CHAPTER 23

Integrating System Center Operations Manager 2007 R2 with Windows Server 2008 R2

IN THIS CHAPTER

System Center Operations Manager (OpsMgr) 2007 R2 provides the best-of-breed approach to monitoring and managing Windows Server 2008 R2 within the environment. OpsMgr helps to identify specific environmental conditions before they evolve into problems through the use of monitoring and alerting components.

OpsMgr provides a timely view of important Windows Server 2008 R2 conditions and intelligently links problems to knowledge provided within the monitoring rules. Critical events and known issues are identified and matched to technical reference articles in the Microsoft Knowledge Base for troubleshooting and quick problem resolution.

The monitoring is accomplished using standard operating system components such as Windows Management Instrumentation (WMI), Windows event logs, and Windows performance counters, along with Windows Server 2008 R2 specific API calls and scripts. OpsMgr-specific components are also designed to perform synthetic transaction and track the health and availability of network services. In addition, OpsMgr provides a reporting feature that allows administrators to track problems and trends occurring on the network. Reports can be generated automatically, providing network administrators, managers, and decision makers with a current and long-term historical view of environmental trends. These reports can be delivered via email or stored on file shares for archive to power web pages.

The following sections focus on defining OpsMgr as a monitoring system for Windows Server 2008 R2. This chapter provides specific analysis of the way OpsMgr operates and presents OpsMgr design best practices, specific to deployment for Windows Server 2008 R2 monitoring.

Windows Server 2008 R2 Monitoring

The Operations Manager 2007 R2 monitoring is organized into management packs (MPs) for ease of installation and versioning. The Operations Manager 2007 R2 includes some of the best management packs for monitoring and maintaining Windows Server 2008 R2. These include the following:

- Windows Server Operating System MPs
- Active Directory Server MPs
- Windows Cluster Management MPs
- Microsoft Windows DNS Server MPs
- Microsoft Windows DHCP Server MPs
- Microsoft Windows Group Policy MPs
- Microsoft Windows Hyper-V MPs
- Windows Server Internet Information Services MPs
- Windows Server Network Load Balancing MPs
- Windows Server Print Server MPs
- Windows Terminal Services MPs

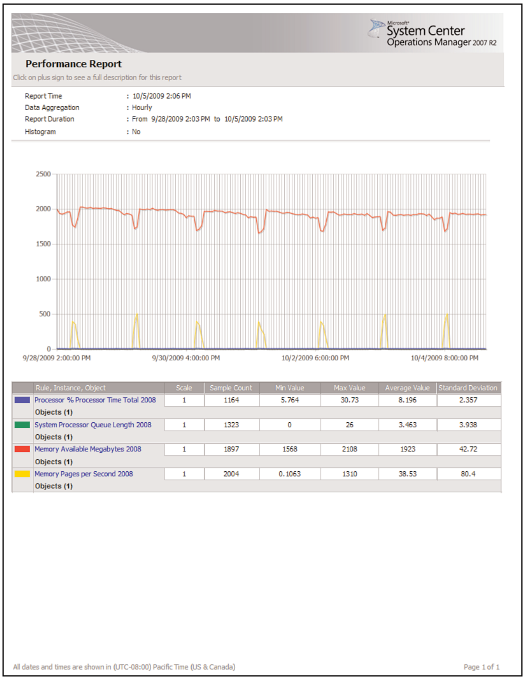
Each of the preceding categories includes several different management packs to support monitoring, discovery, and libraries. These management packs were developed by the product groups and include deep knowledge about the product.

The features of the management packs for the following major systems are as follows:

- **Windows Operating System Management Pack—**Monitors and alerts all the major elements that Windows Server 2008 R2 runs on, including processor, memory, network, disk, and event logs. It gathers performance metrics and alerts on thresholds, as well as critical events.
- **Active Directory Management Pack—**Monitors and alerts on Active Directory key metrics, such as replication latency, domain controller response times, and critical events. The management pack generates synthetic transactions to test the response time of the PDC, LDAP, and other domain services.
- **DNS Management Pack—**Monitors and alerts on DNS servers for resolution failures and latency as well as critical events.
- **IIS Management Pack—**Monitors and alerts on IIS services, application pools, performance, and critical events.

On all these elements, administrators can generate Availability reports to ensure that the servers and systems are meeting the service-level agreements (SLAs) set by the organization.

The management pack includes a comprehensive set of reports that are specific to Windows Server 2008 R2. These include reports on performance, availability, events, and even configuration for the various Windows Server 2008 R2 roles. These reports can be generated ad hoc, scheduled for email delivery on a regular basis, or even generated into web pages for portal viewing. Figure 23.1 shows a Performance report for a server. The report shows that processor utilization is low and that memory utilization is steady, with regular skips of activity in the pages per sec, which correspond to available memory dips.



Performance Report

Click on plus sign to see a full description for this report

Report Time	: 10/5/2009 2:06 PM
Data Aggregation	: Hourly
Report Duration	: From 9/28/2009 2:03 PM to 10/5/2009 2:03 PM
Histogram	: No

	Rule, Instance, Object	Scale	Sample Count	Min Value	Max Value	Average Value	Standard Deviation
🟦	Processor % Processor Time Total 2008	1	1164	5.764	30.73	8.196	2.357
	Objects (1)						
🟩	System Processor Queue Length 2008	1	1323	0	26	3.463	3.938
	Objects (1)						
🟥	Memory Available Megabytes 2008	1	1897	1568	2108	1923	42.72
	Objects (1)						
🟨	Memory Pages per Second 2008	1	2004	0.1063	1310	38.53	80.4
	Objects (1)						

All dates and times are shown in (UTC-08:00) Pacific Time (US & Canada)

Page 1 of 1

FIGURE 23.1 Sample Performance report.

This kind of summary Performance report is invaluable to reporting on the Windows Server 2008 R2 infrastructure and really ties together the low-level technical monitoring into a high-level view that support personnel can use.

What's New in OpsMgr R2

System Center Operations Manager 2007 R2 was released in the spring of 2009 and includes many new improvements on the previous version, Operations Manager 2007 Service Pack 1. Some of these improvements include the following:

- **Cross-platform support—**This is support for non-Microsoft platforms, such as UNIX and Linux. This allows administrators to have a single-pane view of their entire IT environment in OpsMgr.
- **Integration with System Center Virtual Machine Manager 2008—**This integrates with the VMM 2008 and allows synergies such as Performance Resource and Optimization (PRO) Tips, which provides virtual machine recommendations based on observed performance and the ability to implement the recommendation at the click of a button.
- **Notifications—**The notification system has been revamped and now sports an Outlook rule style interface. Notifications can be generated for specific alerts and can be sent out as high-priority emails.
- **Overrides view—**Rather than hunt for overrides within all the management packs, OpsMgr R2 has an authoring view that shows all the overrides defined in the system.
- **Improved Management Pack maintenance—**OpsMgr 2007 R2 allows Microsoft management packs to be browsed, downloaded, and imported directly from the console. It even includes versioning and dependency checks, as well as the ability to search from management pack updates.
- **Service-level monitoring—**Applications can be defined from various monitored objects and the service level of the application can be monitored and reported on against defined target SLAs.
- **Better scaling of URL monitoring—**The URL monitor will now scale to thousands of websites without undue performance impact.
- **Improved database performance—**The overall performance of the database and console has been dramatically improved.

These improvements bring the platform to a new level of performance and interoperability, while retaining the look and feel of the original Operations Manager 2007 tool.

