Troubleshoot Agent Heartbeat Issues

Use the tasks in the Action pane to diagnose the cause of the alert. Different alerts have different tasks. For a Health Service Heartbeat Failure alert, the tasks deal with pinging the system and verifying or restarting the service.

To use the action tasks in troubleshooting

|  |
| --- |
| 1. If necessary, click Actions to make the Actions pane visible.  2. In the Actions pane, under Health Service Watcher Tasks, click Ping Computer. The task opens a dialog box to display its progress.  Note  If the ping fails, use standard networking troubleshooting to figure out the issue with connectivity. Verify that the system is turned on.  3. Click Close to close the dialog box.  4. Under Health Service Watcher Tasks, click Computer Management. A Computer Management dialog box for the target system opens.  5. Click Services and Applications to expand it.  6. Click Services to display services.  7. Right-click the System Center Management service, and then click Start.  Note  After the connection with the agent is restored, the alert will be automatically resolved and the computer status will go back to healthy. |

These steps will fix the test failure created in this topic, as well as address a number of possible causes of a Health Service Heartbeat Failure. If an actual failure is not resolved by these steps, use standard troubleshooting techniques to figure out the cause of the issue. For instance, the alert displayed in Active Alerts shows how old the alert is. Check for events that happened at this time to see what might have caused an issue.

Configuring the Customer Experience Improvement Program (CEIP) in Operations Manager 2007

The Microsoft Customer Experience Improvement Program (CEIP) collects information about how you use Microsoft programs and about some of the issues you might encounter. Microsoft uses this information to improve the products and features you use most often and to help solve issues. Participation in the program is strictly voluntary.

When you choose to participate in the CEIP, you configure clients with Group Policy to redirect CEIP reports to a Microsoft System Center Operations Manager 2007 management server, instead of reporting directly to Microsoft. The management servers are configured to forward these reports to Microsoft.

Important

The CEIP reports do not contain contact information about you or your organization, such as names or an address.

The CEIP reports forwarded from your organization to Microsoft are combined with CEIP reports from other organizations and individual customers to help Microsoft solve issues and improve the Microsoft products and features customers use most often. For more information about the CEIP, see[the CEIP page](http://go.microsoft.com/fwlink/?linkid=75040) (http://go.microsoft.com/fwlink/?linkid=75040).

Use the following procedure to configure CEIP settings. The management server must have access to the Internet to participate in the program.

Important

CEIP is a component of the Client Monitoring feature of Operations Manager 2007. Client Monitoring must be enabled on at least one management server and managed computers to participate in the CEIP. For information about enabling the Client Monitoring feature of Operations Manager 2007, see [Configure Client Monitoring in Operations Manager 2007](#z95a7881bc94f49b099eac2a54cd415f1) in this guide. After a management server has been configured for client monitoring, all agents that are participating in CEIP should be configured via Group Policy to send their CEIP data to that management server.

To configure the CEIP settings for Operations Manager 2007

|  |
| --- |
| 1. Log on to a management server with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 management group.  2. In the Operations console, click the Administration button.  3. In the Administration pane, expand Administration, and then click Settings.  4. In the Settings pane, expand Type: General, right-click Privacy, and then click Properties.  5. In the Global Management Server Group Settings - Privacy dialog box, on the CEIP tab, click Join the Customer Experience Improvement Program to join the CEIP program or click I don't want to join the program at this time to decline participation.  Note  You can click Tell me more about the program to view information about the CEIP program, including the privacy policy. |

Configuring Operational Data Reports in Operations Manager 2007

The Microsoft Customer Experience Improvement Program (CEIP) collects information about how you use Microsoft programs and about some of the issues you might encounter. Microsoft uses this information to improve the products and features you use most often and to help solve issues. Participation in the program is strictly voluntary.

During setup of Microsoft System Center Operations Manager 2007 Reporting, on the Operational Data Reports page, you have the option to join CEIP. If you elect to join CEIP, Operations Manager 2007 Reporting collects a summary of how Operations Manager 2007 is being used and sends reports to Microsoft on a weekly basis. Microsoft uses these reports to improve the quality of its management packs and Operations Manager 2007. You can view the contents of these operational data reports (ODRs) by creating a Microsoft ODR Report.

Note

Before configuring operational data reports, make sure that Operations Manager 2007 Reporting is installed, and that the management server has access to the Internet so that reports can be sent to Microsoft.

To configure the operational data reports settings

|  |
| --- |
| 1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 management group.  2. In the Operations console, click the Administration button.  3. In the Administration pane, expand Administration, and then click Settings.  4. In the Settings pane, expand Type: General, right-click Privacy, and then click Properties.  5. In the Global Management Server Settings - Privacy dialog box, on the Operational Data Reports tab, click Yes, send operational data reports to Microsoft (recommended) to send reports or click No, don't send operational data reports to Microsoft to decline participation.  6. Click OK. |

To create a Microsoft ODR Report

|  |
| --- |
| 1. Log on to the computer with an account that is a member of the Operations Manager Report Operators role for the Operations Manager 2007 management group.  2. In the Operations console, click the Reporting button.  3. In the Reporting pane, expand Reporting, and then click Microsoft ODR Report Library.  4. In the Microsoft ODR Report Library Reports pane, right-click one of the reports (for example, Management Packs), and then click Open.  5. In the Report view, in the Parameter area, click the down arrow in the From box, point to This week, and then click Sunday.  6. Click the down arrow in the To box, point to This week, and then click Saturday.  7. Click Run to display the ODR Report.  8. Click Close to close the report. |

Configure Client Monitoring in Operations Manager 2007

Use the following procedures to configure a management server for the server component of the Client Monitoring feature of Microsoft System Center Operations Manager 2007.

Important

If you plan to configure the management server to forward error reports to Microsoft and receive links to available solutions for those errors or participate in the Customer Experience Improvement Program (CEIP), you must first configure the management server's proxy settings if it uses a proxy server to access the Internet. For more information, see the [Configuring Internet Proxy Settings for a Management Server](#z3) section.

The Operations Manager 2007 Client Monitoring Configuration Wizard is used to configure the server component of Client Monitoring on an Operations Manager 2007 management server. To configure the server component of Client Monitoring on multiple management servers, run the wizard once for each management server. An example of when you might configure multiple management servers for Client Monitoring is if the connection between specific clients and management servers is less expensive.

Important

The management server and error reporting clients must be in the same domain or in fully trusted domains.

To open the Client Monitoring Configuration Wizard

|  |
| --- |
| 1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 management group.  2. In the Operations console, click the Administration button.  3. In the Administration pane, expand Administration, expand Device Management, and then click Management Servers.  4. In the management servers pane, right-click the management server on which you want to enable Client Monitoring, and then click Configure Client Monitoring. This starts the Client Monitoring Configuration Wizard. Use the same procedure to Disable Client Monitoring on the management server. You must also disable Client Monitoring on the clients. For more information, see Configuring Clients for Client Monitoring below.  Note  The Configure Client Monitoring option will be unavailable if the selected computer is a gateway server. |

To configure Client Monitoring using the Client Monitoring Configuration Wizard

|  |
| --- |
| 1. On the Introduction page of the Client Monitoring Configuration Wizard, click Next. The Introduction page will be skipped if the wizard has been run before and Do not show this page again was selected.  2. On the Customer Experience Improvement Program page, do one of the following:   Leave the default option of No if you do not want your organization to participate in the program, and then click Next.  Or follow these steps:  a. Select Yes, if you want your organization to participate in the program.  b. Leave Use Secure Socket Layer (SSL) protocol selected if you have installed a certificate on your management server, and leave Use Windows Authentication selected if you want the client computers to authenticate with the management server; otherwise, clear the options.  c. Type the appropriate Port, or leave the default of 51907, and then click Next.  Important  For information about installing a certificate on a management server, see the [Operations Manager 2007 Security Guide](http://go.microsoft.com/fwlink/?LinkId=64017) (http://go.microsoft.com/fwlink/?LinkId=64017).  3. On the Configure Error Collection page, do the following:  a. Type the local or attached File Share Path, such as C:\ErrorData, for the management server that will be used to collect error reports. The files share will be created at the local path on the management server and shared with the necessary permissions.  Important  The file share path must be on an NTFS partition and have at least 2 GB of free disk space. It is recommended that the path be no longer than 120 characters. The file share path can be a UNC path or mapped drive letter.  b. Select Collect application errors from Windows Vista or later computers if you will be managing Windows Vista or later operating systems with Operations Manager 2007. Type the Port number, or leave the default 51906. Leave Use Secure Socket Layer protocol selected if you have installed a certificate on your management server, and leave Use Windows Authentication selected if you want the client computers to authenticate with the management server; otherwise, clear the options.  c. Type the Organization Name, using no more than 22 characters, and then click Next. The organization name can display on computers experiencing errors and running Windows Server 2008 and earlier operating systems.  4. On the Configure Error Forwarding page, do one of the following:   Leave the Automatically forward all collected errors to Microsoft check box cleared, and then click Next.  Or follow these steps:  a. Select Automatically forward all collected errors to Microsoft if the management server is connected to the Internet and you want to forward error reports to Microsoft and receive links to available solutions for those errors.  b. Select Detailed to help ensure Microsoft can provide a solution to the issue, or leave the default setting of Basic.  c. Click Next.  5. On the Create File Share page, do one of the following:   Select an Existing User Account from the list, and then click Next.   Select Other user account, type the User name and Password, select the Domain from the list, and then click Next.  Important  The account must have the permissions necessary to create a file share on the path provided in step 3a.  6. On the Create File Share: Task Status page, after the file share has been successfully created, click Next.  Note  To modify the Client Monitoring settings on the management server, such as the file share, you must disable and then re-enable Client Monitoring on the management server. You must also then modify the Client Monitoring Group Policy settings on the clients.  7. On the Deploy Configuration Settings page, type or browse to the location where you would like to save the <ServerName>.ADM file that contains the Client Monitoring Group Policy settings you have just made with the wizard, and then click Finish.  Important  You must use the <ServerName>.ADM file to configure clients to redirect their Client Monitoring data to the management server. For more information, see Configuring Clients for Client Monitoring below. |

Configuring Internet Proxy Settings for a Management Server

Use the following procedure to configure the Internet proxy settings for an Operations Manager 2007 management server. You must configure these settings if features of Operations Manager 2007 are enabled that require the management server to communicate over the Internet. For example, you must configure these settings if the Client Monitoring feature of Operations Manager 2007 is configured to transmit or receive data from Microsoft.

To configure the Internet proxy settings for an Operations Manager 2007 management server

|  |
| --- |
| 1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 management group.  2. In the Operations console, click the Administration button.  3. In the Administration pane, expand Administration, expand Device Management, and then click Management Servers.  4. In the results pane, right-click the management server for which you want to view the properties, and then click Properties.  5. In the Management Server Properties dialog box, click the Proxy Settings tab.  6. On the Proxy Settings tab, select Use a proxy server for communication with Microsoft and then do the following:   Select http:// or https:// from the drop-down list, and type the name of the Internet proxy server in the Address text box.   Type the Port number, and then click OK. |

Configuring Clients for Client Monitoring

This topic provides the procedure to configure clients for the Client Monitoring feature of Operations Manager 2007.

Important

You must first configure a management server for the server component of Client Monitoring by running the Client Monitoring Configuration Wizard as described above.

To configure clients for Client Monitoring

|  |
| --- |
| 1. Run the Group Policy Object Editor (gpedit.msc) for the domain or local computer.  Note  For information about Group Policy, see the [Group Policy](http://go.microsoft.com/fwlink/?LinkId=152221) Web page (http://go.microsoft.com/fwlink/?LinkId=152221).  2. Disable the Turn off Windows Error Reporting policy. This policy can be found in Computer Configuration/Administrative Templates/System/Internet Communication Management/Internet Communication settings.  3. Add the Agentless Exception Monitoring (AEM) Group Policy administrative template (<ServerName>.ADM) to the domain or local computer policy. The ADM file is created when the Client Monitoring Configuration Wizard is run.  4. Enable the AEM policies that reflect the configuration of Client Monitoring on the Operations Manager 2007 management server. The AEM policies can be found in Computer Configuration/Administrative Templates/Microsoft Applications/Microsoft Operations Manager.  Note  Use the same procedure to disable the Group Policy settings, thereby disabling Client Monitoring on the clients. |

Configuring Error Reporting in Operations Manager 2007

When error reporting is enabled for Microsoft System Center Operations Manager 2007 components, if an error occurs in an Operations Manager 2007 component, information about the error is anonymously reported to Microsoft. For more information about the Privacy Statement for the Microsoft Error Reporting Service, see the [Microsoft Online Crash Analysis](http://go.microsoft.com/fwlink/?LinkId=64250) Web site (http://go.microsoft.com/fwlink/?LinkId=64250). This information is used with error reports from other Microsoft customers to help identify and resolve common issues with Operations Manager 2007.

Note

This setting enables error reporting only for Operations Manager 2007 components. For information about enabling the Client Monitoring feature of Operations Manager 2007, which includes error reporting for the specified computers, see the [Configure Client Monitoring in Operations Manager 2007](#z95a7881bc94f49b099eac2a54cd415f1) section in this guide.

To configure error reporting settings for Operations Manager 2007 components

|  |
| --- |
| 1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 management group.  2. In the Operations console, click the Administration button.  3. In the Administration pane, expand Administration, and then click Settings.  4. In the Settings pane, expand Type: General, right-click Privacy, and then click Properties.  5. In the Global Management Server Settings - Privacy dialog box, click the Error Reporting tab, and then do one of the following:   Select Automatically send error reports about this product to Microsoft without prompting the user.   Select Prompt the user for approval before sending error reports to Microsoft.  Note  Click Tell me more about error reporting if you want to view the Privacy Statement for the Microsoft Error Reporting Service.  6. When you have made the selection you want, click OK. |

Error Transmission settings allow you to specify which error reports are sent to Microsoft and the additional diagnostic data that is included with the error reports.

To find the Error Transmission tab of the Global Management Server Group Settings - Privacy dialog box

|  |
| --- |
| 1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 management group.  2. In the Operations console, click the Administration button.  3. In the Administration pane, expand Administration, and then click Settings.  4. In the Settings pane, expand Type: General, right-click Privacy, and then click Properties.  5. In the Global Management Server Group Settings - Privacy dialog box, click the Error Transmission tab.  Note  Click Read the privacy statement to view the privacy statement. |

To filter errors that are sent to Microsoft

|  |
| --- |
| 1. On the Error Transmission tab of the Global Management Server Group Settings - Privacy dialog box, click Filter.  2. In the Error Forwarding Filters dialog box, select one or more of the options for sources of errors that you do not want forwarded to Microsoft, such as that come from specific computers.  3. In the Criteria description text box, click specific, and provide the values for the criteria of errors that you do not want forwarded to Microsoft, such as computer.contoso.com.  4. Click OK twice. |

To configure diagnostic data sent to Microsoft with error reports

|  |
| --- |
| 1. On the Error Transmission tab of the Global Management Server Group Settings - Privacy dialog box, do one or more of the following:  a. Select Upload diagnostic data collection request, select the additional diagnostic data that you want to send with error reports from computers reporting errors to the management servers, and then forward them from the management server to Microsoft with the error reports.  b. Set Maximum number of CAB files to send to Microsoft per error group to help Microsoft diagnose the error. The recommended number is 10.  c. Select Display links to solutions from Microsoft on error reporting computers. A link to available solutions will display to end users after the error is first encountered and the link to the solution is downloaded to the management server.  d. Select Display links to surveys from Microsoft on error reporting computers.  e. Specify the Default solution link when no Microsoft solution is available. This can be an internal Web page for technical support, for example.  2. Click OK. |

Maintenance and Best Practices for Operations Manager

After you design, deploy, and configure your Microsoft System Center Operations Manager 2007 environment, and as you start monitoring computers and devices in your organization, large amounts of data accumulates.

To protect your Operations Manager environment and to limit service interruption, you must develop and implement a comprehensive and effective maintenance plan. Effective ongoing maintenance of your Operations Manager environment can improve performance and minimize the chances of failure.

Ensure that your maintenance plan includes the following:

 Regular monitoring of both software and hardware.

 Frequent backups of databases and other critical data so that it can be later restored in case of failure.

If at any time there is an indication of a problem, it is best to respond immediately.

In This Section

[Managing Gateway Servers in Operations Manager 2007](#z635fef1bc81f4d39bc06c9daeed11320)

[Managing Reporting in Operations Manager 2007](#z05983540ced54f0faca020e00352ebf6)

[Managing Web Console Servers in Operations Manager 2007](#zc0a64f4a304a47ffabd3b98c546cd1e6)

[Managing Connected Management Groups in Operations Manager 2007](#z1ad80309ac4b447d9aa0421ef542a96e)

[Changing Passwords for Operations Manager Accounts](#z5ffa3865170841f7b78230e4e8df2e58)

[Identifying the Root Management Server in Operations Manager 2007](#zd1091d4b344c44779630bf185ea3a8c3)

[Scheduling Maintenance and Monitoring](#zfa03e49fa8e24614a60d01e76f776a5a)

[Backing Up and Restoring Operations Manager 2007 Components](#z7344ec7a73b747dfa20dee487557a4f1)

[Making Updates to an Operations Manager 2007 Deployment](#zd84eb3d7276c4e9c87dba8c5dd7785a1)

Managing Gateway Servers in Operations Manager 2007

Microsoft System Center Operations Manager 2007 requires mutual authentication be performed between agents and management servers prior to the exchange of information between them. To secure the authentication process between the two, the process is encrypted. When the agent and the management server reside in the same Active Directory domain or in Active Directory domains that have established trust relationships, they make use of Kerberos V5 authentication mechanisms provided by Active Directory. When the agents and management servers do not lie within the same trust boundary, other mechanisms must be used to satisfy the secure mutual authentication requirement.

In Operations Manager 2007, this is accomplished through the use of X.509 certificates issued for each computer. If there are many agent monitored computers, this results in high administrative overhead for managing all those certificates. In addition, if there is a firewall between the agents and management servers as well, multiple authorized endpoints must be defined and maintained in the firewall rules to allow communication between them.

To reduce this administrative overhead, Operations Manager 2007 has a new server role called the gateway server. Gateway servers are located within the trust boundary of the agents and can participate in the mandatory mutual authentication. Because they lie within the same trust boundary as the agents, the Kerberos V5 protocol for Active Directory is used. Each agent then communicates only with the gateway servers that it is aware of. The gateway servers communicate with the management servers.

To support the mandatory secure mutual authentication between the gateway servers and the management servers, certificates must be issued and installed, but only for the gateway and management servers. This reduces the number of certificates required, and in the case of an intervening firewall it also reduces the number of authorized endpoints to be defined in the firewall rules.

As your IT environment or monitoring requirements change, you might need to add or remove gateway servers from an Operations Manager 2007 management group and perform tasks on the gateway servers.

Determining the Health of Gateway Servers

To determine the health of a gateway server, you must examine it from two perspectives. The first, most direct method is to examine the health status in the Operations console and in Health Explorer. This examination will tell you the status of the monitored components, indicate whether or not there are any open alerts, and show you performance data. The second, indirect method is to be sure that data from the agents that are being monitored through the gateway server is being reported in a timely fashion.

Direct Method

Gateway servers are a type of management server, and therefore they are included in the Management Servers container under Device Management in the Administration view of the Operations console. In the details pane of this view, you can immediately see the Health State of any of management servers in the management group. By selecting any gateway server (or any server for that matter) and opening the context menu, you can view the properties of the server or any of the views that are available. Typically, you can directly access the Event View, Alert View, Performance View, Diagram View, and State View for the selected object.