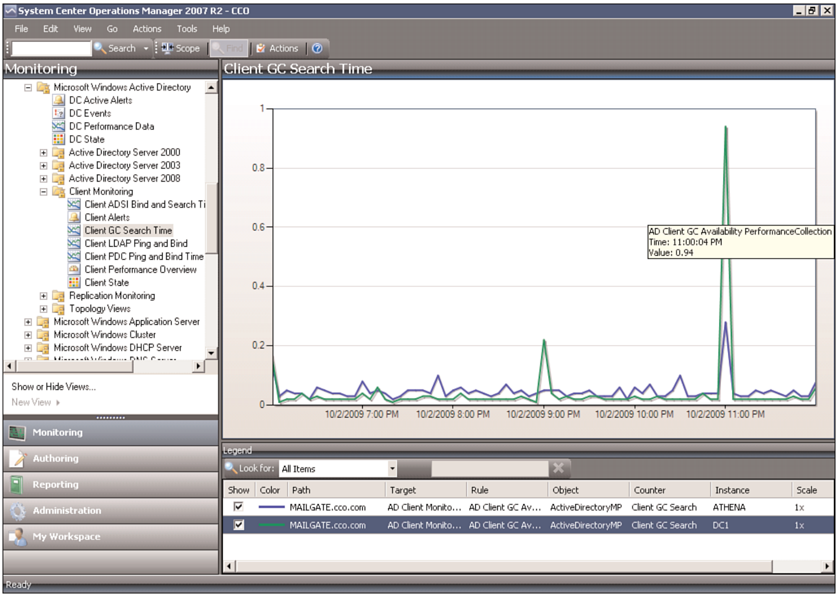
Explaining How OpsMgr Works

OpsMgr is a sophisticated monitoring system that effectively allows for large-scale management of mission-critical servers. Organizations with a medium to large investment in Microsoft technologies will find that OpsMgr allows for an unprecedented ability to keep on top of the tens of thousands of event log messages that occur on a daily basis. In its simplest form, OpsMgr performs two functions: processing monitored data and issuing alerts and automatic responses based on that data.

The model-based architecture of OpsMgr presents a fundamental shift in the way a network is monitored. The entire environment can be monitored as groups of hierarchical services with interdependent components. Microsoft, in addition to third-party vendors and a large development community, can leverage the functionality of OpsMgr components through customizable monitoring rules.

OpsMgr provides for several major pieces of functionality, as follows:

- **Management packs—**Application-specific monitoring rules are provided within individual files called management packs. For example, Microsoft provides management packs for Windows Server systems, Exchange Server, SQL Server, SharePoint, DNS, DHCP, along with many other Microsoft technologies. Management packs are loaded with the intelligence and information necessary to properly troubleshoot and identify problems. The rules are dynamically applied to agents based on a custom discovery process provided within the management pack. Only applicable rules are applied to each managed server.
- **Event monitoring rules—**Management pack rules can monitor for specific event log data. This is one of the key methods of responding to conditions within the environment.
- **Performance monitoring rules—**Management pack rules can monitor for specific performance counters. This data is used for alerting based on thresholds or archived for trending and capacity planning. A performance graph shown in Figure 23.2 shows Client GC Search Time data for a couple of domain controllers. There was a brief spike in latency at about 11:00 p.m., but the latency is normally less than 0.1.



AD Client GC Availability PerformanceCollection
Time: 11:00:04 PM
Value: 0.94

Show	Color	Path	Target	Rule	Object	Counter	Instance	Scale
☑	—	MAILGATE.cco.com	AD Client Monito...	AD Client GC Av...	ActiveDirectoryMP	Client GC Search	ATHENA	1x
☑	—	MAILGATE.cco.com	AD Client Monito...	AD Client GC Av...	ActiveDirectoryMP	Client GC Search	DC1	1x

FIGURE 23.2 Operations Manager 2007 R2 performance charts.

- **State-based monitors—**Management packs contain monitors, which allow for advanced state-based monitoring and aggregated health rollup of services. Monitors also provide self-tuning performance threshold monitoring based on a two- or three-state configuration.
- **Alerting—**OpsMgr provides advanced alerting functionality by enabling email alerts, paging, short message service (SMS), instant messaging (IM), and functional alerting roles to be defined. Alerts are highly customizable, with the ability to define alert rules for all monitored components.
- **Reporting—**Monitoring rules can be configured to send monitored data to both the operations database for alerting and the reporting database for archiving.
- **End-to-end service monitoring—**OpsMgr provides service-oriented monitoring based on System Definition Model (SDM) technologies. This includes advanced object discovery and hierarchical monitoring of systems.

Processing Operational Data

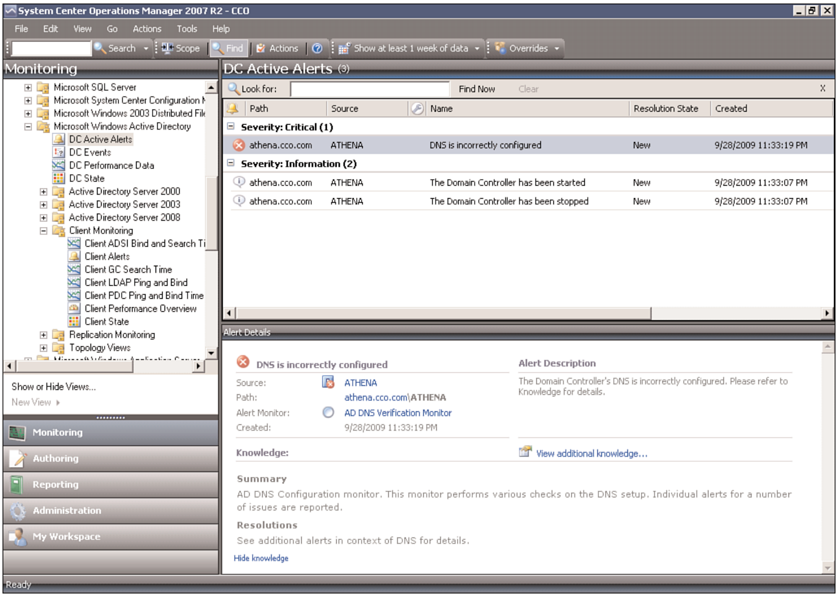
OpsMgr manages Windows Server 2008 R2 infrastructures through monitoring rules used for object discovery, Windows event log monitoring, performance data gathering, and application-specific synthetic transactions. Monitoring rules define how OpsMgr collects, handles, and responds to the information gathered. OpsMgr monitoring rules handle incoming event data and allow OpsMgr to react automatically, either to respond to a predetermined problem scenario, such as a failed hard drive, with predefined corrective and diagnostics actions (for example, trigger an alert, execute a command or script) to provide the operator with additional details based on what was happening at the time the condition occurred.

Generating Alerts and Responses

OpsMgr monitoring rules can generate alerts based on critical events, synthetic transactions, or performance thresholds and variances found through self-tuning performance trending. An alert can be generated by a single event or by a combination of events or performance thresholds. Alerts can also be configured to trigger responses such as email, pages, Simple Network Management Protocol (SNMP) traps, and scripts to notify you of potential problems. In brief, OpsMgr is completely customizable in this respect and can be modified to fit most alert requirements. A sample alert is shown in Figure 23.3. The alert indicates that the domain controller's DNS is incorrectly configured. Also note that there are two information alerts shown, indicating that the domain controller stopped and started.