For a more comprehensive understanding of the health of a gateway server, open the Monitoring view and navigate to the Operations Manager, Management Server folder and select the Management Server State view object in the navigation pane. This displays the state of all management servers in the management group, with gateway servers displayed next to the bottom by default. In the Gateway Management Server State pane, select the health status icon for the server you are interested in under the Gateway column to bring up the health state of the gateway servers component monitors in the details pane. Typically, you will get details on the Health Service Availability, Audit Collection Availability, Configuration, Performance, and Security.

Indirect Method

Gateway servers relay monitoring data from agents to collection management servers in the management group across trust boundaries. They also relay configuration information from the collection management server to the agents that they serve. Therefore, if agents that have a gateway server as their primary management server are reporting their data and are showing a heartbeat, you can be sure that their gateway server is performing satisfactorily.

Viewing Agents by Gateway

Use the following procedure to view the primary management server for an agent.

How to view an agent’s primary management server

|  |
| --- |
| 1. Open the Operations console, and then click the Administration button.  2. In the Administration pane, expand Administration, expand Device Management, and then click Agent Managed.  3. Displayed in the results pane are all the agent-managed devices grouped by their Primary Management Server.  4. Look for the gateway server of interest. Grouped under it are all the agents that are currently using the gateway server. |

Using Multiple Gateway Servers

Multiple gateway servers can be deployed across a trust boundary to provide redundant pathways for agents that lie across that trust boundary. Just as agents can fail over between a primary management server and one or more secondary management servers, they can also fail over between gateway servers. In addition, multiple gateway servers can be used to distribute the workload of managing agentless-managed computers and managed network devices.

In addition to providing redundancy through agent-gateway failover, gateway servers can be configured to fail over between collection management servers in a management group if multiple collection management servers are available.

Configuring Agent Failover Between Multiple Gateway Servers

If you have deployed multiple gateway servers into a domain that does not have a trust relationship established with the domain that the rest of the management group is in, you can configure agents to utilize those gateway servers as necessary. To do this, you must use the Operations Manager 2007 command shell.

Use the Set-ManagementServer -AgentManagedComputer command in the command shell as shown in the following example to configure an agent to fail over to multiple gateway servers. The commands can be run from any command shell in the management group.

Important

When changing the primary management server of an agent, allow the agent to connect to its new primary management server before making changes to its failover server. Allowing the agent to get current topology information from the new primary management server prevents the agent from losing communication with all management servers.

To configure agent failover to multiple gateway servers

|  |
| --- |
| 1. Log on to the computer with an account that is a member of the Administrators group.  2. On the Windows desktop, click Start, point to Programs, point to System Center Operations Manager, and then click Command Shell.  3. In the command shell, run the following command:  $primaryMS = Get-ManagementServer | where {your filter here}  $failoverMS = Get-ManagementServer | where {your filter here}  $agent = Get-Agent | where {your filter here}  Set-ManagementServer -AgentManagedComputer: $agent -ManagementServer: $primaryMS  $agent = Get-Agent | where {your filter here}  Set-ManagementServer -AgentManagedComputer: $agent -ManagementServer: $primaryMS -FailoverServer: $failoverMS  In the code example, you need to create a filter statement for the first three commands. The following is an example of a filter command written to find the computer contoso.com that will be assigned to the $failoverMS variable:  $failoverMS = Get-ManagementServer | where {$\_.Name –eq ’contoso.com’ }  Two Set-ManagementServer commands are used to enable the agent to connect to its new primary management server for configuration information before changing the failover server.  For help with the Set-ManagementServer command, type the following in the command shell window:  Get-help Set-ManagementServer -full |

Configure a Gateway Server to Failover Between Multiple Management Servers

Use the Set-ManagementServer-GatewayManagementServer command in the command shell as shown in the following example to configure a gateway server to fail over to multiple management servers. The commands can be run from any command shell in the management group.

To configure gateway server failover to multiple management servers

|  |
| --- |
| 1. Log on to the gateway server with an account that is a member of the Administrators role for the management group.  2. On the Windows desktop, click Start, point to Programs, point to System Center Operations Manager, and then click Command Shell.  3. In the command shell, run the following command:  $primaryMS = Get-ManagementServer | where {your filter here}  $failoverMS = Get-ManagementServer | where {your filter here}  $gatewayMS = Get-ManagementServer | where {your filter here}  Set-ManagementServer -GatewayManagementServer: $gatewayMS -ManagementServer: $primaryMS  $gatewayMS = Get-ManagementServer | where {your filter here}  Set-ManagementServer -GatewayManagementServer: $gatewayMS -ManagementServer: $primaryMS -FailoverServer: $failoverMS  In the code example, you need to create a filter statement for the first three commands. The following is an example of a filter command written to find the computer contoso.com that will be assigned to the $failoverMS variable:  $failoverMS = Get-ManagementServer | where {$\_.Name –eq ’contoso.com’ }  For help with the Set-ManagementServer command, type the following in the command shell window.  Get-help Set-ManagementServer -full |

Managing Certificate Renewal for Gateway Servers and Management Servers

Eventually, the certificates that were obtained and installed on the gateway server and collection management servers will expire and will need to be replaced with new ones. You might also need to replace an existing certificate if, for security reasons, the certificate has been revoked.

To do this, follow the procedures that were used to obtain and import the certificates in the first place. See “Deploying Gateway Servers” in the “Multiple Server, Single Management Group Scenario” section of the [Operations Manager 2007 Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=95133) (http://go.microsoft.com/fwlink/?LinkId=95133). It is not necessary to rerun the Gateway Approval Tool.

Removing a Gateway Server from a Management Group

Throughout the life cycle of your Operations Manager 2007 implementation, you might need to modify the structure and configuration of your deployment. In the case of gateway servers, these types of changes can stem from the decommissioning of an untrusted domain so that monitoring is no longer required or from the old server hardware being replaced with new hardware. To remove a gateway server from service, complete the following steps.

Overview of Decommissioning a Gateway Server

|  |
| --- |
| 1. Configure all objects that are being managed by the gateway server to use a different primary management server. For an agent-managed computer, this means using either another gateway server or a management server.  2. Uninstall the gateway server software from the server.  3. Delete the gateway server from the management group. |

Configure Managed Objects to Use an Alternate Primary Management Server

Gateway servers can manage three different types of objects: agent-managed computers, agentless-managed computers, and network devices acting as a proxy agent.

To configure agent-managed computers to use a different primary management server using the Operations console

|  |
| --- |
| 1. Log on to a management server with an account that is a member of the Administrators role for the Operations Manager 2007 management group.  2. In the Operations console, click the Administration button.  3. In the Administration pane, expand Administration, expand Device Management, and then click Agent Managed.  4. In the Agent Managed pane, select the computers for which you want to change the primary management server, right-click them, and then select Change Primary Management Server.  Note  The Change Primary Management Server option will be unavailable if Active Directory Domain Services was used to assign any of the selected computers to the management group.  5. In the Change Management Server dialog box, select the new management server from the list, and then click OK. The change takes effect on the agent after its next update interval. |

Alternatively, this configuration can be changed on the agent-managed computer itself using either of the following two procedures.

To change the primary management server for agent-managed computers by using the MOMAgent.msi setup wizard

|  |
| --- |
| 1. Log on to the agent-managed computer with an account that is a member of the Administrators security group for the computer.  2. In Add or Remove Programs, click Change for System Center Operations Manager 2007 Agent.  Note  The Agent Setup Wizard can also be run by double-clicking MOMAgent.msi, which is located on the Operations Manager 2007 installation media.  3. In the Agent Setup Wizard, click Next.  4. On the Program Maintenance page, select Modify, and then click Next.  5. On the Management Group Configuration page, leave Specify Management Group information selected, and then click Next.  6. In the next Management Group Configuration page, do the following:  a. Type the name of the Management Server.  b. Type in a value for Management Server Port, or leave the default 5723.  c. Click Next.  7. On the Ready to Install page, review the settings, and then click Install to display the Installing System Center Operations Manager Agent page.  8. When the Completing the System Center Operations Manager Agent Setup Wizard page displays, click Finish. |

To change the primary management server for agent-managed computers using MOMAgent.msi from the command line

|  |
| --- |
| 1. Log on to the agent-managed computer with an account that is a member of the Administrators security group for the computer.  2. Open the command window.  3. At the prompt, run the following command:  %WinDir%\System32\msiexec.exe /i \\path\Directory\MOMAgent.msi /qn USE\_SETTINGS\_FROM\_AD=0 MANAGEMENT\_GROUP=MG1 MANAGEMENT\_SERVER\_DNS=MS2.Domain1.net  This command reconfigures the agent to use MS2.Domain1.net as its primary management server for management group MG1.  Note  Microsoft Windows Installer public properties must be uppercase, such as PROPERTY=value. For more information about Windows Installer, see [Windows Installer](http://go.microsoft.com/fwlink/?LinkId=70004) in the Microsoft Developer Network library (http://go.microsoft.com/fwlink/?LinkId=70004).  If the Domain Name System (DNS) and Active Directory names for the management server differ, the MANAGEMENT\_SERVER\_AD\_NAME property also needs to be set to the fully qualified Active Directory Domain Services name. |

Redirecting Agentless-Managed Computers and Network Devices

To change the proxy agent for agentless-managed computers and network devices

|  |
| --- |
| 1. Log on to a management server computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 management group.  2. In the Operations console, click the Administration button.  3. In the Administration pane, expand Administration, expand Device Management, and then click Agentless Managed. If you are working with a network device, select Device Management and then Network Devices.  4. In the Agentless Managed pane, select the agentless-managed computers for which you want to change the proxy agent, right-click them, and then select Change Proxy Agent. Or if you are working with a network device, in the Network Devices pane, select the network devices for which you want to change the proxy agent, right-click them, and then select Change Proxy Agent.  5. In the Change Proxy Agent dialog box, select the computer you want to be the new proxy agent, and then click OK. |

The final steps in removing a gateway server from a management group are straightforward:

 Log on to the gateway server with an account that has administrative rights.

 In Add or Remove Programs, select System Center Operations Manager 2007 Gateway, and then click Remove.

In the Operations console, in the Administration view, under Device Management, Management Servers, select the gateway server, right-click it, and then click Delete.

Managing Reporting in Operations Manager 2007

The Reporting feature of Microsoft System Center Operations Manager 2007 focuses on customer scenarios, performance, and usability. As an administrator, you will be involved in setting up access to reports and maintaining the SQL database. For information about how to create, customize, and use reports, see the [Creating Reports](http://go.microsoft.com/fwlink/?LinkId=150369) topic in the Operations Manager 2007 R2 User’s Guide (http://go.microsoft.com/fwlink/?LinkId=150369).

Managing Access to Reports

Operations Manager 2007 uses role-based security. With regard to administering Operations Manager 2007, you will need to manage users as needed. The following roles are relevant to reporting:

 Report Operator

Includes a set of privileges designed for users who need access to reports. This role grants members the ability to view reports according to their configured scope.

Caution

Users assigned to this role have access to all report data in the Reporting data warehouse and are not limited by scope.

 Report Security Administrator

Enables the integration of SQL Server Reporting Services security with Operations Manager user roles. This gives Operations Manager Administrators the ability to control access to reports. This role can have only one member account and cannot be scoped.

Use the procedures in this topic to restrict access to Operations Manager 2007 reports containing sensitive information.

First, using a Command Shell script, you create a new user role. An example of a Command Shell script that is used to create a new user role is shown at the end of this topic.

Second, you use the Get-UserRole command to set permissions on the report.

Caution

After you edit the security properties for a report, folder inheritance for every report in the folder is disabled. When folder inheritance is lost, you are required to manually set permissions for every report in the folder by using the Get-UserRole command.

For more information about the Operations Manager Command Shell, see the [Operations Manager 2007 SDK](http://go.microsoft.com/fwlink/?LinkId=65912) (http://go.microsoft.com/fwlink/?LinkId=65912).

To create a new user role

|  |
| --- |
| 1. Copy the sample Command Shell script to your local hard drive and save the file with a .ps1 extension (for example ReportOperator.ps1).  2. Start the Operations Manager Command Shell.  3. Run the script, for example type C:\ReportOperator.ps1, and then press ENTER.  4. In the Operations console, click Administration.  5. In the Administration pane, expand Administration, expand Security, and then click User Roles.  6. In the User Roles pane, right-click the user role that was previously created from the Command Shell script, and then click Properties.  7. In the User Role Properties dialog box, click the General page, and then click Add.  8. On the Select User or Groups page, enter the users or groups that you want to assign to the user role, and then click OK.  Important  Adding a machine account to user role member would allow all services on that computer to have SDK access. It is recommended that you do not add a machine account to any user role.  9. Click Apply, and then click OK.  10. Now you need to add the GUID for the new user role to SQL Server Reporting Services. Use the following steps:  a. In the User Roles view, double-click the new user role.  b. Click the Identity tab.  c. Click Copy to copy the GUID for the new user, and then click OK to close the Properties window.  d. Start the SQL Server Reporting Services Report Manager by navigating to http://localhost/Reports in a Web browser.  e. Click the Properties tab.  f. Click New Role Assignment.  g. Paste the GUID in the Group or user name field.  h. Select the roles you want to assign to the new Report Operator user role and click OK. |

To set permissions on a report using command shell

|  |
| --- |
| 1. Use the Get-UserRole command to find the particular user role that you want to use for the report.  Note  The command get-userrole | format-list Name,ID | ft displays an easy-to-read table that displays user role names and their associated GUID.  2. Copy the GUID to the clipboard.  3. Access the report by using your browser and connecting to the instance of SQL Server (http://<computername>/reports$instance1).  4. On the SQL Server Reporting Services home page, click the folder containing your report (for example, click Reports, and then click Microsoft.SystemCenter.DataWarehouse.Report.Library).  5. Click the Properties tab, and then in the navigation pane, click Security.  6. Click Edit Item Security.  7. Click the check box for the role Browser, My Reports, Report Builder, and replace the existing GUID with the GUID for the User Role you selected and copied onto the clipboard. |

The following is an example of the code you can use to create a user role for the Report Operator profile. The new user role in this example is named "Test Report Operator Role" but can be changed before running the script.

$mg = (get-item .).ManagementGroup

$reportOperator = $mg.GetMonitoringProfiles() | where {$\_.Name -eq "ReportOperator"}

$obj = new-object Microsoft.EnterpriseManagement.Monitoring.Security.MonitoringUserRole

$obj.Name = "TestReportOperatorRole"

$obj.DisplayName = "Test Report Operator Role"

$obj.Description = "Test Report Operator Role"

$obj.MonitoringProfile = $reportOperator

$mg.InsertMonitoringUserRole($obj)

Grooming

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

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

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

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

To change grooming settings in the Reporting data warehouse

|  |
| --- |
| 1. On the Windows desktop, click Start, point to Programs, point to Microsoft SQL Server 2005 or Microsoft SQL Server 2008, and then click SQL Server Management Studio.  2. In the Connect to Server dialog box, in the Server Type list, select Database Engine; in the Server Name list, select the server and instance for your Reporting data warehouse (for example, computer\INSTANCE1); in Authentication list, select Windows Authentication; and then click Connect.  3. In the Object Explorer pane, expand Databases, expand OperationsManagerDW, and then expand Tables.  4. Right-click dbo.Dataset, and then click Open Table.  5. Locate the dataset for which you want to change the grooming setting in the DatasetDefaultName column and make note of its GUID in the DatasetId column.  6. In the Object Explorer pane, right-click dbo.StandardDatasetAggregation and then click Open Table.  7. In the DatasetId column, locate the dataset GUID you noted in step 5. Multiple entries of the same GUID might display.  8. Locate the aggregation type from the list in the AggregationTypeId column by using the following values:   0 = raw, nonaggregated data   10 = subhourly   20 = hourly   30 = daily  After you have located the dataset and its aggregation type, scroll to the MaxDataAgeDays column, and then edit the value there to set the grooming interval. |

Managing Web Console Servers in Operations Manager 2007

The Web console server provides a browser-based alternative to the Monitoring pane of the Microsoft System Center Operations Manager 2007 Operations console. The Web console server is commonly used when you want to access Operations Manager 2007 management group monitoring data in the following ways:

 From the Internet.

 Without installing the Operations console.

 From a location with low-bandwidth connectivity.

 When notifications are configured to contain hyperlinks to the relevant alerts in the Web console.

As your IT environment or monitoring requirements change, you might need to add or remove Web console servers from an Operations Manager 2007 management group or perform tasks on a Web console server. For information about designing your Operations Manager 2007 management group, see the [Operations Manager 2007 Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=91462) (http://go.microsoft.com/fwlink/?LinkId=91462).

Add a Web Console Server to a Management Group

Add a Web console server to an Operations Manager 2007 management group to provide Web-based access to monitoring data. For information about deploying a Web console server, see the “How to Deploy an Operations Manager 2007 Web Console Server Using the Setup Wizard” topic in the Operations Manager 2007 R2 Help.

Configure Web Console to Fail Over

You can manually configure the Web console to fail over to another root management server (RMS).

To configure the Web console to fail over

|  |
| --- |
| 1. Using Notepad, open the file Web.Config. The default location for this file is C:\Program Files\System Center Operations Manager 2007\Web Console.  Note  You can use any editor that saves in plain text.  2. Change the following line to include the new remote management server:  <add key="MOMServer" value="<provide new RMS server name>" />  3. Save your changes. |

Change the Authentication Used by a Web Console Server

A Web console server is configured at installation to use either Windows or forms-based authentication. To change the authentication used by a Web console server, you must uninstall the Web console server and reinstall it. Use Add or Remove to modify the installation of System Center Operations Manager 2007 and remove the Web console feature. For information about designing your Operations Manager 2007 management group, see the [Operations Manager 2007 Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=91462) (http://go.microsoft.com/fwlink/?LinkId=91462).

Enable Secure Sockets Layer on a Web Console Server

Configure a Web console server that uses forms-based authentication to use Secure Sockets Layer (SSL) for a more secure Web console experience. For information about configuring the Web console server to use SSL, see the “How to Deploy an Operations Manager 2007 Web Console Server Using the Setup Wizard: topic in the Operations Manager 2007 R2 Help.

Update the Certificate on Web Console Servers

Certificates expire, or there can be a security breach involving the certificate used for SSL connections to the Web console server. In both of these cases, you need to apply a new certificate to help maintain uninterrupted secure availability of the Web console server. For information about applying certificates to the Web console server, see the “How to Deploy an Operations Manager 2007 Web Console Server Using the Setup Wizard: topic in the Operations Manager 2007 R2 Help.

Remove a Web Console Server from a Management Group

You might want to remove a Web console server from an Operations Manager 2007 management group for reasons such as hardware consolidation. Use Add or Remove to modify the installation of System Center Operations Manager 2007 and remove the Web console feature.

Managing Connected Management Groups in Operations Manager 2007

Connected management groups enable the consolidation of alerts and the running of tasks from multiple management groups. Tasks can be initiated from a local management group to run on managed objects of a connected management group. This scenario is used to scale up the number of managed computers or objects you can monitor beyond the capabilities of a single management group.

The management group in which the data is consolidated is called the local management group, and those that contribute their data to the local management group are called the connected management groups. They relate to each other in a hierarchical fashion, with connected groups reporting up to local groups. The connected groups are in a peer-to-peer relationship with each other. Each connected group has no visibility or interaction with the other connected groups; the visibility is strictly from the local management group to the connected management group.

Communications between the connected and local management groups occur between the root management servers over TCP port 5724.

To Connect Operations Manager Management Groups

Use the following procedure to connect two management groups.

To connect Operations Manager management groups

|  |
| --- |
| 1. Log on to the computer with a user account that is a member of the Operations Manager Administrator role for the Operations Manager 2007 management group.  2. In the Operations console, click the Administration button.  3. In the Administration pane, expand Administration, right-click Connected Management Groups, and then click Add Management Group.  4. Type the name for the connected management group in the Management Group name text box.  5. In the Root Management Server text box, type the name of the root management server in the connected management group.  Note  You must define the root management server by its fully qualified domain name (FQDN).  6. Select one of the following radio buttons:  Note  In either case, the account you use must be a member of the Operations Manager 2007 Administrators role for the connected management group.   Select Use SDK service account if the SDK Service account is the same account in both management groups.   Select Other user account if different credentials were used for the SDK service account in each management group, and then enter the credentials for the SDK service account used in the connected management group.  7. Click Add. |

To Configure User Roles for Connected Management Groups

If you are attempting to view one or more connected management groups, the credentials you provide must be those of a member of a user role in each of the connected management groups. The scope defined for this user role defines the scope of alerts that can be viewed.

Note

The Show Connected Alerts button will not be displayed to a user if the user is a member of a user role that is scoped for All Groups.

For example, consider an environment where two management groups are needed to monitor a large number of computers running Microsoft SQL Server. Both management groups have been connected. Tom has the responsibility of monitoring computers that are running SQL Server. The Operations Manager administrator wants Tom to be able to view alerts from both management groups in a single view. The Operations Manager administrators in both connected management groups assign Tom's account to a SQL Server Operator user role. When Tom clicks Show Connected Alerts, only SQL Server-related alerts from both management groups are displayed.

On the local management group, Tom needs to be a member of a user role whose group scope includes the connected management groups. Connected management groups are listed as object groups in the Group Scope tab in the User Role Properties dialog box. Only connected management groups that are selected can be viewed. For more information about user roles, see the [Operations Manager 2007 Security Guide](http://go.microsoft.com/fwlink/?LinkId=64017) (http://go.microsoft.com/fwlink/?LinkId=64017).

To View Alerts from Connected Management Groups

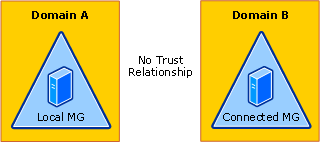
Every time you start the Operations console, only alerts from the local management group are displayed. To view alerts from the connected management group, you need to provide credentials for a user from the connected management group.

To view alerts from the connected Management Group

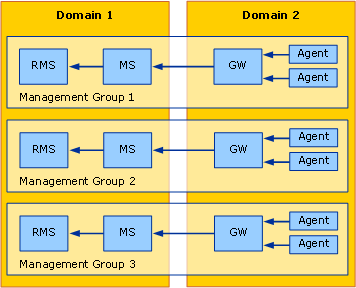
|  |
| --- |
| 1. Start the Operations console, and click the Monitoring button.  2. In the Monitoring pane, expand Monitoring, and then click Active Alerts.  3. In the Active Alerts pane, in the toolbar, click Show Connected Alerts.  4. In the Enter Credentials dialog box, type the user name, password, and domain name of a user in the connected management group.  Note  The credentials entered must be from a user in the connected management groups that is a member of a role in Operations Manager. The scope of alerts that can be viewed is determined by the scope of the user's credentials.  5. Click OK. |

Connecting Management Groups Across Untrusted Domains

There are two topologies available for connecting management groups that span untrusted domains. If only one connected management group is going to be connected to one local management group, the two management groups themselves can exist entirely within their respective domains as shown in the following figure.



If there are more than three management groups that are going to be connected, one local management group and two or more connected management groups, then both the local and connected management groups must span the two domains as shown in the following illustration.



In this example, the same rules for user roles still apply as described in the “To Configure User Roles for Connected Management Groups” topic in this document.

Managing Audit Collection Services in Operations Manager 2007

This topic explains how to configure, use, and maintain an Audit Collection Services (ACS) implementation in your environment. This includes ACS Reporting and how to configure auditing of objects and folders. Auditing for applications, objects and folders is accomplished through group policy at the domain and local level. It does not cover ACS planning and deployment tasks. For planning and deployment guidance, see the Operations Manager 2007 Deployment Guide. This topic presumes a deployed and functioning ACS infrastructure.

Configuring and using ACS consists of the following steps:

1. Planning and implementing your audit policy

2. Setting the filter on the ACS Collector

3. Configuring and using ACS reporting

4. Maintenance

Developing an Audit Plan

ACS collects and stores all the security event log entries from computers on which it is enabled. It does so with no regard to what those events are or what they mean. It is up to you to determine what events you need captured and stored to fulfill your organization’s auditing requirements. The process of determining what those requirements are and how they translate into something that is actionable is called developing an audit plan. From the audit plan, you implement an audit policy via Group Policy objects at the domain or local level. It is the configuration of Group Policy objects that tells the security subsystem to write events to the security event log when a particular event or change occurs on a computer or in your environment. This process creates the trail of audited events that ACS collects.

Determine What Needs to be Audited

Companies are implementing ACS in response to various legal and regulatory requirements and for their own security, so you will not be able to determine by yourself what needs to be audited. You need to involve individuals from several different areas of your company to develop an effective audit plan.

 IT Security—This team includes people who are responsible for responding to security incidents in your company and for developing the IT security policy. They should already have a good idea of the types of events and changes that need to be captured to satisfy the legal and regulatory needs of your company.

 Management and Legal—These individuals are responsible for ensuring your company is in compliance with regulatory policies. They likely have a deep understanding of those policies and can help clarify the type of information that they need.

 Business Process Owners—The business process owners will have the best understanding of the types of activities and events that occur in the applications that they use to run their business. These events and activities are then matched to the requirements from the legal and management areas. You need to understand these events and activities and where they occur to be able to audit them.

In general, it is not effective or efficient to audit all activity and changes and to capture all events. This approach results in gathering a great deal of noise events, which can obscure the data that is really needed when reconstructing a series of events, thereby impeding the overall process.

Audit Best Practices

Each company’s business requirements and IT environments are unique. As such, each company’s audit policy is also unique. What you choose to audit is up to you. Here are some general recommendations on what to audit:

 Audit success and failure events in the system event category.

 Audit success events in the policy change event category on domain controllers.

 Audit success events in the account management category.

 Audit success events in the logon event category.

 Audit success events in the account logon event category on domain controllers.

 Be specific when setting up auditing on an object.

For additional suggestions related to auditing security events, see [Auditing Security Events Best practices](http://go.microsoft.com/fwlink/?LinkId=120541) (http://go.microsoft.com/fwlink/?LinkId=120541).

Implementing Your Audit Policy

Audit plans are implemented in your environment through the modification and application of the Domain Controller Audit Group Policy, Domain Audit Group Policy, and local Audit Group Policy as needed. If your auditing plan calls for tracking interactions with Active Directory or with objects such as files, you will also need to configure the System Access Control List (SACL) on those objects. For in-depth information about Auditing and Windows security, see [Windows Server 2003 Product Help Auditing Policy](http://go.microsoft.com/fwlink/?LinkId=120260) (http://go.microsoft.com/fwlink/?LinkId=120260) and [Special Coverage: Windows Server 2008: Auditing and Compliance in Windows Server 2008](http://go.microsoft.com/fwlink/?LinkId=120263) (http://go.microsoft.com/fwlink/?LinkId=120263).

Audit policy settings are found in the Local Security settings in the Administrative tools folder. Audit policies for domain controllers are defined once and applied to all domain controllers. This is done via the Domain Controller Security Policy tool in the Administrative Tools folder. Audit policy for the rest of the domain member computers can be defined at the domain level in the Domain Security Policy tool, which is located in the Administrative Tools folder on all domain controllers. There are nine common audit policy categories for Windows Server 2003 and Windows Vista, as shown in the following list, and a few more for Windows Server 2008:

 Audit account logon events

 Audit account management

 Audit directory service access

 Audit logon events

 Audit object access

 Audit policy change

 Audit privilege use

 Audit process tracking

 Audit system events

On a member server, each of these audit policy categories can be set to Success, Failure, or No auditing. On a domain controller, in both the domain controller security policies and domain security policies, the options are to Define these policy settings, Success, Failure, or No auditing. In this case, the value of No auditing indicates that the Define these policy settings option has been selected, but that neither success nor failure options have been selected. Note that the Success and Failure options are not mutually exclusive, both can be selected. For the audit directory service access and audit object access audit policy categories, you must also configure the SACLs for the objects you want audited.

To access the Audit Policy categories on a standalone server

|  |
| --- |
| 1. Click Start, and select Administrative Tools, Local Security Policy.  2. Expand the Local Policies node to expose the Audit Policy node. The nine audit policy categories are listed in the results pane.  3. Double-click the audit policy that you are interested in to open its property page. Here you can select to audit success and failure attempts at interaction, as well as get an explanation of the audit policy category on the Explain This Setting tab.  4. Click OK to save your settings. |

To access the Domain Controller Security Policy

|  |
| --- |
| 1. Log on to a domain controller with domain administrator rights.  2. Click Start, and select Administrative Tools, Domain Controller Security Policy.  3. Expand the Local Policies node to expose the Audit Policy node. The nine audit policy categories are listed in the results pane.  4. Double-click the audit policy that you are interested in to open its property page. Here you can select to Define these policy settings and then select to audit Success and/or Failure attempts as desired. |

Note

To access the domain security policy, follow the same procedure as accessing the domain controller security policy except select Domain Security Policy in step 2 of the “To access the Domain Controller Security Policy” procedure.

Preparing the Environment

This topic presumes that you have already successfully deployed the ACS collector server role and database in your Operations Manager 2007 environment. In addition to this, you should have already deployed Operations Manager 2007 agents to the computers that you will be collecting auditing information from. These computers should appear under the Agent Managed folder in the Operations Manager 2007 Operations console Administration view.

Security Event Log Sizing

The ACS forwarder sends all security events from a monitored computer to the ACS collector server in near real time. As it does so, it updates a watermark that indicates which event was last successfully sent to the ACS collector. The ACS collector server buffers the incoming events for performance and reliability. If the ACS forwarder cannot communicate with the ACS collector, security events will not be lost to ACS as long as they can be written to the security event log. Then, when communications are restored, the ACS forwarder consults the watermark and picks up sending events where it left off. In effect, the security event log is the buffer that the ACS forwarder can use if needed.

For the security event log buffering process to work, the log must be of sufficient size to accommodate all the events that could be written to it in the case of a forwarder-to-collector communication failure. This is true regardless of which of the following security log retention methods is used: Overwrite events by days, Overwrite events as needed, or Do not overwrite events (clear log manually).

The maximum size for the security event log in Windows Server 2003 (any edition) is 4 GB. This can be set locally in the properties of the log itself, or it can be set at the domain level for domain-joined computers in the Domain Security Policy and for all domain controllers in the Domain Controller Security Policy.

Enabling ACS Forwarders

Now that you have developed your audit plan and implemented it via an audit policy, you can begin collecting audited events from the security logs of the desired computers. The ACS forwarder component is embedded in the Operations Manager agent and is disabled by default. After it is enabled, the ACS forwarder will send all security event log events to the ACS collector they are configured to send to. ACS forwarders can be enabled either through the Operations console or programmatically by using the Operations Manager 2007 command shell extension to the Windows PowerShell.

To enable the ACS forwarder via the Operations console

|  |
| --- |
| 1. Log on to the Operations console with an account that is scoped to manage the agents that you want to enable ACS forwarding on. This account does not need to have local administrator rights on each agent computer that you want to enable as an ACS forwarder. You can provide these credentials when you run the Enable Audit Collection task.  2. In the Operations console, click the Monitoring button.  3. In the Monitoring pane, expand Operations Manager, expand Agent, and then click Agent Health State. This view has two panes, and the actions in this procedure are performed in the pane on the right side.  4. In the details pane, click all agents that you want to enable as ACS forwarders. You can make multiple selections by pressing CTRL or SHIFT.  5. In the Actions pane, under Health Service Tasks, click Enable Audit Collection. The Run Task - Enable Audit Collection dialog box displays.  6. In the Task Parameters section, click Override. The Override Task Parameters dialog box displays.  7. In the Override the task parameters with the new values section, click the CollectorServer parameter; in the New Value column, type the fully qualified domain name (FQDN) of the ACS collector and then click Override.  8. In the Task credentials section, click Other. In the User Name box, type the name of a user account that belongs to the local Administrators group on the agent computers. In the Password box, type the password for this user account. Click to expand the Domain drop-down list to view the available domains, and then click the domain of the user account.  9. Click Run Task. The Task Status dialog box displays, tracking the progress of the task.  10. When the task completes successfully, click Close. |

Note

If you need to change which ACS collector that an ACS forwarder is assigned to, use this same procedure except in the Override the task parameters with the new values field you need to type the FQDN of the new, desired ACS collector.

On the product CD, Windows PowerShell scripts have been included for enabling and disabling the ACS forwarder. These scripts require a set of credentials that have administrator rights on every machine for which you want to enable ACS and the name of the ACS collector server. These scripts are located on the product CD under \acs\amd64 or acs\i386. They are called EnableForwarding.ps1 for enabling ACS forwarders and DisableForwarding.ps1 for disabling ACS forwarders.

To target enabled ACS forwarders for a computer group

|  |
| --- |
| 1. Log on to the Operations console with an account that is in the Administrator role, and navigate to the Monitoring view.  2. In the Monitoring view, select the Discovered Inventory object, and in the Actions pane select Change target type….  3. Ensure that the View all targets option is selected, and in the Target column, select Computer Group. Doing this lists all the discovered computer groups in your management group.  4. Select the computer group that you want to enable the ACS forwarder for, and right-click to open the context menu.  5. From the context menu, select Open and Command Shell…. This sets the focus of the command shell window to the selected computer group. If you want to see specifically which computers are included in the selected group, type dir for a listing.  6. At the command shell command prompt, type the full path to the script you want to use, followed by the name of the server that the ACS collector is installed on—for example: d:\selectcdimage\acs\i386\enableforwarding.ps1 ContosoACSCollector. You will be prompted for credentials that have administrative rights on all the computers that are agent monitored in the management group in which you are working. You must provide these credentials in domain\username format. |

Note

If you need to change which ACS collector that an ACS forwarder is assigned to, use this same procedure except type d:\selectcdimage\acs\i386\enableforwarding.ps1 <NameOfDesiredCollectorContosoACSCollector>.

Setting the Collector-Side Filter

The first step in implementing ACS was to make sure that the events you want get written to the security event logs on the desired computers. All of these events plus all the events that are written to the security event log by default are sent to the ACS collector. This can result in a very large volume of events being sent to the collector, which processes them and inserts them into the ACS database.

To reduce the volume of data being sent and to help eliminate noise events, you can configure a filter on the ACS collector. The filter is formatted as a Windows Management Instrumentation Query Language (WQL) query. The default filter is select \* from AdtsEvent, which means accept all incoming events. The filter is controlled through the AdtAdmin command-line utility. The filter that can be defined is exclusive in nature only. This means you can configure the filter only to exclude events based on eventid or service name.

The AdtAdmin utility is found in the \Program Files\System Center Operations Manager 2007\acs\<platform> folder. For a full listing of AdtAdmin parameters and options, see the Operations Manager 2007 online help. AdtAdmin has 12 parameters in total. Only two of these switches are relevant to setting the collector site filter, as described in the following list. For a complete listing of the AdtAdmin switches, run the AdtAdmin command with the /? switch.

|  |  |
| --- | --- |
| parameter | description |
| -getquery | Displays the WQL queries that are active on an ACS collector |
| -setquery | Configures the WQL query that the ACS collector uses to filter audit event data |

To Determine What Events to Filter Out

When you developed your audit plan and implemented your audit policy, you defined the events that you needed to capture and save. All events except those are noise events and can be filtered out. Although you make the final determination about what noise events are and what valuable events are, a list of suggested noise events can be found in Appendix A of the  [Security Monitoring and Attack Detection Planning Guide](http://go.microsoft.com/fwlink/?LinkId=120864) (http://go.microsoft.com/fwlink/?LinkId=120864). This list gives you a good place to start your filtering planning from, and it provides descriptions of the events. In addition to this list, you should consult the Planning\_-\_Event\_Counts report under the Audit Reports folder in the Reporting view of the Operations console. This report groups all the audit events that have been received by event ID. It includes the number of events by ID and what percentage of the total number of events any single event type is. After you start collecting events and you know what each event type means, you can use this report to help you identify the most frequently occurring noise events.

Warning

There is some risk in excluding any information from an audit, but you must evaluate the magnitude of that risk against the cost in both performance and hardware that results from increased event collection load and agent load.

How to Set the Filter

You use the AdtAdmin –setquery command to set the query for the filter. This command has two subparameters, –collector, and –query, that must be used to specify which collector to connect to and to specify the syntax of the query, respectively.

To configure the ACS collector filter using AdtAdmin-setquery

|  |
| --- |
| 1. Log on to the ACS collector server on which you want to configure the filter with an account that is a member of the Operations Manager 2007 Administrator role.  2. Open a command prompt, and navigate to the \Program Files\System Center Operations Manager 2007\acs\<platform directory.  3. Type the command following this syntax: adtadmin –setquery –collector:<collectorname> -query:<querysyntax> |

For example, the following query filters out events generated by System, Local Service, and Network Service services, and it also filters events that have specified event ID numbers:

adtadmin -setquery -collector:"Collector Name" /query:"SELECT \* FROM AdtsEvent WHERE NOT ((HeaderUser='SYSTEM' OR HeaderUser='LOCAL SERVICE' OR HeaderUser='NETWORK SERVICE') OR (EventId=538 OR EventId=566 OR EventId=672 OR EventId=680 OR (EventId>=541 AND EventId<=547)))"

To verify the filter is valid

|  |
| --- |
| 1. Open the Operations console, and open the Microsoft Audit Collection Services folder in the Monitoring view.  2. Open the Collector folder, open the State View, and confirm that the collector is in a healthy state.  3. If the collector is not in a healthy state, look in the collector’s Event View for event OpppsMgr log\ADtServer 4670 The collector was unable to start because it was unable to initialize the WMI provider. |

For more information about the WQL query syntax, see [Querying with WQL](http://go.microsoft.com/fwlink/?LinkId=74151) (http://go.microsoft.com/fwlink/?LinkId=74151) and [WMI and SQL](http://go.microsoft.com/fwlink/?LinkID=120966) (http://go.microsoft.com/fwlink/?LinkID=120966).

ACS Reporting

After auditing data is received by the ACS collector and the inbound events are filtered, the events are processed to combine common fields and remove extraneous data and then they are inserted into the ACS database. By default, ACS data is kept in the database for 14 days, though this can be modified. Operations Manager makes this data visible and consumable through its reporting feature. There is a set of report definition files specifically for ACS data that must be installed to be able to access the ACS data. This procedure presumes that you have already installed ACS reporting. For more information about installing ACS reports, see  [Deploying Operations Manager 2007 ACS Reporting](http://go.microsoft.com/fwlink/?LinkId=120983) (http://go.microsoft.com/fwlink/?LinkId=120983).