Outlining OpsMgr Architecture

OpsMgr is primarily composed of five basic components: the operations database, reporting database, Root Management Server, management agents, and Operations Console. These components make up a basic deployment scenario. Several optional components are


System Center Operations Manager 2007 R2 - CCO
File Edit View Go Actions Tools Help
Search Scope Find Actions Show at least 1 week of data Overrides
Monitoring
Microsoft SQL Server
Microsoft System Center Configuration M
Microsoft Windows 2003 Distributed File
Microsoft Windows Active Directory
DC Active Alerts
DC Events
DC Performance Data
DC State
Active Directory Server 2000
Active Directory Server 2003
Active Directory Server 2008
Client Monitoring
Client ADSI Bind and Search Ti
Client Alerts
Client GC Search Time
Client LDAP Ping and Bind
Client PDC Ping and Bind Time
Client Performance Overview
Client State
Replication Monitoring
Topology Views
Show or Hide Views...
New View
Monitoring
Authoring
Reporting
Administration
My Workspace
Ready
DC Active Alerts (3)
Look for: Find Now Clear
Alert Details
Hide knowledge

Path	Source	Name	Resolution State	Created
Severity: Critical (1)				
athena.cco.com	ATHENA	DNS is incorrectly configured	New	9/28/2009 11:33:19 PM
Severity: Information (2)				
athena.cco.com	ATHENA	The Domain Controller has been started	New	9/28/2009 11:33:07 PM
athena.cco.com	ATHENA	The Domain Controller has been stopped	New	9/28/2009 11:33:07 PM

DNS is incorrectly configured

Source: ATHENA
Path: athena.cco.com\ATHENA
Alert Monitor: AD DNS Verification Monitor
Created: 9/28/2009 11:33:19 PM

Alert Description

The Domain Controller's DNS is incorrectly configured. Please refer to Knowledge for details.

Knowledge: View additional knowledge...

Summary

AD DNS Configuration monitor. This monitor performs various checks on the DNS setup. Individual alerts for a number of issues are reported.

Resolutions

See additional alerts in context of DNS for details.

FIGURE 23.3 Operations Manager 2007 R2 alert.

also described in the following bulleted list; these components provide functionality for advanced deployment scenarios.

OpsMgr was specifically designed to be scalable and can subsequently be configured to meet the needs of any size company. This flexibility stems from the fact that all OpsMgr components can either reside on one server or can be distributed across multiple servers.

Each of these various components provides specific OpsMgr functionality. OpsMgr design scenarios often involve the separation of parts of these components onto multiple servers. For example, the database components can be delegated to a dedicated server, and the management server can reside on a second server.

The following list describes the different OpsMgr components:

- **Operations database—**The operations database stores the monitoring rules and the active data collected from monitored systems. This database has a 7-day default retention period.
- **Reporting database—**The reporting database stores archived data for reporting purposes. This database has a 400-day default retention period.
- **Root Management Server—**This is the first management server in the management group. This server runs the software development kit (SDK) and Configuration service and is responsible for handling console communication, calculating the health of the environment, and determining what rules should be applied to each agent.

- **Management server—**Optionally, an additional management server can be added for redundancy and scalability. Agents communicate with the management server to deliver operational data and pull down new monitoring rules.
- **Management agents—**Agents are installed on each managed system to provide efficient monitoring of local components. Almost all communication is initiated from the agent with the exception of the actual agent installation and specific tasks run from the Operations Console. Agentless monitoring is also available with a reduction of functionality and environmental scalability.
- **Operations Console—**The Operations Console is used to monitor systems, run tasks, configure environmental settings, set author rules, subscribe to alerts, and generate and subscribe to reports.
- **Web console—**The Web console is an optional component used to monitor systems, run tasks, and manage Maintenance mode from a web browser.
- **Audit Collection Services—**This is an optional component used to collect security events from managed systems; this component is composed of a forwarder on the agent that sends all security events, a collector on the management server that receives events from managed systems, and a special database used to store the collected security data for auditing, reporting, and forensic analysis.
- **Gateway server—**This optional component provides mutual authentication through certificates for nontrusted systems in remote domains or workgroups.
- **Command shell—**This optional component is built on PowerShell and provides full command-line management of the OpsMgr environment.
- **Agentless Exception Monitoring—**This component can be used to monitor Windows and application crash data throughout the environment and provides insight into the health of the productivity applications across workstations and servers.
- **Connector Framework—**This optional component provides a bidirectional web service for communicating, extending, and integrating the environment with third-party or custom systems.

The Operations Manager 2007 architecture is shown in Figure 23.4, with all the major components and their data paths.

Understanding How OpsMgr Stores Captured Data

OpsMgr itself utilizes two Microsoft SQL Server databases for all collected data. Both databases are automatically maintained through OpsMgr-specific scheduled maintenance tasks.

The operations database stores all the monitoring rules and is imported by management packs and operational data collected from each monitored system. Data in this database is retained for 7 days by default. Data retention for the operations database is lower than the reporting database to improve efficiency of the environment. This database must be

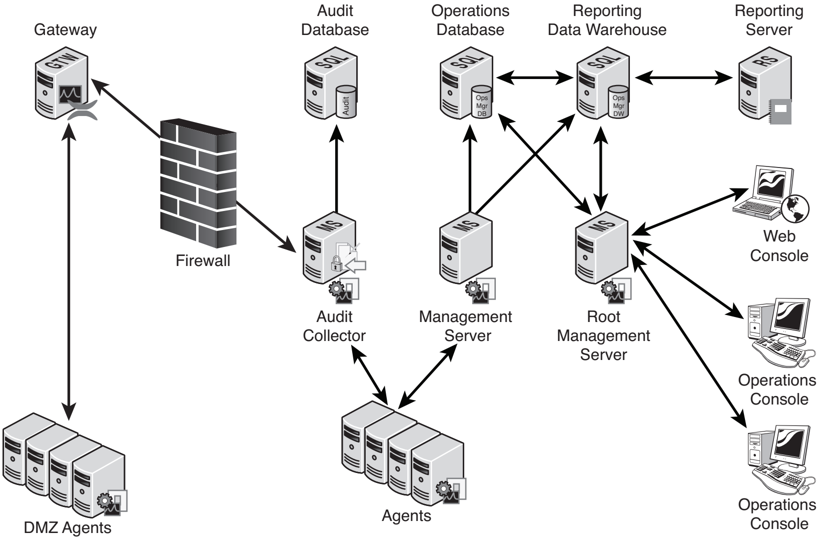


FIGURE 23.4 Operations Manager 2007 R2 architecture.

installed as a separate component from OpsMgr but can physically reside on the same server, if needed.

The reporting database stores data for long-term trend analysis and is designed to grow much larger than the operations database. Data in the reporting database is stored in three states: raw data, hourly summary, and daily summary. The raw data is only stored for 14 days, whereas both daily and hourly data are stored for 400 days. This automatic summarization of data allows for reports that span days or months to be generated very quickly.

Determining the Role of Agents in System Monitoring

The agents are the monitoring components installed on each managed computer. They monitor the system based on the rules and business logic defined in each of the management packs. Management packs are dynamically applied to agents based on the different discovery rules included with each management pack.

Defining Management Groups

OpsMgr utilizes the concept of management groups to logically separate geographical and organizational boundaries. Management groups allow you to scale the size of OpsMgr architecture or politically organize the administration of OpsMgr.

At a minimum, each management group consists of the following components:

- An operations database
- An optional reporting database
- A Root Management Server

- Management agents
- Management consoles

OpsMgr can be scaled to meet the needs of different sized organizations. For small organizations, all the OpsMgr components can be installed on one server with a single management group. In large organizations, on the other hand, the distribution of OpsMgr components to separate servers allows the organizations to customize and scale their OpsMgr architecture. Multiple management groups provide load balancing and fault tolerance within the OpsMgr infrastructure. Organizations can set up multiple management servers at strategic locations, to distribute the workload among them.

NOTE

The general rule of thumb with management groups is to start with a single management group and add on more management groups only if they are absolutely necessary. Administrative overhead is reduced, and there is less need to re-create rules and perform other redundant tasks with fewer management groups.

Understanding How to Use OpsMgr

Using OpsMgr is relatively straightforward. The OpsMgr monitoring environment can be accessed through three sets of consoles: an Operations Console, a Web console, and a command shell. The Operations Console provides full monitoring of agent systems and administration of the OpsMgr environment, whereas the Web console provides access only to the monitoring functionality. The command shell provides command-line access to administer the OpsMgr environment.

Managing and Monitoring with OpsMgr

As mentioned in the preceding section, two methods are provided to configure and view OpsMgr settings. The first approach is through the Operations Console and the second is through the command shell.

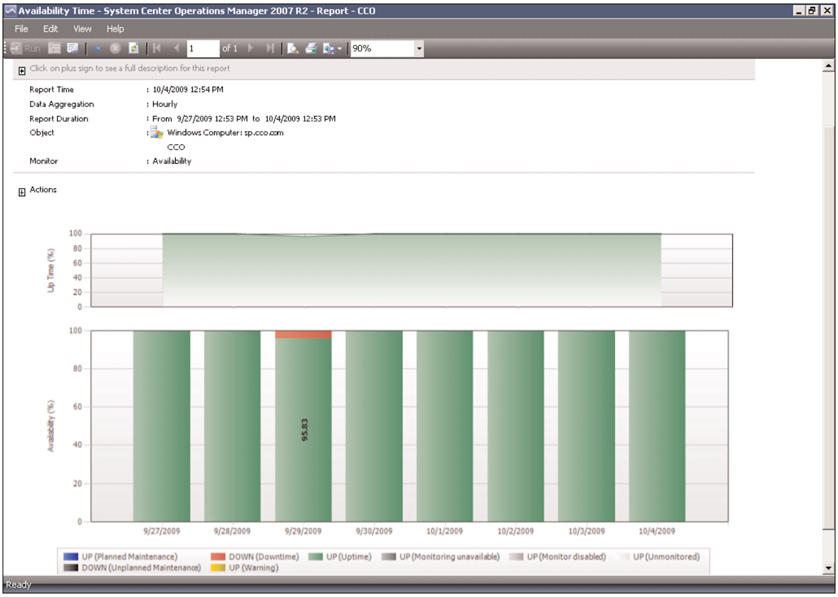
Within the Administration section of the Operations Console, you can easily configure the security roles, notifications, and configuration settings. Within the Monitoring section of the Operations Console, you can easily monitor a quick “up/down” status, active and closed alerts, and confirm overall environment health.

In addition, a web-based monitoring console can be run on any system that supports Microsoft Internet Explorer 6.0 or higher. This console can be used to view the health of systems, view and respond to alerts, view events, view performance graphs, run tasks, and manage Maintenance mode of monitored objects. New to OpsMgr 2007 R2 is the ability to display the Health Explorer in the Web console.

Reporting from OpsMgr

OpsMgr management packs commonly include a variety of preconfigured reports to show information about the operating system or the specific application they were designed to work with. These reports are run in SQL Reporting Services. The reports provide an effective view of systems and services on the network over a custom period, such as weekly, monthly, or quarterly. They can also help you monitor your networks based on performance data, which can include critical pattern analysis, trend analysis, capacity planning, and security auditing. Reports also provide availability statistics for distributed applications, servers, and specific components within a server.

Availability reports are particularly useful for executives, managers, and application owners. These reports can show the availability of any object within OpsMgr, including a server (shown in Figure 23.5), a database, or even a service such as Windows Server 2008 R2 that includes a multitude of servers and components. The Availability report shown in Figure 23.5 indicates that the SP server was down on 9/29/2009 for about 4.17% of the time or just slightly over 1 hour. The rest of the time it had been up.



Click on plus sign to see a full description for this report

Report Time	: 10/4/2009 12:54 PM
Data Aggregation	: Hourly
Report Duration	: From 9/27/2009 12:53 PM to 10/4/2009 12:53 PM
Object	: Windows Computer: sp.cco.com CCO
Monitor	: Availability

FIGURE 23.5 Availability report.

The reports can be run on demand or at scheduled times and delivered via email. OpsMgr can also generate HTML-based reports that can be published to a web server and viewed from any web browser. Vendors can also create additional reports as part of their management packs.

Using Performance Monitoring

Another key feature of OpsMgr is the capability to monitor and track server performance. OpsMgr can be configured to monitor key performance thresholds through rules that are set to collect predefined performance data, such as memory and CPU usage over time. Rules can be configured to trigger alerts and actions when specified performance thresholds have been met or exceeded, allowing network administrators to act on potential performance issues. Performance data can be viewed from the OpsMgr Operations Console.

In addition, performance monitors can establish baselines for the environment and then alert the administrator when the counter subsequently falls outside the defined baseline envelope.

Using Active Directory Integration

Active Directory integration provides a way to install management agents on systems without environmental-specific settings. When the agent starts, the correct environmental settings, such as the primary and failover management servers, are stored in Active Directory. The configuration of Active Directory integration provides advanced search and filter capabilities to fine-tune the dynamic assignment of systems.

Integrating OpsMgr Non-Windows Devices

Network management is not a new concept. Simple management of various network nodes has been handled for quite some time through the use of the SNMP. Quite often, simple or even complex systems that utilize SNMP to provide for system monitoring are in place in an organization to provide for varying degrees of system management on a network.

OpsMgr can be configured to integrate with non-Windows systems through monitoring of syslog information, log file data, and SNMP traps. OpsMgr can also monitor TCP port communication and website transaction sequencing for information-specific data management.

New to OpsMgr 2007 R2 is the ability to monitor non-Microsoft operating systems such as Linux and UNIX, as well as the applications that run on them such as Apache and MySQL. OpsMgr monitors the file systems, network interfaces, daemons, configurations, and performance metrics. Operations Manager 2007 R2 supports monitoring of the following operating systems:

- HP-UX 11i v2 and v3 (PA-RISC and IA64)
- Sun Solaris 8 and 9 (SPARC) and Solaris 10 (SPARC and x86)
- Red Hat Enterprise Linux 4 (x86/x64) and 5 (x86/x64) Server
- Novell SUSE Linux Enterprise Server 9 (x86) and 10 SP1 (x86/x64)
- IBM AIX v5.3 and v6.1

These operating systems are “first-class citizens” in Microsoft’s parlance, meaning they are treated as equals with the Windows operating systems. Agents can be pushed from the console, operations data is collected automatically, tasks can run against the agents, and all major functions are supported.

Special connectors can be created to provide bidirectional information flows to other management products. OpsMgr can monitor SNMP traps from SNMP-supported devices as well as generate SNMP traps to be delivered to third-party network management infrastructures.

Exploring Third-Party Management Packs

Software and hardware developers can subsequently create their own management packs to extend OpsMgr's management capabilities. These management packs extend OpsMgr's management capabilities beyond Microsoft-specific applications. Each management pack is designed to contain a set of rules and product knowledge required to support its respective products. Currently, management packs have been developed for APC, Cisco, Citrix, Dell, F5, HP, IBM, Linux, Oracle, Solaris, UNIX, and VMware to name a few. A complete list of management packs can be found at the following Microsoft site: http://technet.microsoft.com/en-us/opsmgr/cc539535.aspx.

Understanding OpsMgr Component Requirements

Each OpsMgr component has specific design requirements, and a good knowledge of these factors is required before beginning the design of OpsMgr. Hardware and software requirements must be taken into account, as well as factors involving specific OpsMgr components, such as the Root Management Server, gateway servers, service accounts, mutual authentication, and backup requirements.