ACS reports are accessible in the Reporting view of the Operations console. They are in the Audit Reports folder under the Reporting folder. ACS reporting installs 18 reports and two audit report templates. The audit report templates are used when you want to create an entirely new audit report in Microsoft SQL Server Report Builder. Report Builder is accessed by clicking the Design a new report link in the Actions pane. Here is the list of reports:

 Access\_Violation\_-\_Unsuccessful \_Logon\_Attempts

 Account\_Management\_-\_Domain\_and\_Built-in\_Administrators\_Changes

 Account\_Management\_-\_Passwords\_Change\_Attempts\_by\_Non-owner

 Account\_Managment\_-\_User\_Accounts\_Created

 Account\_Management\_-\_User\_Accounts\_Deleted

 Forensic\_-\_All\_Events\_For\_Specified\_Computer

 Forensic\_-\_All\_Events\_For\_Specified\_User

 Forensic\_-\_All\_Events\_With\_Specified\_Event\_ID

 Planning\_-\_Event\_Counts

 Planning\_-\_Event\_Counts\_By\_Computer

 Planning\_-\_Hourly\_Event\_Distribution

 Planning\_-\_Logon\_Counts\_of\_Privileged\_Users

 System\_Integrity\_-\_Audit\_Failure

 System\_Integrity\_-\_Audit\_Log\_Cleared

 Usage\_-\_Object\_Access

 Usage\_-\_Privileged\_Logon

 Usage\_-\_Sensitive\_Security\_Groups\_Changes

 Usage\_-\_User\_Logon

 Audit\_Report\_Template

 Audit5\_Report\_Template

Working with Reports

In the Reporting view, there are four folders:

 Reporting—This folder contains all reports that have been published to the SQL Server Reporting Services (SSRS) site. This includes all reports that are imported as components of management packs, reports that are designed and saved using the Report Builder tool, and any reports that you customize, save, and publish so that they are publicly available.

 Authored Reports—This folder contains reports that you have modified from the Reporting folder and published to the SSRS site. By default, these reports are not viewable to the public, only to the publisher of the report. This is true when the report is accessed via the Operations console or the SSRS Web site, where it will appear in the My Reports folder.

 Favorites—This folder is for reports that you use frequently and that you want to be available in the Operations Manager Web console. You can preset parameters for a published report, run the report, and then from the reports’ File menu, select Save to favorites… .

 Scheduled Reports—This folder is for reports that you want to run on a one-time or recurring basis. Scheduling reports is useful for delivering rendered reports to a variety of locations, such as file shares, or to an e-mail address in a variety of formats, such as Microsoft Office Excel, .PDF, TIFF, CSV, and so forth.

For more information about running, publishing, and working with reports, see [Managing Reporting in Operations Manager 2007](#z05983540ced54f0faca020e00352ebf6) in this guide and the [Reporting in Operations Manager 2007 topic in the Operations Users guide](http://go.microsoft.com/fwlink/?LinkId=156056) (

Tip

ACS reporting has not been fully integrated with Operations Manager Reporting yet; therefore, use of functions such as scheduling and relative dates in the generation of ACS reports might not give the desired results.

Maintenance

The day-to-day care and feeding of your ACS infrastructure is minimal. Most commonly, you might need to change the data-retention period that you configured during setup and change which collector a forwarder works with. For more information about how to change the ACS collector that an ACS forwarder is reporting to, see the [Enabling ACS Forwarders](#z4) section earlier in this topic.

Changing the ACS Data-Retention Period

Operations Manager grooms, or removes, data from its various databases at regular configurable intervals. For the Operations database, this is done in the Operations console. For the ACS database, these settings are configured during setup with a default value of 14 days. This means that every day, all database partitions (and their data) that are older than 14 days are dropped or deleted. Because of the volume of data that ACS can accumulate, 14 days is not an unreasonable setting. However, some companies might need to retain data for longer periods and they must have already planned for that when making the sizing and performance calculations for their environment. You can change the retention period for the ACS data by following this procedure.

To change the ACS data-retention period

|  |
| --- |
| 1. Log on to the computer running SQL Server that hosts the ACS database with an account that has administrative rights to the ACS database.  2. Open the SQL Server Management Studio tool, and connect to the database engine.  3. Expand the Databases folder, and select the OperationsManagerAC database.  4. Right-click to open the context menu and select New Query….  5. In the Query pane, type the following, where number of days to retain data + 1 equals the number of days you want to pass before data that has aged past that point is deleted. For example, if you want to retain data for 30 days, type 31  USE OperationsManagerAC UPDATE dtConfig SET Value = <number of days to retain data + 1> WHERE Id = 6 and then click the Execute button on the toolbar. This runs the query and then opens the Messages pane, which should read (1 row(s) affected).  6. To view the new setting, delete the previous query text from the Query pane and type SELECT \* FROM dtConfig. This opens the Results pane below the Query pane.  7. Look at the value in the sixth row; it should now equal the value you entered for <number of days to retain data + 1>.  8. Restart the Operations Manager Audit Collection Service for this to take effect. |

Using the Operations Manager Command Shell

The Microsoft System Center Operations Manager 2007 command shell is installed with the Operations Manager console; it provides a command-line environment and task-based scripting technology that you can use to automate most Operations Manager administrative tasks.

How the Operations Manager Command Shell Works

The Operations Manager command shell is built on Windows PowerShell. The Operations Manager command shell extends the Windows command shell with over 80 additional small utility programs, called cmdlets, which can either be run directly from the command shell prompt or called from within a batch file or script. Cmdlets can be used by themselves, or they can be combined with other cmdlets to perform complex administrative tasks. Unlike traditional command-line environments that work by returning text results to the end user or routing (“piping”) text to different command-line utilities, PowerShell manipulates Microsoft .NET Framework objects directly. This provides a more robust and efficient mechanism for interacting with the system.

This topic serves as an overview to the Operations Manager command shell. To learn more about PowerShell, see the [Windows PowerShell 1.0 Documentation Pack](http://go.microsoft.com/fwlink/?LinkID=128867) (http://go.microsoft.com/fwlink/?LinkID=128867).

Using the Operations Manager Command Shell

In this section, we will walk through some common tasks with the Operations Manager 2007 command shell.

Launch the Operations Manager 2007 command shell and list the available commands

|  |
| --- |
| 1. To launch the Operations Manager 2007 command shell, click Start, select Programs, and then select Command Shell from the System Center Operations Manager 2007 menu.  2. From the command shell prompt, type Get-OperationsManagerCommand to retrieve a list of all of the available Operations Manager 2007 cmdlets.  3. To see help for any specific cmdlet, type get-help followed by the name of the cmdlet. For example, type  get-help Get-State to retrieve help information about the Get-State cmdlet. |

Command Shell Usage Examples

This section contains a number of examples of command shell usage. Enter the commands at a command shell prompt, or use them in a batch file or script.

Important

The –name and –criteria parameters that are used by the command shell are case sensitive.

Export management packs

|  |
| --- |
| 1. To export a management pack, run the following command:  get-managementPack -name Microsoft.SQLServer.2005.Monitoring | export-managementPack -path c:\mp  2. To export all management packs in a management group, run the following command:  get-managementPack | export-managementPack -path c:\mp  3. To export all management packs that contain a specified string in their name, run the following command:  get-managementPack | where {$\_.name –match 'SQL'} |

Examine management pack elements

|  |
| --- |
| 1. To list all rules by management pack, run the following command:  get-rule | select @{name="MP";expression={foreach-Object {$\_.GetManagementPack().DisplayName}}},DisplayName | sort mp,displayName  2. To list all monitors in a specific management pack, run the following command:  (get-managementPack -name Microsoft.SQLServer.2005.Monitoring) | get-monitor | sort displayName | ft displayName  3. To list all disabled discoveries, run the following command:  get-discovery | where {$\_.enabled -eq 'false'} | ft displayName |

View Alert Data

|  |
| --- |
| 1. To view all unresolved alerts, run the following command:  get-alert -criteria "ResolutionState <> 255"  2. To view all alerts grouped by severity and name, run the following command:  get-alert -criteria "ResolutionState <> 255" | sort severity,name | group severity,name  3. To resolve all alerts generated by rules, run the following command:  get-alert -criteria "ResolutionState <> 255 and IsMonitorAlert = 'False'" | resolve-Alert |

Retrieve Performance Data

|  |
| --- |
| 1. The example below extracts processor utilization data for all computers for the month of October 2008 to a comma-delimited file:  > $startTime = get-date '10/1/2008'  > $endTime = get-date '10/31/2008'  > $pc = get-performanceCounter -criteria: "ObjectName='Processor' and  CounterName='% Processor Time' and MonitoringObjectPath='web.contoso.com'"  > get-performanceCounterValue -startTime $startTime -endTime $endTime -  performanceCounter $pc | export-csv c:\scripts\mom\perf.csv |

Additional Resources

For more information about Windows PowerShell, consult the following resources:

 [Windows PowerShell Technology Center](http://go.microsoft.com/fwlink/?LinkID=152209) (http://go.microsoft.com/fwlink/?LinkID=152209)

 [Scripting With Windows PowerShell](http://go.microsoft.com/fwlink/?LinkID=152211) (http://go.microsoft.com/fwlink/?LinkID=152211)

 [Windows PowerShell Owner’s Manual](http://go.microsoft.com/fwlink/?LinkID=133858) (http://go.microsoft.com/fwlink/?LinkID=133858)

Changing Passwords for Operations Manager Accounts

After the initial configuration of the Microsoft System Center Operations Manager 2007 accounts passwords, you might need to change those passwords under some circumstances.

You will need to change the password for Operations Manager 2007 accounts in either of the following situations:

 You specified a domain or local computer account for an Operations Manager 2007 account.

 Your organization has instituted password expiration.

For more information about changing the passwords for Operations Manager 2007 accounts, see the "Account Information for Operations Manager 2007" section of the [Operations Manager 2007 Security Guide](http://go.microsoft.com/fwlink/?LinkId=64017) (http://go.microsoft.com/fwlink/?LinkId=64017).

Identifying the Root Management Server in Operations Manager 2007

The root management server is the first management server for a management group. Features unique to the root management server include:

 The Web console connects to the root management server.

 The root management server contains the root management server encryption key, which is used to read and write data to the OperationsManager database.

 You enter the computer name for the root management server when installing reporting.

 While the System Center Data Access and System Center Management Configuration services will be installed on both a root management server and a management server, these two services should be running only on the root management server and they should be disabled on the management server.

You might need to identify the root management server if you want to install a Secure Sockets Layer (SSL) certificate for the Web console, to find the computer name, or to back up the root management server encryption key. Use the following procedure to identify the root management server.

To identify the root management server using the Operations console

|  |
| --- |
| 1. Log on to the computer hosting an Operations console with an account that is a member of the Operations Manager Administrators role for the Microsoft System Center Operations Manager 2007 management group.  2. In the Operations console, click the Administration button.  3. Expand Administration, expand Device Management, and then click Management Servers.  4. In the Management Servers pane, the management server with Root Management Server equal to Yes is the root management server. |

If the root management server has failed, the Operations console will be unable to connect; however, the computer name that the Operations console attempted to connect to will be displayed.

If a computer with an installation of the Operations console is unavailable, you can use the following procedure to examine the registry of any computer hosting a management server or gateway server.

Caution

Incorrectly editing the registry can severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.

To identify the root management server using the registry

|  |
| --- |
| 1. Log on to the computer with an account that is a member of the Administrators group.  2. On the Windows desktop, click Start, click Run, type regedit and then click OK.  3. On the Registry Editor page, expand HKEY\_LOCAL\_MACHINE, expand SOFTWARE, expand Microsoft, expand Microsoft Operations Manager, expand 3.0, and then click Machine Settings.  4. In the results pane, examine the string DefaultSDKService. The value of this string contains the name of the computer hosting the root management server.  Note  A management server that was recently promoted to a root management server might not be immediately reflected in the registry. |

Scheduling Maintenance and Monitoring

This topic provides general guidelines for scheduling Microsoft System Center Operations Manager 2007 maintenance tasks.

Maintenance Tasks Schedule

By default, Operations Manager 2007 performs maintenance tasks daily to maintain optimal performance of the Operations Manager database. These maintenance tasks are defined as System Rules in the Operations Manager 2007 management pack.

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

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

To check the schedules for the grooming jobs

|  |
| --- |
| 1. In the Operations Manager 2007 Operations console, click Authoring.  2. Under Authoring, expand Management Pack Objects, and then click Rules.  3. In the Rules pane, change the scope of management pack objects by clicking Scope.  4. In the Scope Management Pack Objects by target(s) dialog box, click Clear All.  5. In Look for, type Root Management Server to locate the root management server target from the System Center Core Library.  6. Select Root Management Server, and then click OK.  7. In the Rules pane, right-click the specific rule, and then click Properties.  8. In the Properties dialog box, click the Configuration tab.  9. Under Data Sources, click View to display the configured schedule for the rule.  10. Click Close twice to close the Properties dialog box.  Note  The scheduled times of the grooming jobs cannot be reconfigured by using an override. If you need to change the schedules of these maintenance tasks, you must first disable them with an override and then create new system rules that match the configuration of the original rules with new schedules. |

How to Configure Grooming Settings for the Operations Manager 2007 Database in Operations Manager 2007

Use the following procedure to specify when specific record types, such as Resolved Alerts, are deleted, or groomed, from the Operations Manager database of an Operations Manager 2007 management group. The default grooming setting for all record types is data older than 7 days. Grooming helps maintain the performance of the Operations Manager database by managing its size through the deletion of unnecessary records.

Note

Use the Reporting feature of Operations Manager 2007 for historical analysis of the management group. For more information about Reporting, see Reporting in Operations Manager 2007.

To configure database grooming settings for a management group

|  |
| --- |
| 1. In the Global Management Group Settings - Database Grooming dialog box, select a record type, and then click Edit.  Note  For more information about how to get to the Global Management Group Settings - Database Grooming, dialog box, see How to View Properties of a Setting for an Operations Manager 2007 Management Group.  2. In the dialog box for the record type, specify Older than days, and then click OK.  3. In the Global Management Group Settings - Database Grooming dialog box, select another record type to Edit or click OK. |

See Also

Backing Up and Restoring Operations Manager 2007 Components

Before reading this section, you should review the [Operations Manager 2007 Design Guide](http://go.microsoft.com/fwlink/?LinkId=86432) (http://go.microsoft.com/fwlink/?LinkId=86432) to understand the components of Microsoft System Center Operations Manager 2007, and to learn how to prepare for failure recovery.

As part of your maintenance plan, it is important to include a backup plan. This plan should be thoroughly tested and documented in a simulated environment using production backups. Ensure that the Operations Manager backup plan integrates into any existing backup procedures in the organization.

Decide on issues such as:

 What to back up

 How often to back up

 Complete or incremental backups

 How and when to practice a restore

After you decide what the best backup strategies for your Operations Manager environment, develop and document a backup plan that will become part of the overall disaster recovery plan.

It is strongly recommend that you test your backup and restore procedures thoroughly. Testing helps to ensure that you have the required backups to recover from various failures and that staff can run the procedures smoothly and quickly if a failure occurs.

You can use a test environment including all the Operations Manager 2007 components to test your backup and restore processes.

Note

The overall backup practices in your organization might include backing up the disk drives that the Operations Manager 2007 is installed on. When backing up those disk drives, including the management servers, be sure to exclude the <Installed Partition>\System Center Operations Manager 2007\Health Service State folder.

In This Section

[What to Back Up in Operations Manager 2007](#zaf93257f382741949b2e3b25cf17563a)

[Complete and Incremental Backups in Operations Manager 2007](#zc133e1e083c54971a2eacd3410390d6e)

[Backup File Naming Conventions in Operations Manager 2007](#z3c150c8d4bf24353a3b9f5b46db29172)

[Recommended Backup Schedule in Operations Manager 2007](#z0debc110e1a6426ab84aac3094a7e860)

[Failure and Restore in Operations Manager 2007](#zfed33f8d1b544bda9b25552d42659693)

Complete and Incremental Backups in Operations Manager 2007

You must ensure that database backups are as recent and complete as possible. This topic provides information to help you decide how to incorporate both complete and incremental database backups into an overall backup plan.

Complete Database Backups

A complete database backup captures the entire database, including all entries in the transaction log, and excluding any unallocated extents in the files. Pages are read directly from disk to increase the speed of the operation.

You can re-create a database from its backup in one step by restoring a backup of the database. The restore process overwrites the existing database or creates the database if it does not exist. The restored database will match the state of the database at the time the backup completed, minus any uncommitted transactions. Uncommitted transactions are rolled back when the database is restored.

A complete database backup uses more storage space per backup than transaction log and incremental database backups. Consequently, complete database backups take longer and therefore are typically created less frequently than incremental database or transaction log backups.

Incremental Database Backups

An incremental (differential) database backup records only the data that has changed since the last database backup. You can frequently make incremental backups of a database because incremental database backups are smaller and faster than complete database backups. Making frequent incremental backups decreases your risk of losing data.

In case of database failure, you can use incremental database backups to restore the database to the point at which the incremental database backup was completed.

Transaction Log Backups

The transaction log is a serial record of all the transactions that have been performed against the database since the transaction log was last backed up. With transaction log backups, you can restore the database to a specific point in time (for example, prior to entering unwanted data) or to the point of failure.

When restoring a transaction log backup, Microsoft SQL Server rolls forward all changes recorded in the transaction log. When SQL Server reaches the end of the transaction log, the state of the database is exactly as it was at the time the backup operation started. If the database is recovered, SQL Server then rolls back all transactions that were incomplete when the backup operation started.

Note

The OperationsManagerDW database uses a simple recovery model that truncates all transactions after completion. This means that backing up the log file is insufficient. Perform a complete database file backup.

Backup File Naming Conventions in Operations Manager 2007

Proper use of naming conventions for backup files can help you distinguish between them. Backups will be unique based on the management group that they are a backup of and the time that the backup was created. Consistent use of a standard naming convention can help you avoid the unintentional restoration of a backup to the wrong management group or restoring a backup that is from the wrong time.

Database File Naming Conventions

There might be multiple management groups in your System Center Operations Manager 2007 environment; therefore, be sure to include the management group name or some distinguishing name in the database backup file names.

You can also include other information in the file name, such as the database name, date, and type of backup. For example, a file name might be formatted as follows: OpsMgrDB\_DIFFERENTIAL\_<management group name>\_11\_01\_2007 or REPORTING\_FULL\_<management group name>\_11\_01\_2007.

Custom Management Pack Naming Conventions

If your monitoring infrastructure consists of multiple management groups, it is highly likely that the configuration of management packs and their overrides will vary across those management groups. Therefore, implementing a standard naming convention for custom management packs will help prevent the same problems as having a standard naming convention for databases does.

Include the management group name or some distinguishing name in the XML file name for these backups. Also include the version of the sealed management pack that the custom management pack contains overrides for. You can also include other information in the file name, such as the date. For example, a file name might be in the following format: <management group name>\_<Management pack name>\_<Management pack version>\_11\_01\_2007.xml.

What to Back Up in Operations Manager 2007

To be able to preserve data in case of a failure, you must have a recent backup of System Center Operations Manager 2007 databases and other important data as listed in this topic.

Data to Back Up

To ensure your ability to properly preserve and restore your Operations Manager 2007 environment, you should back up several key items as follows:

 OperationsManager database, OperationsManagerDW database, and the OperationsManagerAC database.