Exploring Hardware Requirements

Having the proper hardware for OpsMgr to operate on is a critical component of OpsMgr functionality, reliability, and overall performance. Nothing is worse than overloading a brand-new server only a few short months after its implementation. The industry standard generally holds that any production servers deployed should remain relevant for three to four years following deployment. Stretching beyond this time frame might be possible, but the ugly truth is that hardware investments are typically short term and need to be replaced often to ensure relevance. Buying a less-expensive server might save money in the short term but could potentially increase costs associated with downtime, troubleshooting, and administration. That said, the following are the Microsoft-recommended minimums for any server running an OpsMgr 2007 server component:

- 2.8GHz processor or faster
- 20GB of free disk space
- 2GB of random access memory (RAM)

These recommendations apply only to the smallest OpsMgr deployments and should be seen as minimum levels for OpsMgr hardware. More realistic deployments would have the following minimums:

- 2–4 2.8GHz cores
- 64-bit Windows operating system
- 64-bit SQL Server
- 60GB free disk space on RAID 1+0 for performance
- 4–8GB RAM

Operations Manager 2007 R2 is one of Microsoft's most resource-intensive applications, so generous processor, disk, and memory are important for optimal performance. Future expansion and relevance of hardware should be taken into account when sizing servers for OpsMgr deployment, to ensure that the system has room to grow as agents are added and the databases grow.

Determining Software Requirements

OpsMgr components can be installed on either 32-bit or 64-bit versions of Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2. The database for OpsMgr must be run on a Microsoft SQL Server 2005 or Microsoft SQL Server 2008 server. The database can be installed on the same server as OpsMgr or on a separate server, a concept that is discussed in more detail in following sections.

OpsMgr itself must be installed on a member server in a Windows Active Directory domain. It is commonly recommended to keep the installation of OpsMgr on a separate server or set of dedicated member servers that do not run any other applications that could interfere in the monitoring and alerting process.

A few other requirements critical to the success of OpsMgr implementations are as follows:

- Microsoft .NET Framework 2.0 and 3.0 must be installed on the management server and the reporting server.
- Windows PowerShell.
- Microsoft Core XML Services (MSXML) 6.0.
- WS-MAN v1.1 (for UNIX/Linux clients).
- Client certificates must be installed in environments to facilitate mutual authentication between nondomain members and management servers.
- SQL Reporting Services must be installed for an organization to be able to view and produce custom reports using OpsMgr's reporting feature.

OpsMgr Backup Considerations

The most critical piece of OpsMgr, the SQL databases, should be regularly backed up using standard backup software that can effectively perform online backups of SQL databases. If integrating these specialized backup utilities into an OpsMgr deployment is not possible, it becomes necessary to leverage built-in backup functionality found in SQL Server.

Understanding Advanced OpsMgr Concepts

OpsMgr's simple installation and relative ease of use often belie the potential complexity of its underlying components. This complexity can be managed with the right amount of knowledge of some of the advanced concepts of OpsMgr design and implementation.

Understanding OpsMgr Deployment Scenarios

As previously mentioned, OpsMgr components can be divided across multiple servers to distribute load and ensure balanced functionality. This separation allows OpsMgr servers to come in four potential "flavors," depending on the OpsMgr components held by those servers. The four OpsMgr server types are as follows:

- **Operations database server—**An operations database server is simply a member server with SQL Server installed for the OpsMgr operations database. No other OpsMgr components are installed on this server. The SQL Server component can be installed with default options and with the system account used for authentication. Data in this database is kept for 7 days by default.
- **Reporting database server—**A reporting database server is simply a member server with SQL Server and SQL Server Reporting Services installed. This database stores data collected through the monitoring rules for a much longer period than the operations database and is used for reporting and trend analysis. This database requires significantly more drive space than the operations database server. Data in this database is kept for 13 months by default.
- **Management server—**A management server is the communication point for both management consoles and agents. Effectively, a management server does not have a database and is often used in large OpsMgr implementations that have a dedicated database server. Often, in these configurations, multiple management servers are used in a single management group to provide for scalability and to address multiple managed nodes.
- **All-in-one server—**An all-in-one server is effectively an OpsMgr server that holds all OpsMgr roles, including that of the databases. Subsequently, single-server OpsMgr configurations use one server for all OpsMgr operations.

Multiple Configuration Groups

As previously defined, an OpsMgr management group is a logical grouping of monitored servers that are managed by a single OpsMgr SQL database, one or more management servers, and a unique management group name. Each management group established operates completely separately from other management groups, although they can be configured in a hierarchical structure with a top-level management group able to see “connected” lower-level management groups.

The concept of connected management groups allows OpsMgr to scale beyond artificial boundaries and also gives a great deal of flexibility when combining OpsMgr environments. However, certain caveats must be taken into account. Because each management group is an island in itself, each must subsequently be manually configured with individual settings. In environments with a large number of customized rules, for example, such manual configuration would create a great deal of redundant work in the creation, administration, and troubleshooting of multiple management groups.

Deploying Geographic-Based Configuration Groups

Based on the factors outlined in the preceding section, it is preferable to deploy OpsMgr in a single management group. However, in some situations, an organization needs to divide its OpsMgr environment into multiple management groups. The most common reason for division of OpsMgr management groups is division along geographic lines. In situations in which wide area network (WAN) links are saturated or unreliable, it might be wise to separate large “islands” of WAN connectivity into separate management groups.

Simply being separated across slow WAN links is not enough reason to warrant a separate management group, however. For example, small sites with few servers would not warrant the creation of a separate OpsMgr management group, with the associated hardware, software, and administrative costs. However, if many servers exist in a distributed, generally well-connected geographical area, that might be a case for the creation of a management group. For example, an organization could be divided into several sites across the United States but decide to divide the OpsMgr environment into separate management groups for East Coast and West Coast, to roughly approximate their WAN infrastructure.

Smaller sites that are not well connected but are not large enough to warrant their own management group should have their event monitoring throttled to avoid being sent across the WAN during peak usage times. The downside to this approach, however, is that the reaction time to critical event response is increased.

Deploying Political or Security-Based Configuration Groups

The less-common method of dividing OpsMgr management groups is by political or security lines. For example, it might become necessary to separate financial servers into a separate management group to maintain the security of the finance environment and allow for a separate set of administrators.

Politically, if administration is not centralized within an organization, management groups can be established to separate OpsMgr management into separate spheres of control. This would keep each OpsMgr management zone under separate security models.

As previously mentioned, a single management group is the most efficient OpsMgr environment and provides for the least amount of redundant setup, administration, and troubleshooting work. Consequently, artificial OpsMgr division along political or security lines should be avoided, if possible.

Sizing the OpsMgr Database

Depending on several factors, such as the type of data collected, the length of time that collected data will be kept, or the amount of database grooming that is scheduled, the size of the OpsMgr database will grow or shrink accordingly. It is important to monitor the size of the database to ensure that it does not increase well beyond the bounds of acceptable size. OpsMgr can be configured to monitor itself, supplying advance notice of database problems and capacity thresholds. This type of strategy is highly recommended because OpsMgr could easily collect event information faster than it could get rid of it.

The size of the operations database can be estimated through the following formula:

```
Number of agents x 5MB x retention days + 1024 overhead = estimated database size
```

For example, an OpsMgr environment monitoring 1,000 servers with the default 7-day retention period will have an estimated 35GB operations database:

```
(1000 * 5 * 7) + 1024 = 36024 MB
```

The size of the reporting database can be estimated through the following formula:

```
Number of agents x 3MB x retention days + 1024 overhead = estimated database size
```

The same environment monitoring 1,000 servers with the default 400-day retention period will have an estimated 1.1TB reporting database:

```
(1000 * 3 * 400) + 1024 = 1201024 MB
```

It is important to understand that these estimates are rough guidelines only and can vary widely depending on the types of servers monitored, the monitoring configuration, the degree of customization, and other factors.

Defining Capacity Limits

As with any system, OpsMgr includes some hard limits that should be taken into account before deployment begins. Surpassing these limits could be cause for the creation of new management groups and should subsequently be included in a design plan. These limits are as follows:

- **Operations database—**OpsMgr operates through a principle of centralized, rather than distributed, collection of data. All event logs, performance counters, and alerts are sent to a single, centralized database, and there can subsequently be only a single operations database per management group. Considering the use of a backup and high-availability strategy for the OpsMgr database is, therefore, highly recommended, to protect it from outage. It is recommended to keep this database with a 50GB limit to improve efficiency and reduce alert latency.

- **Management servers—**OpsMgr does not have a hard-coded limit of management servers per management group. However, it is recommended to keep the environment between three to five management servers. Each management server can support approximately 2,000 managed agents.
- **Gateway servers—**OpsMgr does not have a hard-coded limit of gateway servers per management group. However, it is recommended to deploy a gateway server for every 200 nontrusted domain members.
- **Agents—**Each management server can theoretically support up to 2,000 monitored agents. In most configurations, however, it is wise to limit the number of agents per management server, although the levels can be scaled upward with more robust hardware, if necessary.
- **Administrative consoles—**OpsMgr does not limit the number of instances of the Web and Operations Console; however, going beyond the suggested limit might introduce performance and scalability problems.

Defining System Redundancy

In addition to the scalability built in to OpsMgr, redundancy is built in to the components of the environment. Proper knowledge of how to deploy OpsMgr redundancy and place OpsMgr components correctly is important to the understanding of OpsMgr redundancy. The main components of OpsMgr can be made redundant through the following methods:

- **Management servers—**Management servers are automatically redundant and agents will failover and failback automatically between them. Simply install additional management servers for redundancy. In addition, the RMS system acts as a management server and participates in the fault tolerance.
- **SQL databases—**The SQL database servers hosting the databases can be made redundant using SQL clustering, which is based on Windows clustering. This supports failover and failback.
- **Root Management Server—**The RMS can be made redundant using Windows clustering. This supports failover and failback.

Having multiple management servers deployed across a management group allows an environment to achieve a certain level of redundancy. If a single management server experiences downtime, another management server within the management group will take over the responsibilities for the monitored servers in the environment. For this reason, it might be wise to include multiple management servers in an environment to achieve a certain level of redundancy if high uptime is a priority.

The first management server in the management group is called the Root Management Server. Only one Root Management Server can exist in a management group and it hosts the software development kit (SDK) and Configuration service. All OpsMgr consoles communicate with the management server so its availability is critical. In large-scale environments, the Root Management Server should leverage Microsoft Cluster technology to provide high availability for this component.

Because there can be only a single OpsMgr database per management group, the database is subsequently a single point of failure and should be protected from downtime. Utilizing Windows Server 2008 R2 clustering or third-party fault-tolerance solutions for SQL databases helps to mitigate the risk involved with the OpsMgr database.

Monitoring Nondomain Member Considerations

DMZ, Workgroup, and Nontrusted Domain Agents require special configuration; in particular, they require certificates to establish mutual authentication. Operations Manager 2007 R2 requires mutual authentication, that is, the server authenticates to the client and the client authenticates to the server, to ensure that the monitoring communications are not hacked. Without mutual authentication, it is possible for a hacker to execute a man-in-the-middle attack and impersonate either the client or the server. Thus, mutual authentication is a security measure designed to protect clients, servers, and sensitive Active Directory domain information, which is exposed to potential hacking attempts by the all-powerful management infrastructure. However, OpsMgr relies on Active Directory Kerberos for mutual authentication, which is not available to nondomain members.

NOTE

Workgroup servers, public web servers, and Microsoft Exchange Edge Transport role servers are commonly placed in the DMZ and are for security reasons not domain members, so almost every Windows Server 2008 R2 environment will need to deploy certificate-based authentication.

In the absence of Active Directory, trusts, and Kerberos, OpsMgr 2007 R2 can use X.509 certificates to establish the mutual authentication. These can be issued by any PKI, such as Microsoft Windows Server 2008 Enterprise CA. See Chapter 14, “Transport-Level Security,” for details on PKI and Windows Server 2008 R2.

Installing agents on DMZ servers is discussed later in this chapter in the section “Monitoring DMZ Servers with Certificates.”

Securing OpsMgr

Security has evolved into a primary concern that can no longer be taken for granted. The inherent security in Windows Server 2008 R2 is only as good as the services that have access to it; therefore, it is wise to perform a security audit of all systems that access information from servers. This concept holds true for management systems as well because they collect sensitive information from every server in an enterprise. This includes potentially sensitive event logs that could be used to compromise a system. Consequently, securing the OpsMgr infrastructure should not be taken lightly.

Securing OpsMgr Agents

Each server that contains an OpsMgr agent and forwards events to management servers has specific security requirements. Server-level security should be established and should include provisions for OpsMgr data collection. All traffic between OpsMgr components, such as the agents, management servers, and database, is encrypted automatically for security, so the traffic is inherently secured.

In addition, environments with high-security requirements should investigate the use of encryption technologies such as IPSec to scramble the event IDs that are sent between agents and OpsMgr servers, to protect against eavesdropping of OpsMgr packets.

OpsMgr uses mutual authentication between agents and management servers. This means that the agent must reside in the same forest as the management server. If the agent is located in a different forest or workgroup, client certificates can be used to establish mutual authentication. If an entire nontrusted domain must be monitored, the gateway server can be installed in the nontrusted domain, agents can establish mutual authentication to the gateway server, and certificates on the gateway and management server are used to establish mutual authentication. In this scenario, you can avoid needing to place a certificate on each nontrusted domain member.

Understanding Firewall Requirements

OpsMgr servers that are deployed across a firewall have special considerations that must be taken into account. Port 5723, the default port for OpsMgr communications, must specifically be opened on a firewall to allow OpsMgr to communicate across it.

Table 23.1 describes communication for this and other OpsMgr components.

TABLE 23.1 OpsMgr Communication Ports

From	To	Port
Agent	Root Management Server	5723
Agent	Management server	5723
Agent	Gateway server	5723
Agent (ACS forwarder)	Management server ACS collector	51909
Gateway server	Root Management Server	5723
Gateway server	Management server	5723
Management or Gateway server	UNIX or Linux computer	1270
Management or Gateway server	UNIX or Linux computer	22

TABLE 23.1 OpsMgr Communication Ports

From	To	Port
Management server	Operations Manager database	1433
Management server	Root Management Server	5723, 5724
Management server	Reporting data warehouse	1433
Management server ACS collector	ACS database	1433
Operations Console	Root Management Server	5724
Operations Console (reports)	SQL Server Reporting Services	80
Reporting server	Root Management Server	5723, 5724
Reporting server	Reporting data warehouse	1433
Root Management Server	Operations Manager database	1433
Root Management Server	Reporting data warehouse	1433
Web console browser	Web console server	51908
Web console server	Root Management Server	5724

The firewall port for the agents is the port that needs to be opened most often, which is only port 5723 from the agent to the management servers for monitoring. Other ports, such as 51909 for ACS, are more rarely needed. Figure 23.6 shows the major communications paths and ports between OpsMgr components.

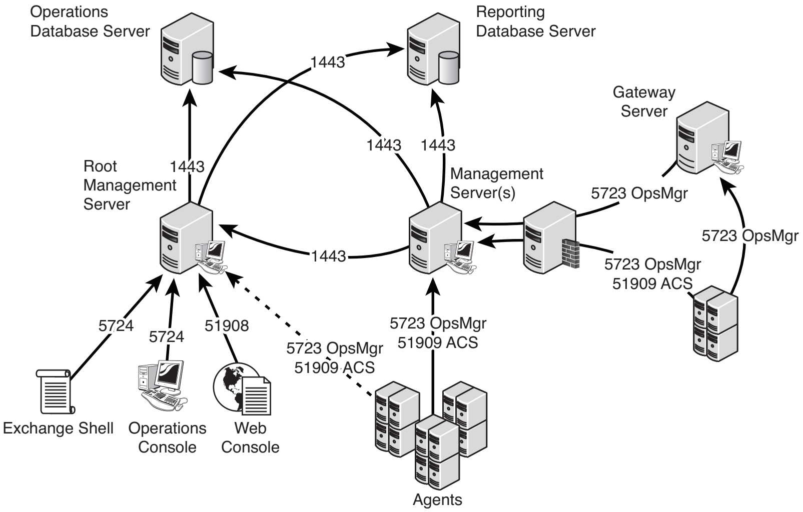


FIGURE 23.6 Communications ports.