 Root management server encryption key

 Internet Information Services (IIS) 6.0 Metabase

 Internet Information Services (IIS) 7.0 configuration

 Custom management packs

 custom report definition files and computer certificates

In the event that the entire management group is lost, you must have backups of both the OperationsManager database and the root management server key to ensure a successful recovery. Therefore, at a minimum, ensure that your backup plans include both the OperationsManager database and the root management server encryption key.

How to Schedule Backups of Operations Manager Databases

Schedule a Database Backup

Use the procedure below to schedule a database backup using Microsoft SQL Server Management Studio 2005 or SQL Server Management Studio 2008). Use this procedure to back up the OperationsManager, OperationsManagerAC, and OperationsManagerDW databases.

To schedule a database backup to a file

|  |
| --- |
| 1. Start SQL Server Management Studio.  2. In the Connect to Server dialog box, select the appropriate values in the Server type drop-down list, in the Server name box, and in the Authentication box.  3. Click Connect.  4. In Object Explorer, expand Databases.  5. Right-click the database that you want to back up, click Tasks, and then click Back Up.  6. In the Back Up Database dialog box, type the name of the backup set in the Name box, and then under Destination, click Add.  7. In the Select Backup Destination dialog box, type a path and a file name in the Destination on disk box, and then click OK.  Important  The destination location must have enough available free disk space to store the backup files based upon the frequency of your backup schedule.  8. In the Script list, click Script Action to Job.  9. If you want to change job parameters, in the New Job dialog box, under Select a page, click Steps, and then click Edit.  10. Under Select a page, click Schedules, and then click New.  11. In the New Job Schedule dialog box, type in the job name in the Name box, specify the job schedule, and then click OK.  Note  If you want to configure alerts or notifications, you can click Alerts or Notifications under Select a page.  12. Click OK twice. |

OperationsManager Database

The OperationsManager database contains almost all of the Operations Manager environment configuration settings, agent information, management packs with customizations, operations data, and other data required for Operations Manager to operate properly.

It is critical that you back up the OperationsManager database regularly to preserve the latest information about your Operations Manager environment. A database failure without a recent backup will result in the loss of almost all Operations Manager-specific data, and you will need to rebuild the entire Operations Manager environment.

Note

If your backup procedure sets the OperationsManager database to be offline during backup, Operations Manager caches incoming data, and then, after backup is complete, Operations Manager stores that data in the database.

Reporting Databases

Operations Manager Reporting uses the following databases:

 Operations Manager 2007 data warehouse (OperationsManagerDW)

 SQL Server Reporting Services databases (ReportServer and ReportServerTempDB)

The OperationsManagerDW database contains all of the performance and other operational data from your Operations Manager environment. SQL Reporting Services then uses this data to generate reports such as trend analysis and performance tracking.

To be able to restore reporting functionality in case of failure, it is critical that you back up the OperationsManagerDW database. When determining how often and when to back up this database, you should consider the following:

 This database can grow to a very large size (more than one terabyte) over time.

 Management servers frequently write data to this database.

 IT SLA requirements are based on the need for reporting availability in the organization.

Note

The OperationsManagerDW database uses a simple recovery model, which truncates all transactions after completion. Therefore, backing up only the log file is insufficient; you must back up the entire database.

The SQL Server Reporting Services databases store report definitions, report metadata, cached reports, and snapshots. In case of failure, you can re-create report definitions by re-importing the reports. However, cached reports, which are reports that have already been created, will be lost.

To be able to restore reporting functionality in case of failure, it is recommended that you back up the SQL Server Reporting Server databases.

ACS Database

The Audit Collection Services (ACS) database, OperationsManagerAC, is the central repository for events and security logs that are collected by ACS forwarders on monitored computers.

The OperationsManagerAC database can grow significantly depending upon how many ACS forwarders send events to the ACS database and the filters configured to control what events are written to the database.

Master Database

The master database is a system database, which records all of the system-level information for a Microsoft SQL Server system, including the location of the database files. It also records all logon accounts and system configuration settings. The proper functionality of the master database is key to the operation of all of the databases in a SQL Server instance.

MSDB Database

The MSDB database, Msdbdata, is a SQL system database, which is used by the SQL Server agent to schedule jobs and alerts and for recording operators. The proper functionality of the MSDB database is key to the operation of all the databases in a SQL Server instance.

Note

This database contains task schedules that are vital to the health of the Operations Manager 2007 database, and it should be included in your backup plan. You need to back up this database only after you configure Operations Manager 2007 or if you change the scheduled agent jobs.

How to Back Up the Root Management Server Encryption Key

The root management server (RMS) is the central point of configuration management and overall health monitoring for the entire managed environment.

The root management server encryption key holds all the Run As Account information defined in the management group. To successfully restore a failed root management server, you must use that key to reattach the databases and to access the Run As Accounts that have been encrypted with this key. If you need to restore the root management server without this backup, you need to re-enter your entire Run As Accounts.

To back up or to restore the root management server key, you need to use the SecureStorageBackup tool. The tool can start the Encryption Key Backup or Restore Wizard, or run as a command-line tool. The availability and the behavior of the tool depend on whether or not the console is installed on the management server.

The SecureStorageBackup tool functions as follows:

 If the console and a management server are both installed, the tool is installed in the System Center Operations Manager 2007 installation folder.

In this case, by default, the Encryption Key Backup or Restore Wizard runs at the final stage of setup, allowing you to back up the key. Also, if you start the tool without arguments, it starts the Encryption Key Backup or Restore Wizard, and if you start the tool with arguments, it runs as a command-line tool.

 If the console is not installed, the SecureStorageBackup tool is not installed. For example, this happens if you are installing Operations Manager RMS on a cluster without installing the console on any server. In this case, to use the tool, you must first copy it from the SupportTools folder on the installation media to the installation folder on the management server.

In this case, the tool runs as a command-line tool, and you must provide proper arguments. You can run SecureStorageBackup.exe with the '/?' switch to get help for the tool.

When backing up the encryption key, always ensure that you provide a backup location that is easily accessible in case you later need to retrieve the key. For more information about backing up the root management server encryption key, see the Microsoft System Center Operations Manager 2007 Deployment Guide.

Use the procedures below to back up the root management server encryption key.

To start the Encryption Key Backup or Restore Wizard to back up the root management server encryption key

|  |
| --- |
| 1. Log on to the computer hosting the root management server with an account that is a member of the Administrators group.  2. Open a command prompt window using the Run as Administrator option.  3. At the command prompt, type  cd <Operations Manager Installation Folder>  4. Type SecureStorageBackup and then press ENTER.  5. In the Encryption Key Backup or Restore Wizard, on the Backup or Restore? page, select the Backup the Encryption Key option, and then complete the wizard. |

To run the SecureStorageBackup tool in a command-line mode to back up the root management server encryption key

|  |
| --- |
| 1. Log on to the computer hosting the root management server with an account that is a member of the Administrators group.  2. Open a command prompt window using the Run as Administrator option.  3. At the command prompt, type  cd\<Operations Manager Installation Folder>  SecureStorageBackup Backup <BackupFile>  4. At the Please enter the password to use for storage/retrieval prompt, type a password that is at least eight characters long, and then press ENTER.  5. At the Please re-enter your password prompt, type the same password, and then press Enter. |

How to Back Up the IIS 6.0 Metabase

The Internet Information Services (IIS) 6 metabase is a hierarchical store that contains configuration information and schema used to configure IIS. For Microsoft System Center Operations Manager 2007, IIS supports components such as the Web console server and SQL Server Reporting Services; therefore, you must back up the IIS metabase. Operations Manager 2007 SP1 and Operations Manager 2007 R2 Web components will both run on Windows Server 2003 and IIS 6. This procedure is the same for any version of Operations Manager 2007 running on Windows Server 2003 and IIS 6.

Use the following procedure to back up the IIS 6.0 metabase. For more information about the IIS 6.0 metabase, see the [IIS 6.0 Technical Reference](http://go.microsoft.com/fwlink/?LinkId=93786) (http://go.microsoft.com/fwlink/?LinkId=93786).

To back up the IIS 6.0 metabase

|  |
| --- |
| 1. Open Control Panel, double-click Administrative Tools, and then double-click Internet Information Services (IIS) Manager.  2. Right-click the name of your computer in IIS Manager, point to All Tasks, and then click Backup/Restore Configuration.  3. In the Configuration Backup/Restore dialog box, click Create Backup, and then type a name for this backup.  Note  If you want to create secure backup, in the Configuration Backup dialog box, select the Encrypt backup using password check box, type a password in the Password box, and then type the same password in the Confirm password box. The backup name cannot contain any symbols, just letters and numbers.  4. Click OK to back up the administrative settings in the metabase.  The backup name and its date and time are now listed under Previous backups.  5. Click Close, and then close IIS Manager. |

How to Back Up an IIS 7 Configuration

Operations Manager 2007 SP1 or Operations Manager 2007 R2 can run on both Windows Server 2003 and Windows Server 2008. This means that you may have to back up either the IIS 6 metabase or the IIS 7 configuration, depending on the operating system that is being used. This procedure tells you how to back up the IIS 7 configuration. The IIS 7 configuration is split between the web.config files and the applicationHost.config files. You should follow IIS 7 recommendations on how to back up the configuration in the web.config files. The applicationHost.config files include configuration information for the sites, applications, virtual directories, application pool definitions, and the default configuration settings for all sites on the Web server.

To back up the IIS 7 configuration from a command prompt

|  |
| --- |
| 1. Log on to the Windows Server 2008 computer that is hosting the Operations Manager 2007 components with an account that has administrator rights.  2. Open a command prompt by using the Run as Administrator option and change directory to %windir%\system32\inetsrv.  3. At the command prompt, type appcmd add backup <backupname>. If you do not include the name of the backup, the system will name it for you by using a date, time format. |

For more information about the IIS 7 appcmd.exe command and how to use it, see the “IIS 7.0: Appcmd.exe” topic in the [IIS 7.0 Operations Guide](http://go.microsoft.com/fwlink/?LinkId=150156) (http://go.microsoft.com/fwlink/?LinkId=150156).

How to Back Up Custom Management Packs

Management packs contain monitoring rules for applications and services. Both sealed and unsealed management packs can be customized by superseding their default values using overrides, or by defining custom rules or monitors. Custom management packs are unsealed and are saved to a separate .xml management pack file. Only custom management packs can be exported. By default, the file is saved to the My Default management pack folder.

You should back up custom management packs regularly even though backing up the OperationsManager database captures management pack information. Running management pack backups as an independent operation from database backups allows you to re-import them separately from the database, which can be useful in cases when you must roll back the customized changes in one or more custom management packs.

Use the export feature from the Operations console to back up management packs.

To export a custom management pack

|  |
| --- |
| 1. Log on to a management server with an account that is a member of the Microsoft System Center Operations Manager 2007 Administrators role for the Operations Manager 2007 management group.  2. In the Operations console, click Administration.  3. In the Administration pane, click Management Packs.  4. In the management packs pane, right-click the custom management pack you want to export, and then click Export Management Pack.  5. In the Save As dialog box, type the path and file name for the management pack file, or click Browse to save the file to a different directory, and then click Save. |

Recommended Backup Schedule in Operations Manager 2007

You should determine how often and when to run backups. In general, you should perform database backups according to your company’s backup policy.

Backup Schedule

The following table suggests a schedule for regular backups of your Microsoft System Center Operations Manager 2007 components and related items. These suggestions are specific to your Operations Manager 2007 environment and are meant to complement other regularly scheduled backups in your environment.

You should schedule those backup jobs at a time that does not conflict with the schedule of the Operations Manager grooming tasks. The Operations Manager grooming jobs run on the Operations Manager 2007 Database Server and both read from and write to the database. Backing up the database during the same time might cause failures in the backup job, the grooming job, or both.

At a minimum, an incremental backup of the Operations Manager database should be performed on a daily basis. A complete backup should be performed on the Operations Manager database weekly. The master and msdb databases should be backed up any time a change occurs that affects either database, but you should back them up at least monthly.

|  |  |  |
| --- | --- | --- |
| Component to Back Up | Full Backup | Incremental Backup |
| OperationsManager | Weekly | Daily |
| OperationsManagerDW | Monthly | Weekly |
| ReportServer | On a recurring basis, with the frequency depending on how often reports change in your organization, and every time after significant changes are made to report definitions (including additions, changes, and deletions). | Same as full backup |
| OperationsManagerAC | Monthly | Weekly |
| Master database (Master) | Every time, after installing and configuring the Operations Manager database components and after making significant changes to logons or other security changes. | Per IT policies |
| Msdb database (Msdbdata) | After the initial installation and configuration of the Operations Manager database components. | After changing the scheduled Microsoft SQL Server Agent jobs that Operations Manager uses. |
| Custom Management Packs (.xml files) | Monthly or after making significant changes to management packs. | Not applicable |

Failure and Restore in Operations Manager 2007

Even with the best maintenance practices, data might become corrupted, causing interruption to System Center Operations Manager 2007 functionality and loss of data.

There are various causes for failure. Some of the most common causes can be classified as follows:

 Hardware failure, such as the storage system having an impact on data availability or integrity

 Security breach or virus infection

 Accidental deletion or corruption of Active Directory Domain Services (AD DS) security information, such as accounts or groups

 Physical disaster

This section describes various Operations Manager failure scenarios and how to restore Operations Manager components to resume services.

In This Section

[Failure Recovery Scenarios for the Root Management Server](#z32989ce26b544eb7b6d6015e4347ee88)

Impact of Failure in Operations Manager 2007

Various Microsoft System Center Operations Manager 2007 servers and components can potentially fail, impacting Operations Manager functionality.

The amount of data and functionality lost during a failure is different in each failure scenario. It depends on the role of the failing component, on the Operations Manager deployment, on the length of time it takes to restore the failing component, and on the availability of backups.

Impact of Failure

The impact of failure is minimized if the Operations Manager deployment includes failover servers or clustering. The impact is greater if clustering and failover management servers are not implemented. This is because it will take longer to restore a failed component. When it takes longer to restore the functions provided by a failed component, there is a greater risk of data loss occurring and when data loss does occur, the amount of data lost will be greater. For more information about minimizing the impact of failure, see Reduce the Impact of Failure below.

In some failure scenarios, Operations Manager is able to continue to function properly for a short period of time without losing data. Then, after you repair the failing component, complete functionality is automatically restored without any further intervention.

The following table lists the impact of failure of various Operations Manager components. In this table, the assumption is that each server listed performs only a single role, as specified.

|  |  |  |
| --- | --- | --- |
| Failed Component | Impact: Best-Case Scenario | Impact: Worst-Case Scenario |
| Management server | Workload on additional management servers in the management group is increased until the failed management server is restored. |  Data is queued on managed computers and is not processed because agents are unable to send it to the management server.   Agentless computers are not managed.   Gateway servers cannot transfer data from agents to the management server. |
| Root management server | With at least one server in the cluster functioning, there is no impact. |  Operations consoles and Web consoles are unable to connect and manage the configuration of the management group.   Configuration management for the management group is unavailable.   Connections to other management groups are unavailable.   Cannot perform any Operations Manager administrative tasks, such as viewing, editing, or managing objects.   The Operations console does not function.   Connections to third-party management products using connectors are unavailable. |
| Operations Manager reporting server (OperationsManager database is intact) |  |  Reports are not accessible.   The Reporting view in the Operations console does not function. |
| OperationsManager database | If the OperationsManager database has been installed in a failover cluster, and as long as one of the cluster nodes is functioning, there is no impact. If log shipping is implemented, services might be reduced until the database is rebuilt. |  Data from managed computers is not processed and is not stored in the database. This data might eventually be lost.   Management servers start to queue data in their cache. When the cache is full, the management servers start to drop data, starting with performance data.   Cannot perform any Operations Manager administrative tasks, such as viewing, editing, or managing objects.   Reports do not contain up-to-date information.   The Operations console does not function.   Changes to management packs are not propagated to agents. |
| Data warehouse server (OperationsManagerDW database is intact) | With at least one server in the cluster functioning, there is no impact. If the OperationsManagerDW database has failed, clustering does not reduce the impact of failure. (See the next column for impact.) |  Cannot view, edit or manage reports.   Cannot view, edit, or manage Audit Collection Services (ACS) Reports if installed on the same computer that is running SQL Server. |
| Gateway server | With multiple gateway servers deployed, agents can fail over to another gateway server, and communication with management servers is not interrupted. |  Up-to-date monitoring data is not available because agents and management servers cannot communicate. |
| Audit Collection Database | If the Audit Collection Database is intact, with at least one server in the cluster functioning, there is no impact. If the Audit Collection Database has failed, clustering does not reduce the impact of failure. (See the next column for impact.) |  Security events are queued on managed computers and are not processed. This data might eventually be lost.   Performance on managed computers is degraded because of the accumulated data.   ACS reports do not contain up-to-date information. |
| Computer hosting the Operations console | Not applicable. |  Cannot use the console on the failed computer. |
| ACS Collector Server | Not applicable. |  Audit events from ACS Forwarders are not processed. |

Reduce the Impact of Failure

The effects of some server failures can be reduced significantly by adding redundancy or implementing a failover solution, such as clustering. This also reduces the urgency of restoration.

The following list includes configuration options that add redundancy and clustering to the Operations Manager deployment. Implementing any of these options reduces the impact of failure and contributes to the high availability of Operations Manager in your organization:

 Add management servers.

 Install the root management server into a Cluster service failover cluster.

 Place the databases in a Cluster service failover cluster.

 Configure gateway servers for failover.

 Configure log shipping.

 Configure multihoming of agents across management groups.

Each option is further described below. For further information about deployment options that help ensure high availability and help reduce the impact of failure, see the [Operations Manager 2007 Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=93785) (http://go.microsoft.com/fwlink/?LinkId=93785).

Add Management Servers

Deploy more than one management server in a management group. This allows agents to fail over if a management server has failed.

If a management server has failed, the agents that report to that management server automatically start reporting to another management server in the same management group. After the failed management server is restored, agents can resume reporting to the original management server.

If the root management server is failing, you can promote an existing management server to the root management server role. After the root management server is restored, you can demote the temporary root management server and re-promote the restored server to its original root management server role.

Install the Root Management Server into a Cluster Services Failover Cluster

Install the root management server into a Cluster service failover cluster. If a node in the root management server cluster fails, the root management server role moves to another cluster node. This allows the RMS to continue to function normally.

After you restore the failed cluster node, you can move the RMS back to the original node or leave it running on another node in the failover cluster.

Place Databases in a Cluster Services Failover Cluster

Place the OperationsManager, the OperationsManagerDW, and the OperationsManagerAC databases in a Cluster service failover cluster. As in the case of the RMS cluster, if a node fails, all the databases would be moved to another node in the cluster and continue to function normally. If a database becomes corrupted however, you may need to restore it from your most recent backup.

Configure Gateway Server Failover

Deploy multiple gateway servers to allow agents to fail over between gateway servers and to distribute the management workload.

Gateway servers can also be configured for failover between collection management servers in a management group if multiple collection management servers are available.

Configure Log Shipping

Log shipping maintains a copy of an Operations Manager database on a separate Microsoft SQL Server 2005 or SQL Server 2008 server. Log shipping keeps the copy of the database up to date by sending the transaction logs from the source database in the active management group to the destination database in the standby management group.

If a database becomes corrupted, you can configure Operations Manager to temporarily use the standby database. After the original database is restored, you can reconfigure Operations Manager to use that database.

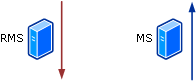
Failure Recovery Scenarios for the Root Management Server

This topic describes three failure recovery scenarios for the root management server.

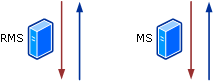
These scenarios involve promoting a management server to replace a failed root management server. In all cases, a management server must be present in the management group prior to the failure of the RMS in order to be promoted to be the RMS.

Root Management Server Recovery

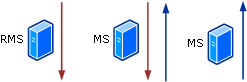
To use any of these scenarios, you must either have a back up of the root management server encryption key or the root management server must be available to allow backing up of the encryption key.



 If the root management server fails, promote another management server to be the root management server.



 If the root management server fails, promote another management server to be the root management server. After the failed computer is available again, you have the option of promoting it back to being the root management server.



 If the root management server fails, promote another management server to be the root management server. In the future, you can set up a new management server and promote it to be the root management server.

Use the [How to Promote a Management Server to a Root Management Server Role in Operations Manager 2007](#zd766717bb34b4d86975eaae1cb175a6c) procedure to promote a management server to be the root management server. You can apply this procedure to all three scenarios.

See Also

[How to Promote a Management Server to a Root Management Server Role in Operations Manager 2007](#zd766717bb34b4d86975eaae1cb175a6c)

[How to Back Up the Root Management Server Encryption Key](#za5685bf2110e4991af8c45ae9a0b2f13)

[The Root Management Server encryption key is unavailable after you replace or reinstall the Root Management Server server in Microsoft System Center Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=151501)

High-Level Restore Guidelines in Operations Manager 2007

Use the following table for information about possible failure scenarios and the general steps required to restore operations and data in that scenario.

General Restore Steps

|  |  |  |
| --- | --- | --- |
| Failed Component | General Restoration Steps | Required Backups |
| Management server | With additional management servers:  1. Repair the server.  2. Reinstall the Operations Manager management server on the repaired server.  3. After the failed management server is restored, Operations Manager agents will eventually resume reporting to that management server.  Without additional management servers:  1. Configure the root management server (RMS) as the primary management server in the management group.  2. Install a new management server in the management group. Use the computer running Microsoft SQL Server that is hosting the OperationsManager database, and use the same action account that was previously defined.  3. Configure the newly installed management server as the primary management server. | none |
| Root management server | Clustered:   Repair the failed server, and re-connect to the cluster.  Not clustered:  1. Promote an existing management server to root management server.  2. Repair the failed server.  3. Reinstall the Operations Manager management server on the repaired server.  4. Demote the temporary root management server to management server.  5. Promote the repaired server to root management server. | Root management server encryption key |
| Data warehouse server/Operations Manager reporting server (assumes the OperationsManager database is intact | Clustered:  1. Repair the failed server, or reinstall SQL Server and reconnect to the cluster.  2. If needed, configure all management servers to point to the repaired server.  Not clustered:  1. Repair the server as needed.  2. Restore the OperationsManager database. |  OperationsManager database   Root management server encryption key |
| OperationsManager database | 1. Reinstall the Operations Manager reporting server component if needed.  2. Restore the OperationsManager database.  If log shipping has been implemented:   Rebuild and restore the database. |  OperationsManager database   root management server encryption key |
| Operations Manager reporting server | Clustered:  1. Reinstall the Operations Manager reporting server if needed.  2. Restore the OperationsManagerDW database, and the ReportServer and ReportServerTempDB databases if needed. |  OperationsManagerDW database |
| Gateway server | 1. Repair the server if needed.  2. Reinstall the Operations Manager gateway server if needed. | None |
| Computer hosting Operations console | 1. Repair the computer.  2. Reinstall the Operations Manager console. | None |
| OperationsManagerAC (Audit Collection) database | 1. Repair the Operations Manager Audit Collection Services (ACS) database server if needed.  2. Reinstall SQL Server if needed.  3. Reinstall the Operations Manager ACS database component if needed.  4. Restore the Audit Collection database. | Audit Collection database |
| ACS Collector Server | Do either of the following:  1. Repair the ACS Collector server if needed.  2. Install the ACS Collector on another management server in the management group if needed.  3. Install another management server in the management group and install the ACS Collector if needed. | None |

How to Restore Operations Manager 2007 Databases

Use the following procedure to restore a Microsoft System Center Operations Manager 2007 database using Microsoft SQL Server Management Studio. This procedure applies to databases on both SQL Server 2005 and SQL Server 2008.

Note

If you want to resize the OperationsManager database, you must resize it by using SQL Server. For more information, see [Microsoft SQL Server](http://go.microsoft.com/fwlink/?LinkID=162007) (http://go.microsoft.com/fwlink/?LinkID=162007) in the TechNet Library.

To restore a database backup

|  |
| --- |
| 1. Start SQL Server Management Studio.  2. In the Connect to Server dialog box, select the appropriate values in the Server type drop-down combo box, in the Server name box, and in the Authentication box.  3. Click Connect.  4. In Object Explorer, expand Databases, and then select the OperationsManager, OperationsManagerAC, or OperationsManagerDW database.  5. Right-click the database, point to Tasks, and then click Restore.  6. Click Database to open the Restore Database dialog box.  7. On the General page, the name of the restoring database appears in the To database list.  8. In the To a point in time text box, either retain the default (the most recent possible) or select a specific date and time by clicking the browse button, which opens the Point in Time Restore dialog box.  9. To specify the source and location of the backup sets to restore, click the From Device option.  10. Click Browse to open the Specify Backup dialog box.  11. In the Backup media list box, select one of the listed device types. To select one or more devices for the Backup location list box, click Add.  12. In the Select the backup sets to restore grid, select the backups to restore. This grid displays the backups available for the specified location.  13. In the Restore options panel, select the Overwrite the existing database option.  14. In the Restore the database files as options panel, verify the original database file name and path are correct.  15. For the Recovery state options, specify the state option Leave the databases ready to use by rolling back the uncommitted transactions. Additional transaction logs cannot be restored.  16. Click OK to restore the database. |

How to Restore the IIS 6.0 Metabase Backup in Operations Manager 2007

Use the following procedure to restore an Internet Information Services (IIS) 6.0 Metabase backup. Operations Manager 2007 SP1 and Operations Manager 2007 R2 can both run on Windows Server 2003 with IIS 6. This procedure can be used for any version of Operations Manager 2007 that makes use of IIS 6.

To restore an IIS 6.0 Metabase backup

|  |
| --- |
| 1. Open Control Panel, double-click Administrative Tools, and then double-click Internet Information Services (IIS) Manager.  2. Right-click the name of your computer in IIS Manager, point to All Tasks, and then click Backup/Restore Configuration.  3. Under Previous backups, select the file name that you want, and then click Restore. If prompted for a password, type the password. |

How to Restore an IIS 7 Configuration

Both Operations Manager 2007 SP1 and Operations Manager 2007 R2 can run on Windows Server 2008, which means that they can use IIS 7. The following procedure should be used for any Operations Manager 2007 version that is running Windows Server 2008 and IIS 7.

To restore the IIS 7 configuration from a command prompt

|  |
| --- |
| 1. Log on to the Windows Server 2008 computer that is hosting Operations Manager 2007 components with an account that has administrator rights.  2. Open a command prompt by using the Run as Administrator option and change directory to %windir%\system32\inetsrv.  3. At the command prompt, type appcmd restore backup <backupname>. |

How to Restore the Root Management Server Encryption Key in Operations Manager 2007

To restore the root management server (RMS) key, you need to use the SecureStorageBackup tool. The tool can start the Encryption Key Backup or Restore Wizard, or run as a command-line tool. The availability and behavior of the tool depends on whether or not the console is installed on the management server.

The SecureStorageBackup tool behaves as follows:

 If the console and a management server are both installed, the tool is installed in the Microsoft System Center Operations Manager 2007 installation folder.

In this case, if you start the tool without arguments, it starts the Encryption Key Backup or Restore Wizard. If you start the tool with arguments, it runs as a command-line tool.

 If the console is not installed, the SecureStorageBackup tool is not installed. In this case, to use the tool, you must first copy it from the SupportTools folder on the installation media to the installation folder on the management server. For example, this happens if you are installing Operations Manager on a clustered RMS without installing the console on any server.

In this case, the tool runs as a command-line tool, and you must provide proper arguments. You can run SecureStorageBackup.exe with the '/?' switch to get help for the tool.

Use the procedures below to restore the root management server encryption key, which is on the same server when recovering the root management server or on a different server when creating a clustered root management server.

To start the Encryption Key Backup or Restore Wizard to restore the Root Management Server encryption key

|  |
| --- |
| 1. Log on to the computer hosting the root management server with an account that is a member of the Administrators group.  2. Open a command prompt window using the Run as Administrator option.  3. At the command prompt, enter the following:  cd <Operations Manager Installation Folder>  SecureStorageBackup  4. In the Encryption Key Backup or Restore Wizard, on the Backup or Restore? page, select the Restore the Encryption Key option and then complete the wizard. |

To run the SecureStorageBackup tool in command-line mode to restore the root management server encryption key

|  |
| --- |
| 1. In a command prompt window using the Run as Administrator option and, enter the following:  cd\<Operations Manager Installation Folder>  SecureStorageBackup Restore <BackupFile>  2. At the Please enter the password to use for storage/retrieval prompt, type the password, and then press ENTER.  Use the same password that was used to back up the encryption keys. |

Making Updates to an Operations Manager 2007 Deployment

After the initial deployment of Microsoft System Center Operations Manager 2007, you might need to make changes or upgrades to the original deployment for reasons such as the following:

 You need to replace hardware that is experiencing problems and that is no longer considered reliable.

 You need to add additional hardware to improve scalability and performance.

 You need to move a database and log file to a different volume because of space or performance reasons.

 You need to change hardware that is leased and is due to expire soon.

 You need to change or upgrade hardware to comply with new hardware standards.

 You initially installed multiple Operations Manager components on a single server and you need to distribute some components to other servers.

 You need to restore functionality in a failure scenario.

Operations Manager supports changes to your Operations Manager deployment as listed below. Be cautious when performing these operations because they can result in data loss if not performed correctly.

In This Section

[How to Move the OperationsManager Database in Operations Manager 2007](#z73ece35cf2c54fc5990624aac95f7739)

[How to Move the OperationsManagerDW Database in Operations Manager 2007](#z285e3494091740e6b4b79149762acbb8)

[How to Move the OperationsManagerAC Database in Operations Manager 2007](#zcc96f98747114c3c9bef7a1269245300)

[How to Promote a Management Server to a Root Management Server Role in Operations Manager 2007](#zd766717bb34b4d86975eaae1cb175a6c)

[How to Remove a Management Server From a Computer in Operations Manager 2007](#z566c62c3f85840908d94535a9fc87313)

[How to Move the Operations Manager Reporting Server in Operations Manager 2007](#z31b34d1d9cb64e8a8fe9b539da81501e)

How to Move the OperationsManager Database in Operations Manager 2007

After the initial deployment of Microsoft System Center Operations Manager 2007, you might need to move the Operations Manager database from one Microsoft SQL Server-based computer to another.

SQL Server 2005 and SQL Server 2008 support the ability to change the location of the data files and of the log files between SQL Server-based computers, between instances on the same SQL Server-based computer, and different volumes on the same SQL Server-based computer. For more information about using this function in SQL Server, see the [SQL Server documentation](http://go.microsoft.com/fwlink/?LinkId=93787) (http://go.microsoft.com/fwlink/?LinkId=93787).

The high-level steps of moving the OperationsManager database are as follows:

1. Back up the OperationsManager database.

2. Uninstall the OperationsManager database.

3. Delete the Operations Manager database.

4. Restore the OperationsManager database.

5. Update management servers with the new database server name.

6. Update the Operations Manager database with the new database server name.

7. Update the Operations Manager database logins on the new database server. Ensure that for the root management server, the SDK Account and the Action Account are included in the logins and that they have appropriate permissions. If reporting is installed, ensure that the Data Warehouse Action Account has appropriate permissions.

8. Set ENABLE\_BROKER if needed.

9. Verify that the move is successful by ensuring that the console is displaying valid data.

OperationsManager Database Relocation

Use the procedure below to move the OperationsManager database to a new server.

To move the OperationsManager database

|  |
| --- |
| 1. Install and configure a new SQL Server-based computer. Ensure that you have system administrator permissions on both the original SQL Server-based computer and the new SQL Server-based computers.  2. Back up the following:   Back up all databases. On the current server that hosts the Operations Manager database, use SQL Server Management Studio to back up the Operations Manager (default name) database.   Back up the encryption key on the root management server by using the SecureStorageBackup.exe utility.  3. Stop the Operations Manager services (System Center Management, System Center Data Access, and System Center Management Configuration for root management servers, and System Center Management for management servers) on the management servers in the management group.  In a clustered root management server environment, use Cluster Administrator (Windows Server 2003) or Failover Cluster Management (Windows Server 2008) to configure each of the three services listed above with the Take Offline option.  4. On the current server that hosts the OperationsManager database, uninstall the database component as follows (these steps do not physically remove the OperationsManager database from SQL Server):  Note  Perform this step if the database is the only component on the server. Otherwise, you will still be able to delete the database following the next step.  a. Click Start, click Control Panel, and then click Add or Remove Programs for Windows Server 2003 or Programs and Features for Windows Server 2008.  b. In the Add or Remove Programs dialog box for Windows Server 2003 or Programs and Features dialog box for Windows Server 2008, select System Center Operations Manager 2007 R2, and then select Remove for Windows Server 2003 or select Uninstall for Windows Server 2008.  c. Complete the wizard.  5. On the current server that hosts the OperationsManager database, delete the OperationsManager database as follows:  a. In Microsoft SQL Server Management Studio, navigate to Databases.  b. Right-click OperationsManager, and then click Delete.  c. In the Delete Object dialog box, ensure that the Delete backup and restore history information for databases and Close existing connections options are both selected.  d. Click OK to complete the operation.  6. On the new server, use Microsoft SQL Server Management Studio to restore the OperationsManager database that you previously backed up. To access the database backup file, copy the backup file to a local drive or map a local drive to the folder that contains the backup file.  7. Update the registry on each management server in the management group to reference the new SQL Server-based computer. Complete this step also on the root management server. If the root management server is clustered, you must complete this step on all the nodes in the cluster.  Note  Before editing the registry, follow your site's backup policies with regard to the registry.  a. Log on to the management server with Administrator permissions.  b. Click Start, select Run, type regedit in the Open box, and then click OK to start Registry Editor.  c. Under HKEY\_LOCAL\_MACHINE\Software\Microsoft\Microsoft Operations Manager\3.0\Setup, double-click the value DatabaseServerName, and then change the value to the hostname of the SQL Server-based computer now hosting the OperationsManager database.  d. Click OK.  e. Close the Registry Editor.  f. After you have completed this step on all management servers in the management group, restart the System Center Management, System Center Data Access, and System Center Management Configuration services on the root management server, and then restart only the System Center Management service on the remaining management servers.  Important  Do not start the System Center Management Configuration and System Center Data Access services on the management servers, as these services should be running only on the root management server.  8. Update the OperationsManager database with the New Database Server Name, and ensure that the account that you are logged on with has sufficient privileges on the SQL Server instance.  a. Open SQL Server Management Studio.  b. Expand Databases, OperationsManager, and Tables.  c. Right-click dbo.MT\_ManagementGroup, and then click Open Table if you are using SQL Server 2005 or click Edit Top 200 Rows if you are using SQL Server 2008.  d. Change the value in the SQLServerName\_6B1D1BE8\_EBB4\_B425\_08DC\_2385C5930B04 column to reflect the name of the new SQL Server-based computer.  e. Save your change.  9. On the new server hosting the OperationsManager database, add the correct permission for the login of the root management server on which the SDK Account is running, as follows:  a. Open Microsoft SQL Server Management Studio, and in the Object Explorer pane, navigate to Security and then expand Logins.  b. Locate the SDK Account, and add the account if it is not listed.  Note  If the SDK Account is running as LocalSystem, use the format <domain\computername$> in SQL Logins, where <computername> is the name of the root management server.  c. Right-click the SDK Account, and select Properties.  d. In the Login Properties dialog box, in the Select a page pane, select User Mapping.  e. In the Users mapped to this login list, in the Map column, select the box that corresponds to OperationsManager (default name).  f. In the Database role membership for: OperationsManager list, ensure that the following items are selected: configsvc\_users, db\_datareader, db\_datawriter, db\_ddladmin, and sdk\_users.  g. Click OK to save your changes and to close the Login Properties dialog box.  10. On the new server hosting the Operations Manager database, add the correct permission for the login of the root management server on which the Action Account is running, as follows:  a. Open Microsoft SQL Server Management Studio, and in the Object Explorer pane, navigate to Security and then expand Logins.  b. Locate the Action Account, and add the account if it is not listed. If the Action Account is running as LocalSystem, use the format <domain\computername$> in SQL Logins, where <computername> is the name of the root management server.  c. Right-click the Action Account, and select Properties.  d. In the Login Properties dialog box, in the Select a page pane, select User Mapping.  e. In the Users mapped to this login list, in the Map column, select the box that corresponds to OperationsManager (default name).  f. In the Database role membership for: OperationsManager list, ensure that the following items are selected: db\_datareader, db\_datawriter, db\_ddladmin, and dbmodule\_users.  g. Click OK to save your changes and to close the Login Properties dialog box.  11. On the new server hosting the Operations Manager database, add the correct permission for the login of the Data Warehouse server on which the Data Warehouse Action Account is running, as follows:  a. Open Microsoft SQL Server Management Studio, and in the Object Explorer pane, navigate to Security and then expand Logins.  b. Locate the Data Warehouse Action Account, and add the account if it is not listed.  c. Right-click the Data Warehouse Action Account, and select Properties.  d. In the Login Properties dialog box, in the Select a page pane, select User Mapping.  e. In the Users mapped to this login list, in the Map column, select the box that corresponds to OperationsManager (default name).  f. In the Database role membership for: OperationsManager list, ensure that the following items are selected: db\_datareader and dwsynch\_users.  g. Click OK to save your changes and to close the Login Properties dialog box. |

Set ENABLE\_BROKER

Before you can run tasks and use the Discovery Wizard to install agents, you need to set the ENABLE\_BROKER value.

After moving the Operations Manager database, the status of the Sql Broker Availability Monitor might be set to Critical or Sql Broker is disabled. You can check the state of the Sql Broker Availability Monitor by running the following SQL query:

SELECT is\_broker\_enabled FROM sys.databases WHERE name='OperationsManager'

Where ‘OperationsManager’ is the default database name, replace this name as appropriate.

If the query result is ‘0’, the Sql Broker is disabled and you must re-enable it using the following procedure.

To set ENABLE\_BROKER

|  |
| --- |
| 1. Open SQL Server Management Studio.  2. In the Connect to Server dialog box, select the appropriate values in the Server type list, Server name list, and Authentication list, and then click Connect.  3. Click New Query.  4. In the query window, enter the following query:  ALTER DATABASE OperationsManager SET SINGLE\_USER WITH ROLLBACK IMMEDIATE  5. Click Execute.  6. Enter the following query:  ALTER DATABASE OperationsManager SET ENABLE\_BROKER  7. Click Execute.  8. Close SQL Server Management Studio.  Note  Closing SQL Server Management Studio closes the connection to the database in single-user mode. Depending on your configuration, you might have to manually stop any process that is connected to the database before completing the ALTER query below.  9. Open SQL Server Management Studio.  10. In the Connect to Server dialog box, select the appropriate values in the Server type list, Server name list, and Authentication list, and then click Connect.  11. Click New Query.  12. In the query window, enter the following query:  ALTER DATABASE OperationsManager SET MULTI\_USER  13. Click Execute. |

You can verify the setting for ENABLE\_BROKER is set to 1 by using this SQL query: SELECT is\_broker\_enabled FROM sys.databases WHERE name='OperationsManager'.