Outlining Service Account Security

In addition to the aforementioned security measures, security of an OpsMgr environment can be strengthened by the addition of multiple service accounts to handle the different OpsMgr components. For example, the Management Server Action account and the SDK/Configuration service account should be configured to use separate credentials, to provide for an extra layer of protection in the event that one account is compromised.

- **Management Server Action account—**The account responsible for collecting data and running responses from management servers.
- **SDK and Configuration service account—**The account that writes data to the operations database; this service is also used for all console communication.
- **Local Administrator account—**The account used during the agent push installation process. To install the agent, local administrative rights are required.
- **Agent Action account—**The credentials the agent will run as. This account can run under a built-in system account, such as Local System, or a limited domain user account for high-security environments.
- **Data Warehouse Write Action account—**The account used by the management server to write data to the reporting data warehouse.
- **Data Warehouse Reader account—**The account used to read data from the data warehouse when reports are executed.
- **Run As accounts—**The specific accounts used by management packs to facilitate monitoring. These accounts must be manually created and delegated specific rights as defined in the management pack documentation. These accounts are then assigned as Run As accounts used by the management pack to achieve a high degree of security and flexibility when monitoring the environment. New to OpsMgr 2007 R2 is the ability to selectively distribute the Run As Account to just the agents that need them.

Installing Operations Manager 2007 R2

As discussed in the previous section, Operations Manager 2007 R2 is a multitier and multicomponent application that can be deployed in a variety of architectures. This allows OpsMgr to support scaling from a small organization to a very large enterprise.

For the purposes of this chapter, an all-in-one single-server install is used. This allows for monitoring of small- to medium-sized Windows Server 2008 R2 organizations spanning a handful of servers to up to 250 servers.

Single-Server OpsMgr 2007 R2 Install

This section steps through the install of OpsMgr and Reporting on a single-server configuration. The specification for a single-server configuration to support up to 250 agent systems is as follows:

- 2 x 2.8GHz Cores
- 8GB RAM
- 4 Drive RAID 0+1 Disk (200+GB Space)

These hardware requirements ensure that the system can perform to specification.

NOTE

If the configuration were to be virtualized on a Windows Server 2008 Hyper-V host or a VMware ESX host, a single-server configuration is not recommended. Instead, a two-server configuration is recommended and SQL Server 2008 should be installed on the second server to balance the load.

The steps in this section assume that the single server has been prepared with the following:

- Windows Server 2008 R2 operating system installed
- Web role with the appropriate features installed

NOTE

To install SQL Reporting Services and the Web components of OpsMgr 2007 R2, the following Windows Server 2008 Web role features need to be installed: Static Content, Default Document, HTTP Redirection, Directory Browsing, ASP, ASP.NET, ISAPI Extension, ISAPI Filters, Windows Authentication, IIS Metabase, and IIS 6 WMI.

- SQL Server 2008 with Reporting Services installed
- An OpsMgr service account with local administrator rights to the server and system administrator rights to SQL Server 2008

This prepares the system for the install of OpsMgr 2007 R2. See the following prerequisite checker information for additional requirements and how to check them.

Before installing, it is important to run the built-in prerequisite checker. This utility is available on the OpsMgr installation media and confirms a host of software prerequisites before attempting the actual installation. This gives the administrator time to download and install the necessary software, rather than have the installation bomb out in the middle after entering a lot of configuration information.

This section assumes a Windows Server 2008 and SQL Server 2008 server will be used for the single-server installation, but the prerequisite checker looks at more general requirements based on the OpsMgr supported platforms. The prerequisite checker looks for the following software on a single-server configuration:

- Windows Server 2003 Service Pack 1 or Windows Server 2008 Service Pack 1
- Microsoft SQL Server 2005 Service Pack 1 or SQL Server 2008 Service Pack 1
- Microsoft SQL Server 2005 Reporting Services Service Pack 1 or SQL Server 2008 Reporting Services Service Pack 1
- World Wide Web Service is running and set for automatic startup
- WS-Management v1.1
- MDAC version 2.80.1022.0 or higher
- ASP.NET AJAX Extensions 1.0
- .NET Framework 2.0 and .NET Framework 3.0 components
- Windows PowerShell
- Key hotfixes

To use the Prerequisite Viewer for a single-server configuration, run the following steps:

1. Log on with an account that has administrator rights.
2. Insert the Operations Manager 2007 R2 installation media.
3. The setup will start automatically or launch the `SetupOM.exe`.
4. Click Check Prerequisites to start the Prerequisite Viewer.
5. Select Operational Database, Server, Console, PowerShell, Web Console, Reporting, and Data Warehouse, and then click Check.

NOTE

The prerequisite checker findings will be displayed and will have active links that can be clicked to get specific guidance, as well as links to download software and hotfixes.

6. When you are finished with the Prerequisite Viewer, click Close.

Follow the corrections in the prerequisite checker to resolve any problems before proceeding to the installation. Some of the guidance will be warnings, particularly with some of the hotfixes. Leaving out hotfixes might allow the installation to proceed, but might make the OpsMgr application less stable. It is highly recommended that all the recommendations be applied to ensure the most stable platform possible. If any of the installations require a reboot, it is recommended to run the prerequisite checker again.

Once the server meets all the prerequisites and is ready for installation, the steps to run the install are as follows:

1. Logon with the OpsMgr service account.
2. Launch `SetupOM.exe` from the OpsMgr installation media.
3. Click Install Operations Manager 2007 R2.
4. Click Next.
5. Accept the license agreement and click Next.
6. Enter the CD key if required and then click Next.
7. When the Custom Setup page displays, leave the components set to their defaults, and then click Next.
8. Type the management group name in the Management Group text box and click Next.
9. Select the instance of SQL Server on which to install the Operations Manager 2007 R2 database (the local system because this is a single-server install), and then click Next.
10. Leave the default database size of 1,000 MB, and then click Next.
11. Select Domain or Local Computer Account, type the user account and password, select the domain or local computer from the list, and then click Next.
12. On the SDK and Config Service Account page, select Domain or Local Account, type the user account and password, select the domain or local computer from the list, and then click Next.
13. On the Web Console Authentication Configuration page, select Use Windows Authentication and click Next.
14. On the Operations Manager Error Reports page, leave the Do You Want to Send Error Reports to Microsoft option cleared and click Next to not send Operations Manager 2007 R2 error reports to Microsoft.
15. On the Customer Experience Improvement Program page, leave the default option of I Don't Want to Join the Program Selected, and then click Next.
16. On the Ready to Install page, click Install.
17. When the Completing the System Center Operations Manager 2007 R2 Setup Wizard page appears, leave the Backup Encryption Key check box selected to back up the encryption key.

NOTE

A copy of the encryption key is needed to promote a management server to the role of the Root Management Server in the event of a failure of the RMS.

18. Leave Start the Console selected to open the Operations Console.
19. Click Finish.

Operations Manager 2007 R2 is now installed in a single-server configuration. This configuration can manage up to 250 servers.

Importing Management Packs

After the initial installation, OpsMgr only includes a few management packs. The management packs contain all the discoveries, monitors, rules, knowledge, reports, and views that OpsMgr needs to be able to effectively monitor servers and applications. One of the first tasks after installing OpsMgr 2007 is to import management packs into the system.