Note

Before you can use discovery, you must restart the following services: System Center Data Access, System Center Management Configuration, and System Center Management Services. You might also need to restart the following services: SQL Server and SQL Server Agent.

How to Move the OperationsManagerDW Database in Operations Manager 2007

For various reasons, it might be necessary to move the OperationsManagerDW database from its original server to another server.

Caution

This procedure can result in data loss if it is not performed correctly and within a reasonable length of time of the failure. Ensure that you follow all steps precisely, without unnecessary delays between the steps.

The high-level steps to move the OperationsManagerDW database are as follows:

1. Stop Microsoft System Center Operations Manager 2007 services to prevent updates to the OperationsManagerDW database during the move.

2. Back up the OperationsManagerDW database to preserve the data that Operations Manager has already collected from the management group.

3. Uninstall the current Data Warehouse component, and delete the OperationsManagerDW database.

4. Install the Reporting Data Warehouse component on the new Data Warehouse server.

5. Restore the original OperationsManagerDW database.

6. Configure Operations Manager to use the OperationsManagerDW database on the new Data Warehouse server.

7. Restart Operations Manager services.

OperationsManagerDW Database Relocation Procedure

Use the procedure below to move the OperationsManagerDW database to a new Data Warehouse server.

To move the OperationsManagerDW database

|  |
| --- |
| 1. Stop Operations Manager services as follows:  a. On the root management server, stop the System Center Data Access, and the System Center Management Configuration Services.  b. On the root management server and on all other management servers, stop the System Center Management Service.  2. On the current Data Warehouse server, use SQL Server Management Studio to back up the OperationsManagerDW database (default name) to a shared folder on the server. It is recommended that you also back up the associated master database.  3. On the current Data Warehouse server, uninstall the Reporting Data Warehouse component as follows:  a. Click Start, click Control Panel, and then select Add or Remove Programs if you are using Windows Server 2003 or select Programs and Features if you are using Windows Server 2008.  b. In the Add or Remove Programs for Windows Server 2003 or Programs and Features for Windows Server 2008, dialog box, select System Center Operations Manager 2007 R2 Reporting Server, and then select Change.  c. In the System Center Operations Manager 2007 Reporting Setup Wizard, on the Operations Manager 2007 R2 Maintenance page, select Modify, and then click Next.  d. On the Custom Setup page, configure the Data Warehouse component with the This component will not be available option.  e. Complete the wizard.  Note  This does not physically remove the OperationsManagerDW database from Microsoft SQL Server.  4. On the current Data Warehouse server, delete the OperationsManagerDW database as follows:  a. In Microsoft SQL Server Management Studio, navigate to Databases.  b. Right-click OperationsManagerDW, and then select Delete.  c. In the Delete Object dialog box, ensure that the Delete backup and restore history information for databases and Close existing connections options are both selected.  5. On the new Data Warehouse server, run SetupOM.exe to install the Reporting Data Warehouse component as follows:  a. On the System Center Operations Manager 2007 R2 Setup page, select Install Operations Manager 2007 R2 Reporting.  b. In the System Center Operations Manager 2007 R2 Reporting Setup Wizard, on the Custom Setup page, configure only the Data Warehouse component for installation.  If you are moving the OperationsManagerDW database to a server that is different than the server on which the Operations Manager Reporting component is installed, Configure the Reporting Server component with the This component will not be available option.  6. On the new Data Warehouse server, delete the OperationsManagerDW database as follows:  a. In Microsoft SQL Server Management Studio, navigate to Databases.  b. Right-click OperationsManagerDW, and then select Delete.  c. In the Delete Object dialog box, ensure that the Delete backup and restore history information for databases and Close existing connections options are both selected.  7. On the new Data Warehouse server, use SQL Management Studio to restore the OperationsManagerDW database backup (from step 2). Access the database backup by copying the backup to a local drive or by mapping a local drive to the folder that contains the backup.  8. On the new Data Warehouse server, use SQL Management Studio to create a login for the System Center Data Access Service account, the Data Warehouse Action Account, and the Data Reader Account.  Note  If localsystem was used as the System Center Data Access account, enter <domain\computername$> in SQL Logins.  9. On the new Data Warehouse server, add the correct login permission for the computer on which the SDK Service is running, as follows:  a. In Microsoft SQL Server Management Studio, in the Object Explorer pane, navigate to Security and then expand Logins.  b. Right-click the account that corresponds to the computer on which the SDK Service is running (for example, if localsystem is used, it will be <domain\computername$>). Select Properties.  c. In the Login Properties dialog box, in the Select a page pane, select User Mapping.  d. In the Users mapped to this login list, in the Map column, select the box that corresponds to the OperationsManagerDW database.  e. In the Database role membership for: OperationsManagerDW list, select OpsMgrReader and db\_datareader.  f. Click OK to save your changes and to close the Login Properties dialog box.  10. On the new Data Warehouse server, add the correct login permission for the computer on which the Data Reader Account is running, as follows:  a. In Microsoft SQL Server Management Studio, in the Object Explorer pane, navigate to Security and then expand Logins.  b. Right-click the Data Reader Account and select Properties.  c. In the Login Properties dialog box, in the Select a page pane, select User Mapping.  d. In the Users mapped to this login list, In the Map column, select the box that corresponds to OperationsManagerDW.  e. In the Database role membership for: OperationsManagerDW list, select OpsMgrReader and db\_datareader.  f. Click OK to save your changes and to close the Login Properties dialog box.  11. On the new Data Warehouse server, add the correct permission for the login of the computer on which the Data Warehouse Action Account is running, as follows:  a. In Microsoft SQL Server Management Studio, in the Object Explorer pane, navigate to Security and then expand Logins.  b. Right-click the Data Warehouse Action Account, and select Properties.  c. In the Login Properties dialog box, in the Select a page pane, select User Mapping.  d. In the Users mapped to this login list, in the Map column, select the box that corresponds to OperationsManagerDW.  e. In the Database role membership for: OperationsManagerDW list, select the following items: OpsMgrWriter and db\_owner.  f. Click OK to save your changes and to close the Login Properties dialog box.  12. On the root management server, start the System Center Data Access Service.  13. On the server running SQL Server Reporting Services, modify the data source as follows:  a. In Internet Explorer, open http://localhost/reports<$instancename> (include <$instancename> only when using a named instance).  b. On the SQL Server Reporting Services Home page, ensure that you are viewing the Contents page. Select Show Details.  c. In the list that is displayed, click Data Warehouse Main.  d. In the Data Warehouse Main properties page, in the Connection string text box, change the name of the database server to the new Data Warehouse server.  e. Click Apply.  14. On the server running SQL Server Reporting Services, update the registry to point to the name of the new Data Warehouse server as follows:  a. Locate the key HKEY\_LOCAL\_MACHINE\Software\Microsoft\Microsoft Operations Manager\3.0\Reporting.  b. Double-click the value DWDBInstance, and then modify it to be the name of the new Data Warehouse server.  If the OperationsManagerDW database was installed on the same server as the Operations Manager Reporting Server, this key does not exist and you need to add it (as a string value).  15. Configure the Operations Manager database with the name of the new Data Warehouse server as follows:  a. On the server that hosts the Operations Manager database, open SQL Server Management Studio and navigate to Databases, OperationsManager, and then to Tables.  b. Right-click dbo.MT\_DataWarehouse, and then select Open Table if you are using SQL Server 2005 or select Edit Top 200 Rows if you are using SQL Server 2008.  c. Change the value in the MainDatabaseServerName\_16781F33\_F72D\_033C\_1DF4\_65A2AFF32CA3 column to the name of the new Data Warehouse server.  d. Close SQL Server Management Studio to save your changes.  16. Configure the OperationsManagerDW database with the name of the new Data Warehouse server as follows:  a. On the new Data Warehouse server, open SQL Server Management Studio and navigate to Databases, OperationsManagerDW, and then to Tables.  b. Right-click dbo.MemberDatabase table and select Open Table if you are using SQL Server 2005 or select Edit Top 200 Rows if you are using SQL Server 2008.  c. Change the value in the ServerName column to the name of the new Data Warehouse server.  d. Close SQL Server Management Studio to save your changes.  17. Restart services as follows:  a. On the root management server, restart the System Center Management Configuration Service.  b. On all management servers, restart the System Center Management Service.  18. Verify that the database move was successful as described in the following procedures. |

To verify a successful move of the OperationsManagerDW database

|  |
| --- |
| 1. Verify that you can successfully run a report from the console.  2. Ensure that the health state of all management servers in the management group are Healthy.  If the health state of any management server is Critical, open Health Explorer, expand Availability - <server name>, and then continue to expand until you can navigate to Data Warehouse SQL RS Deployed Management Pack List Request State. Check the associated events to determine if there is an issue accessing the OperationsManagerDW database.  3. Check operating system events:  a. Open the operating system's Event viewer. Navigate to Event Viewer, and then to Operations Manager.  b. In the Operations Manager pane, search for events with a Source of Health Service Module and a Category of Data Warehouse.  The move was successful if event number 31570, 31558, or 31554 exists.  There is an issue accessing the OperationsManagerDW database if event numbers 31563, 31551, 31569, or 31552 exists.  4. Check events in Operations Manager:  a. In the Operations console, select Monitoring.  b. Navigate to Monitoring, Operations Manager, Health Service Module Events, and then to Performance Data Source Module Events.  c. Search the Performance Data Source Module Events pane for events with a Date and Time that is later than the move.  There is a problem with the OperationsManagerDW database if events have a Source of Health Service Module and an Event Number of 10103. |

How to Move the OperationsManagerAC Database in Operations Manager 2007

For various reasons, it might be necessary to move the Audit Collection (OperationsManagerAC) database from its original server to another server.

Caution

This procedure can result in data loss if it is not performed correctly and within a reasonable length of time. Ensure that you follow all steps precisely, and without unnecessary delays between steps.

The high-level steps for moving the OperationsManagerAC database are as follows:

1. Stop Operations Manager Audit Collection Service (ACS) to prevent updates to the OperationsManagerAC database during the move.

2. Back up the OperationsManagerAC database.

3. Delete the OperationsManagerAC database on the original Audit Collection database server.

4. Restore the OperationsManagerAC database to the new Audit Collection database server.

5. Configure SQL Server permissions on the new Audit Collection database server.

6. Configure the Audit Collection Server to point to the new Audit Collection database server.

7. Restart Operations Manager Audit Collection Service.

OperationsManagerAC Database Relocation Procedure

Use the following procedure to move the OperationsManagerAC database to a new Audit Collection database server.

To move the OperationsManagerAC database

|  |
| --- |
| 1. On the original Audit Collection database server, stop Operations Manager Audit Collection Service.  2. On the original Audit Collection database server, use Microsoft SQL Server Management Studio to back up the OperationsManagerAC database (default name) to a shared folder on the server. It is recommended that you also back up the associated master database.  3. On the original Audit Collection database server, delete the OperationsManagerAC database as follows:  a. In SQL Server Management Studio, navigate to Databases.  b. Right-click OperationsManagerAC, and then select Delete.  c. In the Delete Object dialog box, ensure that the Delete backup and restore history information for databases and the Close existing connections options are both selected.  4. On the new Audit Collection database server, use SQL Management Studio to restore the OperationsManagerAC database backup. Access the database backup by copying the backup file to a local drive or by mapping a local drive to the folder that contains the backup.  5. On the new Audit Collection database server, use SQL Management Studio to create a login for the Audit Collection Service server. Use the format <domain\computername$> in SQL Logins (where computername is the name of the Audit Collection Service server).  6. On the new Audit Collection database server, add the correct permission for the login of the computer on which the ACS Service is running, as follows:  a. In SQL Server Management Studio, navigate to Security and then to Logins.  b. Right-click the account that corresponds to the computer on which the ACS service is running (use the <domain\computername$> format). Select Properties, and then select User Mapping.  c. Select the box in the Map column that corresponds to the OperationsManagerAC database, and then select db\_owner in the Database role membership for: OperationsManagerAC list.  d. Click OK.  7. On the computer hosting Audit Collection Service, locate the registry key HKEY\_LOCAL\_MACHINE\Software\ODBC\ODBC.INI\OpsMgrAC. Double-click the value Server, and set it to the name of the new Audit Collection Service database server.  8. On the server on which the ACS service is running, start Audit Collection Service.  9. Verify that the database move was successful by checking the OperationsManagerAC database for entries in the most recent dtEvent\_<GUID> table that have a date/time stamp that is more recent than when the service was restarted in the previous step. |

How to Promote a Management Server to a Root Management Server Role in Operations Manager 2007

Use the following procedures to promote a management server to a root management server role, and then, if needed, to reset the value of ENABLE\_BROKER in the Operations Manager database to 1.

Some of the high-level guidelines for promoting management servers are:

 In a failure recovery scenario, you can change the root management server by promoting another management server to the role of root management server. In this scenario, the management server that you plan to promote to root management server must have already been installed before the failure of the current root management server occurred.

 If you promote the root management server role away from a clustered root management server, you must ensure that the services (the System Center Management Service, System Center Management Configuration Service, and System Center Data Access Service) for that clustered root management server are offline. These services might be already stopped (for example, as a result of the clustered root management server no longer being in operation). However, if these services are still running, you must manually stop them from within Cluster Administrator if you are using Windows Server 2003 or Failover Cluster Management if you are using Windows Server 2008.

 For clustered Operations Manager 2007 SP1, never let the HealthService run on any node of the clustered RMS while the another management server is promoted to the RMS role.

 For clustered Operations Manager 2007 R2, never let the System Center Management service run on any node of the clustered RMS while another management server is promoted to the RMS role.

 After promoting the root management server role away from a clustered root management server, you cannot configure the individual nodes as management servers. This scenario is not supported, and therefore you should not use the UpdateDemotedRMS action on these nodes. If you will not be using the cluster again, uninstall all Operations Manager 2007 components from the cluster node computers

 In Operations Manager 2007 SP1, it is possible to promote the root management server back to the original clustered root management server configuration. To do this, you must first ensure that the cluster RMS group (Windows Server 2003) or Service or Application (Windows Server 2008) is offline, and then perform the PromoteRMS action on the active node of the cluster. Failure to take the cluster resources offline will result in corrupting your OperationsManager database

 In a scenario where a management server was promoted to root management server and the original root management server was not demoted at that time, (for various reasons such as connectivity issues or hardware problems with the computer), if at a later time the original server recovers and you want to use it again as the root management server, you must first demote it to a management server role. You must do this because you have already promoted another management server to a root management server role.

After you demote the original root management server to a management server role by running the UpdateDemotedRMS action of the ManagementServerConfigTool locally on that original root management server, you can re-promote it to the root management server role.

Note

Running the PromoteRMS action automatically demotes the previous root management server to a management server role unless the original root management server is not accessible or if /DemoteExistingRMS: is set to ‘True’ (which will delete, rather than demote, the previous root management server from the database).

The high-level steps for promoting a management server to root management server are:

1. Promote a management server to a root management server role.

2. Configure the reporting server with the name of the new root management server.

3. Configure the Web console with the name of the new root management server.

4. Set ENABLE\_BROKER to 1 if needed. After you successfully complete the promotion, you might need to set the value of the SQL Broker Availability Monitor to 1. Check the state of the SQL Broker Availability Monitor by running the following SQL query:

SELECT is\_broker\_enabled FROM sys.databases WHERE name='OperationsManager'

If the query result is ‘0’, the SQL Broker is disabled and you must re-enable it by using the 'To set ENABLE\_BROKER to 1' procedure later in this topic.

To promote a management server to a root management server role

|  |
| --- |
| 1. On the management server that you want to promote, copy the ManagementServerConfigTool.exe tool from the SupportTools folder of the installation media to the installation folder (by default, C:\Program Files\System Center Operations Manager 2007), called installdir in this example.  2. Open a command prompt window using the Run as Administrator option, and then change the folder to the installdir folder.  3. Type the following command:  SecureStorageBackup.exe Restore <filename>  Here, filename is the root management server encryption key backup file.  4. Provide a password as required.  5. On the management server, open a command prompt window using the Run as Administrator option, and then type the following command:  ManagementServerConfigTool.exe PromoteRMS  6. You will see two warnings come up. The first warns you to backup your OperationsManager database, the second warns you to take the System Center Management, System Center Management Configuration and System Center Data Access services offline if your RMS is on a cluster. Type in Y for both.  7. Demote the original root management server to a management server by doing the following on the original root management server:  Note  This step is required only if the original root management server is to be used as a management server.  a. Type the following command: ManagementServerConfigTool.exe UpdateDemotedRMS. Type in Y to the backup database warning.  b. Delete the existing subfolders of the Health Service State folder in the installdir. |

To configure the reporting server with the name of the new root management server

|  |
| --- |
| 1. Log on to the reporting server.  2. Navigate to the installation folder of Reporting Services for example, %ProgramFiles%\Microsoft SQL Server\MSSQL.2\Reporting Services\ReportServer if you are using SQL Server 2005 or %ProgramFiles%\Microsoft SQL Server\MSRS10.MSSQLSERVER\Reporting Services\ReportServer if you are using SQL Server 2008.  3. Open the rsreportserver.config file in Notepad, and locate the two instances of <ServerName>ServerName</ServerName>, where ServerName is the name of the original root management server. Change ServerName to be the name of the new root management server.  4. Save the file, and then close Notepad.  5. Open the registry and locate the key HKEY\_LOCAL\_MACHINE\Software\Microsoft\Microsoft Operations Manager\3.0\Reporting.  6. Change the DefaultSDKServiceMachine value to be the name of the new root management server. |

To configure the data warehouse server with permissions for the new root management server

|  |
| --- |
| 1. On the server hosting the data warehouse, open Microsoft SQL Server Management Studio, and in the Object Explorer pane, navigate to Security and then expand Logins.  2. Locate the account that corresponds to the new root management server and on which the System Center Data Access Service is running (if it’s running under LocalSystem, the format is <domain\computername$>).  3. Right-click the account and select Properties.  4. In the Login Properties dialog box, in the Select a page pane, select User Mapping.  5. In the Users mapped to this login list, in the Map column, select the box that corresponds to the OperationsManagerDW database.  6. In the Database role membership for: OperationsManagerDW list, ensure that the following items are selected: configsvc\_users, db\_datareader, db\_datawriter, db\_ddladmin, and sdk\_users.  7. Click OK to save your changes and to close the Login Properties dialog box. |

To configure the Web console with the name of the new root management server

|  |
| --- |
| 1. Log on to the Web console server.  2. Navigate to the installation folder of the Web console (by default, %ProgramFiles%\System Center Operations Manager 2007\Web Console).  3. Open the Web.config file in Notepad.  4. Locate the line ‘<add key="MOMServer" value="RootManagementServer "/>’, where RootManagementServer is the name of the original root management server. Change RootManagementServer to be the name of the new root management server.  5. Save your changes, and then close Notepad. |

To set ENABLE\_BROKER to 1

|  |
| --- |
| 1. Open SQL Server Management Studio.  2. In the Connect to Server dialog box, select the appropriate values in the Server type list, in the Server name list, and in the Authentication list, and then click Connect.  3. Click New Query.  4. In the query window, enter the following query:  ALTER DATABASE OperationsManager SET SINGLE\_USER WITH ROLLBACK IMMEDIATE  5. Click Execute.  6. Enter the following query:  ALTER DATABASE OperationsManager SET ENABLE\_BROKER  7. Click Execute.  8. In the Connect to Server dialog box, select the appropriate values in the Server type list, in the Server name list, and in the Authentication list, and then click Connect.  9. Click New Query.  10. In the query window, enter the following query:  ALTER DATABASE OperationsManager SET MULTI\_USER  11. Click Execute.  12. Verify that ENABLE\_BROKER is set to 1 by using the following SQL query:  Select is\_broker\_enabled FROM sys.databases WHERE name='OperationsManager' |

How to Remove a Management Server From a Computer in Operations Manager 2007

Use the following procedure to remove the management server role from a computer. For example, you might need to do this if you need to free up a computer hosting the management server role and install a gateway server.

Before you remove the management server role from a computer, you must configure any objects that are managed by that management server, to be managed by a different management server as described below.

The high level steps to remove a management server role are as follows:

1. [Delete the Management Server](#z11) from the management group.

2. If the management server you are about to remove functions as a primary management server for an agent, then you must configure those agents to use a new primary management server. See [Change the Primary Management Server](#z12) below.

3. If the management server you are about to remove acts as a proxy agent for an agentless managed computer, you need to identify a new management server. See [Configure an Agentless Managed Computer to Use a Different Proxy Agent](#z13) below.

4. If the management server you are about to remove acts as a proxy agent for a network device, you need to identify a new management server. See [Configure a Network Device to Use a Different Operations Manager 2007 Proxy Agent](#z14) below.

5. Remove the management server role from a computer. See [Remove the Management Server from a Computer](#z15) below.

Procedures

To delete a management server from the management group

|  |
| --- |
| 1. Open the Operations console with an account that is a member of the Operations Manager 2007 Administrator role for the management group.  2. In the Operations console, click the Administration button.  Note  When you run the Operations console on a computer that is not a Management Server, the Connect To Server dialog box will display. Type the name of the Operations Manager 2007 management server you want the Operations console to connect to in the Server name text box.  3. In the Administration pane, click Management Servers.  4. Right-click the desired management server and click delete.  5. In the Confirm Delete Management Server dialog, click Yes. |

Change the Primary Management Server

Use the following procedure to change the primary management server for agent-managed computers that are assigned to Primary and Secondary management servers without using Active Directory Domain Services.

To change the Primary Management Server for agent-managed computers using the Operations console

|  |
| --- |
| 1. Open the Operations console with an account that is a member of the Operations Manager 2007 Administrator role for the management group.  2. In the Operations console, click the Administration button.  Note  When you run the Operations console on a computer that is not a management server the Connect To Server dialog box will display. In the Server name text box, type the name of the Operations Manager 2007 management server that you want the Operations console to connect to.  3. In the Administration pane, expand Administration, expand Device Management, and then click Agent Managed.  4. In the Agent Managed pane, select the computers for which you want to change the Primary management server, right-click them, and then select Change Primary Management Server .  Note  The Change Primary Management Server option will be unavailable if Active Directory Domain Services was used to assign any of the selected computers to the management group.  5. In the Change Management Server dialog box, select the desired management server from the list, and then click OK. The change takes effect on the agent after its next update interval. |

Configure an Agentless Managed Computer to Use a Different Proxy Agent

Use the following procedure to change the Operations Manager 2007 proxy agent for an agentless managed computer. The proxy agent can be any agent-managed computer in the management group configured to be a proxy.

To change the proxy agent for agentless managed computers

|  |
| --- |
| 1. Open the Operations console with an account that is a member of the Operations Manager Administrators role.  2. In the Operations console, click the Administration button.  Note  When you run the Operations console on a computer that is not a management server the Connect To Server dialog box displays. In the Server name text box, type the name of the Operations Manager 2007 management server that you want the Operations console to connect to.  3. In the Administration pane, expand Administration, expand Device Management, and then click Agentless Managed.  4. In the Agentless Managed pane, select the agentless managed computers for which you want to change the proxy agent, right-click them, and then select Change Proxy Agent .  5. In the Change Proxy Agent dialog box, select the computer you want to be the new proxy agent, and then click OK. |

Configure a Network Device to Use a Different Operations Manager 2007 Proxy Agent

Use the following procedure to change the Operations Manager 2007 proxy agent for network devices. The proxy agent can be any agent-managed computer in the management group. It must have SNMP installed, an optional Windows component, and be able to connect to the devices using SNMP.

To change the proxy agent for network devices

|  |
| --- |
| 1. Open the Operations console with an account that is a member of the Operations Manager Administrators role.  2. In the Operations console, click the Administration button.  Note  When you run the Operations console on a computer that is not a management server the Connect To Server dialog box displays. In the Server name text box, type the name of the Operations Manager 2007 management server that you want the Operations console to connect to.  3. In the Administration pane, expand Administration, expand Device Management, and then click Network Devices.  4. In the Network Devices pane, select the network devices for which you want to change the proxy agent, right-click them, and then select Change Proxy Agent .  5. In the Change Proxy Agent dialog box, select the computer you want to be the new proxy agent, and then click OK. |

Remove the Management Server from a Computer

Use the following procedure to remove a management server role from a computer.

To remove a management server role from a computer

|  |
| --- |
| 1. Run Add or Remove Programs if you are using Windows Server 2003 or Programs and Features if you are using Windows Server 2008 on the computer you want to remove the management server component from.  2. Select System Center Operations Manager 2007 R2, click Change or Remove, and then follow the instructions in the wizard. |

How to Move the Operations Manager Reporting Server in Operations Manager 2007

You can move the Microsoft System Center Operations Manager 2007 reporting server component to a new server, or reinstall the component on the original server.

Important

Moving a reporting server is supported only on the Service Pack 1 or R2 version of System Center Operations Manager 2007.

The high-level steps of moving the Operations Manager reporting server are as follows:

1. Back up the OperationsManagerDW database.

2. Note the accounts that are being used for the Data Warehouse Action Account and for the Data Warehouse Report Deployment Account. You will need to use the same accounts later, when you reinstall the Operations Manager reporting server.

3. Uninstall the current Operations Manager reporting server component.

4. Restore the original OperationsManagerDW database.

5. If you are reinstalling the Operations Manager reporting server component on the original server, run the ResetSRS.exe tool to clean up and prepare the reporting server for the reinstallation.

6. Reinstall the Operations Manager reporting server component.

During this move, Operations Manager stops storing data in the OperationsManagerDW database until you complete the Operations Manager reporting server reinstall.

Use the procedures in this topic to move the reporting server to a new server and verify the success of the move. You must back up any custom reports that were authored outside of Operations Manager 2007. For more information about this, see [Moving the Report Server Databases to Another Computer](http://go.microsoft.com/fwlink/?LinkId=151513) in the SQL Server 2008 Books Online (http://go.microsoft.com/fwlink/?LinkId=151513).

Note

Ensure that you follow all steps precisely, as not doing so might result in data corruption.

To move the Operations Manager reporting server

|  |
| --- |
| 1. On the current Data Warehouse server, use SQL Server Management Studio to back up the OperationsManagerDW database (default name).  2. On the current Operations Manager reporting server computer, uninstall the Operations Manager reporting server component as follows:  a. Click Start, click Control Panel, and then click Add or Remove Programs if you are using Windows Server 2003, or click Programs and Features if you are using Windows Server 2008.  b. In the Add or Remove Programs or Programs and Features dialog box, select System Center Operations Manager 2007 R2 Reporting Server, and then select Change.  c. In the System Center Operations Manager 2007 R2 Reporting Setup Wizard, on the Operations Manager 2007 R2 Maintenance page, select Modify, and then click Next.  d. On the Custom Setup page, configure the Reporting Server component with the This component will not be available option.  e. Complete the wizard.  3. On the Data Warehouse server, use SQL Management Studio to restore the OperationsManagerDW database backup that you created in step 1.  4. If you are reinstalling the Operations Manager reporting server component on the original server, you must remove any data that is left from the original installation by doing the following:  a. Copy the ResetSRS.exe tool from the SupportTools folder on the product CD to a local folder.  b. Open a command prompt window using the Run as Administrator option and run the tool as follows:  ResetSRS.exe <SQL Server instance name>  Here, SQL Server instance name is the SQL Server instance that SQL Reporting Services is installed on, such as 'Instance1'.  If SQL Server is using the default instance, enter MSSQLSERVER.  c. Open the Reporting Configuration Manager by clicking Start, pointing to Programs, pointing to Microsoft SQL Server 2005 or Microsoft SQL Server 2008, pointing to Configuration Tools, and then clicking Reporting Services Configuration.  d. For SQL Reporting Services 2005, in the Configure Report Server page, check the status of the Web Service Identity item. If the status is not Configured (green), click that item, and then click Apply.  Check the status of the rest of the items on that page. Configure any items that are designated with a red ‘X’, indicating an unhealthy configuration status.  5. For SQL Server Reporting Services 2008, confirm the correct configuration of SQL Server 2008 Reporting Services. Click Start, point to Programs, point to Microsoft SQL Server 2008, point to Configuration Tools, and click Reporting Services Configuration Manager. Connect to the instance that you installed Reporting Services on.  6. In the left pane, select the <servername>\SQLinstance. This displays the Report Server status in the results pane. Ensure that the Report Server Status is Started.  7. In the left pane, select Scale-out Deployment and ensure that the Status column has the value of Joined .  8. If Report Server is not started and the Scale out Deployment is not joined, check the configuration of Service Account, Web Service URL, and Database.  9. Confirm that the SQL Server Reporting Services service is running. In Server Manager, expand the Configuration container for Windows Server 2008 or Services for Windows Server 2003 and select Services.  10. In the Name column, find the SQL Server Reporting Services instance service and confirm that its status reads Started and that its Startup Type is Automatic.  11. On the new Operations Manager reporting server computer, run SetupOM.exe to reinstall the Operations Manager reporting server component by pointing the reporting server to the existing OperationsManagerDW database and using the original accounts for the Data Warehouse Action Account and the Data Warehouse Report Deployment Account, as follows:  a. On the System Center Operations Manager 2007 R2 Setup page, select Install Operations Manager 2007 R2 Reporting.  b. In the System Center Operations Manager 2007 R2 Reporting Setup Wizard, on the Custom Setup page, configure only the Reporting Server component for installation. Configure the Data Warehouse component with the This component will not be available option.  12. Verify that the database move was successful as described in the next procedure. |

To verify a successful move of the reporting server

|  |
| --- |
| 1. Verify that you can successfully run a report from the Operations Manager Operations console.  2. Ensure that the health state of all management servers in the management group is Healthy.  If the health state of any management server is Critical, open Health Explorer, expand Availability - <server name>, and then continue to expand until you can navigate to Data Warehouse SQL RS Deployed Management Pack List Request State. Check the associated events to determine if there is an issue accessing the OperationsManagerDW database. |

Appendix A - Cross Platform Operating System Package Dependencies

The following tables describe the required UNIX and Linux operating systems and package dependencies.

IBM AIX 5L 5.3

|  |  |  |
| --- | --- | --- |
| Required Package | Description | Minimum Version |
| OS version | Version of the operating system | AIX 5.3, Technology Level 6, Service Pack 5 |
| xlC.rte | XL C/C++ Runtime | 9.0.0.2 |
| openssl.base | OpenSSL Libraries; Secure Network Communications Protocol | 0.9.8.4 |

IBM AIX 6.1

|  |  |  |
| --- | --- | --- |
| Required Package | Description | Minimum Version |
| OS version | Version of operating system | AIX 6.1, any Technology Level and Service Pack |
| xlC.rte | XL C/C++ Runtime | 9.0.0.5 |
| OpenSSL/openssl.base | OpenSSL Libraries; Secure Network Communications Protocol | 0.9.8.4 |

HP-UX 11i v2 IA 64

|  |  |  |
| --- | --- | --- |
| Required Package | Description | Minimum Version |
| HPUXBaseOS | Base OS | B.11.23 |
| HPUXBaseAux | HP-UX Base OS Auxiliary | B.11.23.0706 |
| HPUXBaseAux.openssl | OpenSSL Libraries; Secure Network Communications Protocol | A.00.09.07l.003 |
| PAM | Pluggable Authentication Modules | On HP-UX, PAM is part of the core operating system components. There are no other dependencies. |

HP-UX 11i v2 PA-RISC

|  |  |  |
| --- | --- | --- |
| Required Package | Description | Minimum Version |
| HPUX11i-OE | HP-UX Foundation Operating Environment | B.11.23.0706 |
| OS-Core.MinimumRuntime.CORE-SHLIBS | Compatible development tools libraries | B.11.23 |
| HPUXBaseAux | HP-UX Base OS Auxiliary | B.11.23.0706 |
| HPUXBaseAux.openssl | OpenSSL Libraries; Secure Network Communications Protocol | A.00.09.071.003 |
| PAM | Pluggable Authentication Modules | On HP-UX, PAM is part of the core operating system components. There are no other dependencies. |

HP-UX 11i v3 PA-RISC

|  |  |  |
| --- | --- | --- |
| Required Package | Description | Minimum Version |
| HPUX11i-OE | HP-UX Foundation Operating Environment | B.11.31 |
| OS-Core.MinimumRuntime.CORE2-SHLIBS | Specific IA emulator libraries | B.11.31 |
| openssl/Openssl.openssl | OpenSSL Libraries; Secure Network Communications Protocol | A.00.09.08d.002 |
| PAM | Pluggable Authentication Modules | On HP-UX, PAM is part of the core operating system components. There are no other dependencies. |

HP-UX 11i v3 IA64

|  |  |  |
| --- | --- | --- |
| Required Package | Description | Minimum Version |
| HPUX11i-OE | HP-UX Foundation Operating Environment | B.11.31.0709 |
| OS-Core.MinimumRuntime.CORE-SHLIBS | Specific IA development libraries | B.11.31 |
| SysMgmtMin | Minimum Software Deployment Tools | B.11.31.0709 |
| SysMgmtMin.openssl | OpenSSL Libraries; Secure Network Communications Protocol | A.00.09.08d.002 |
| PAM | Pluggable Authentication Modules | On HP-UX, PAM is part of the core operating system components. There are no other dependencies. |

Red Hat Enterprise Linux ES Release 4

|  |  |  |
| --- | --- | --- |
| Required Package | Description | Minimum Version |
| glibc | C Standard Libraries | 2.3.4-2 |
| Openssl | OpenSSL Libraries; Secure Network Communications Protocol | 0.9.7a-43.1 |
| PAM | Pluggable Authentication Modules | 0.77-65.1 |

Red Hat Enterprise Linux Server release 5.1 (Tikanga)

|  |  |  |
| --- | --- | --- |
| Required Package | Description | Minimum Version |
| glibc | C Standard Libraries | 2.5-12 |
| Openssl | OpenSSL Libraries; Secure Network Communications Protocol | 0.9.8b-8.3.el5 |
| PAM | Pluggable Authentication Modules | 0.99.6.2-3.14.el5 |

Solaris 8 SPARC

|  |  |  |
| --- | --- | --- |
| Required Package | Description | Minimum Version |
| Required OS patch | PAM memory leak | 108434-22 |
| SUNWlibC | Sun Workshop Compilers Bundled libC (sparc) | 5.8,REV=99.06.09 |
| SUNWlibms | Sun Workshop Bundled Shared libm (sparc) | 5.8,REV=99.10.21 |
| OpenSSL | SMCossl (sparc)  Sun does not provide a version of OpenSSL for Solaris 9 SPARC. There is a version available from Sunfreeware. | 0.9.8h |
| PAM | Pluggable Authentication Modules  SUNWcsl, Core Solaris, (Shared Libs) (sparc) | 11.8.0,REV=2000.01.08.18.12 |

Solaris 9 SPARC

|  |  |  |
| --- | --- | --- |
| Required Package | Description | Minimum Version |
| Required OS patch | PAM memory leak | 112960-48 |
| SUNWlibC | Sun Workshop Compilers Bundled libC (sparc) | 5.9,REV=2002.03.18 |
| SUNWlibms | Forte Developer Bundled Shared libm (sparc) | 5.9,REV=2001.12.10 |
| OpenSSL | SMCosslg (sparc)  Sun does not provide a version of OpenSSL for Solaris 9 SPARC. There is a version available from Sunfreeware. | 0.9.7g |
| PAM | Pluggable Authentication Modules  SUNWcsl, Core Solaris, (Shared Libs) (sparc) | 11.9.0,REV=2002.04.06.15.27 |

Solaris 10 SPARC

|  |  |  |
| --- | --- | --- |
| Required Package | Description | Minimum Version |
| Required OS patch | PAM memory leak | 117463-05 |
| SUNWlibC | Sun Workshop Compilers Bundled libC (sparc) | 5.10, REV=2004.12.22 |
| SUNWlibms | Math & Microtasking Libraries (Usr) (sparc) | 5.10, REV=2004.11.23 |
| SUNWlibmsr | Math & Microtasking Libraries (Root) (sparc) | 5.10, REV=2004.11.23 |
| SUNWcslr | Core Solaris Libraries (Root) (sparc) | 11.10.0, REV=2005.01.21.15.53 |
| SUNWcsl | Core Solaris Libraries (Root) (sparc) | 11.10.0, REV=2005.01.21.15.53 |
| OpenSSL | SUNopenssl-librararies (Usr)  Sun provides the OpenSSL libraries for Solaris 10 SPARC. They are bundled with the operating system. | 11.10.0,REV=2005.01.21.15.53 |
| PAM | Pluggable Authentication Modules  SUNWcsr, Core Solaris, (Root) (sparc) | 11.10.0, REV=2005.01.21.15.53 |

Solaris 10 x86

|  |  |  |
| --- | --- | --- |
| Required Package | Description | Minimum Version |
| Required OS patch | PAM memory leak | 117464-04 |
| SUNWlibC | Sun Workshop Compilers Bundled libC (i386) | 5.10,REV=2004.12.20 |
| SUNWlibmsr | Math & Microtasking Libraries (Root) (i386) | 5.10, REV=2004.12.18 |
| SUNWcsl | Core Solaris, (Shared Libs) (i386) | 11.10.0,REV=2005.01.21.16.34 |
| SUNWcslr | Core Solaris Libraries (Root) (i386) | 11.10.0, REV=2005.01.21.16.34 |
| OpenSSL | SUNWopenssl-libraries; OpenSSL Libraries (Usr) (i386) | 11.10.0, REV=2005.01.21.16.34 |
| PAM | Pluggable Authentication Modules  SUNWcsr Core Solaris, (Root)(i386) | 11.10.0,REV=2005.01.21.16.34 |

SUSE Linux Enterprise Server 9 (i586)

|  |  |  |
| --- | --- | --- |
| Required Package | Description | Minimum Version |
| OS Patch lib gcc-41.rpm | Standard shared library | 41-4.1.2\_20070115-0.6 |
| OS Patch lib stdc++-41.rpm | Standard shared library | 41-4.1.2\_20070115-0.6 |
| Openssl | OpenSSL Libraries; Secure Network Communications Protocol | 0.9.7d-15.10 |
| PAM | Pluggable Authentication Modules | 0.77-221.1 |

SUSE Linux Enterprise Server 10 SP1 (i586)

|  |  |  |
| --- | --- | --- |
| Required Package | Description | Minimum Version |
| glibc-2.4-31.30 | C Standard shared library | 2.4-31.30 |
| OpenSSl | OpenSSL Libraries; Secure Network Communications Protocol | 0.9.8a-18.15 |
| PAM | Pluggable Authentication Modules | 0.99.6.3-28.8 |