There are a large number of management packs in the Internet catalog on the Microsoft website. These include updated management packs, management packs for new products, and third-party management packs. It is important to load only those management packs that are going to be used, as each additional management pack increases the database size, adds discoveries that impact the performance of agents, and, in general, clutters up the interface.

The key management packs for a Windows Server 2008 R2 environment are as follows:

- Windows Server Operating System MPs
- Active Directory Server MPs
- Windows Cluster Management MPs
- Microsoft Windows DNS Server MPs
- Microsoft Windows DHCP Server MPs
- Microsoft Windows Group Policy MPs
- Microsoft Windows Hyper-V MPs
- Windows Server Internet Information Services MPs
- Windows Server Network Load Balancing MPs
- Windows Server Print Server MPs
- Windows Terminal Services MPs
- SQL Server MPs (to monitor the OpsMgr database roles)

There might be other management packs that are appropriate for the environment, depending on the applications that are installed. For example, if the organization has deployed Exchange Server 2010 and HP Proliant server hardware, it would be good for the organization to deploy the Exchange management packs and the HP Proliant management packs.

For each of these management packs, it is important to load the relevant versions only. For example, if the environment includes Windows Server 2008 only, only load the Windows Server Core OS 2008 management pack. If the environment includes both Windows Server 2003 and Windows Server 2008, load both the Windows Server Core OS

2003 and the Windows Server Core OS 2008. In addition, a number of language packs don't need to be loaded unless those particular languages are supported by the organization at the server level.

Some collections of management packs require that all versions be loaded, but the Management Pack Import Wizard will check and warn if that's the case.

In versions of OpsMgr prior to R2, the management packs had to be downloaded from the Microsoft website one by one, the MSI installed one by one, and the management packs imported one by one. Dependencies would not be checked unless additional steps were taken to consolidate the management pack files prior to importing. This was a very labor-intensive process. Also, there was no easy way for checking for updates to already installed management packs.

In OpsMgr 2007 R2, a new Management Pack Import Wizard was introduced. This wizard connects directly to the Microsoft management pack catalog and will download, check, and import management packs. It even does version checks to ensure that the management packs are the latest versions. This is a huge improvement over the old method of importing management packs.

To import the key management packs, use the following steps:

1. Launch the Operations Console.
2. Select the Administration section.
3. Select the Management Packs folder.
4. Right-click the Management Packs folder and select Import Management Packs.
5. Click the Add button and select Add from Catalog.
6. Click the Search button to search the entire catalog.

NOTE

The View pull-down menu in the Management Pack Import Wizard includes four options, which are All Management Packs in the Catalog, Updates Available for Installed Management Packs, All Management Packs Released in the Last 3 Months, and All Management Packs Released in the Last 6 Months. The Updates option checks against the already installed management packs and allows the download of updated versions of those.

7. Select the key management packs from the previous bulleted list and click the Add button for each of them. Each of the major management packs might include a number of submanagement packs for discovery, monitoring, and other breakdowns of functionality.
8. When done adding management packs, click OK.
9. The wizard now validates the added management packs, checking for versions, dependencies, and security risks. It allows problem management packs to be removed and dependencies to be added to the list.

10. Click Install to begin the download and import process. Progress will be shown for each of the management packs being imported.
11. After all the management packs are imported, click Close to exit the wizard.

After the import completes, the management packs take effect immediately. Agents will begin discovering based on the schedule specified in the management packs and monitors and rules will begin deploying.

Deploying OpsMgr Agents

OpsMgr agents are deployed to all managed servers through the OpsMgr Discovery Wizard, or by using software distribution mechanisms such as Active Directory GPOs or System Center Configuration Manager 2007. Installation through the Operations Console uses the fully qualified domain name (FQDN) of the computer. When searching for systems through the Operations Console, you can use wildcards to locate a broad range of computers for agent installation. Certain situations, such as monitoring across firewalls, can require the manual installation of these components.

The Discovery Wizard can discover and configure monitoring for Windows computers, UNIX/Linux computers, and for network devices. It will push agents to Windows and UNIX/Linux computers, as long as the proper rights are provided, such as an account with local administrator rights or a root account.

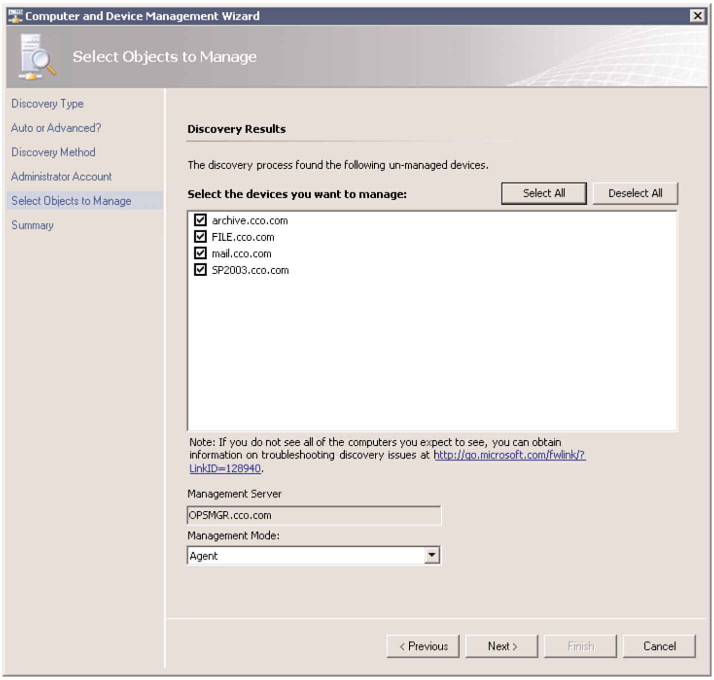
To install domain member agents using the Discovery Wizard, run the following steps:

1. Launch the Operations Console and select the Administration section.
2. Right-click the top-level Administration folder and select Discovery Wizard.
3. Select the Windows computers and click Next.
4. Select Automatic Computer Discovery and click Next. This scans the entire Active Directory domain for computers.
5. Leave the Use Selected Management Server Action Account and click Discover. This starts the discovery process.
6. After the discovery process runs (this might take a few minutes), the list of discovered computers is displayed. Select the devices that should have agents deployed to them, as shown in Figure 23.7.

NOTE

The list only includes systems that do not already have agents installed. If a computer has an agent installed, the wizard excludes it from the list of devices.

7. Click Next.
8. Leave the Agent Installation Directory and the Agent Action Account at the defaults, and then click Finish.
9. The Agent Management Task Status window appears, listing all the computers selected and the progress of each installation. As shown in Figure 23.8, the agent installation task started for the selected computers.
10. Click Close when the installation completes.



Discovery Results

The discovery process found the following un-managed devices.

Select the devices you want to manage:

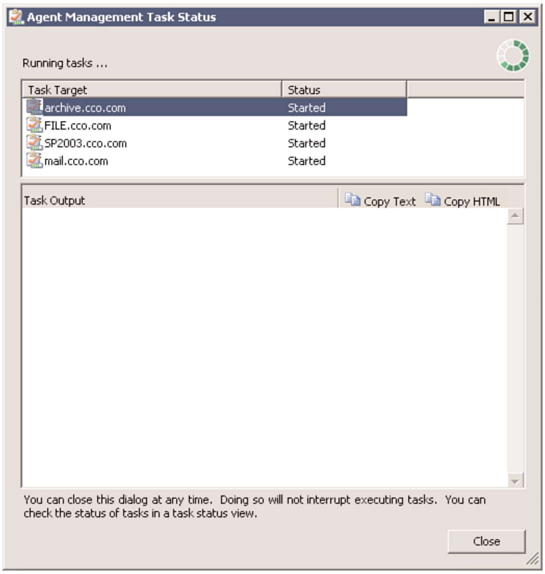
- ☑ archive.cco.com
- ☑ FILE.cco.com
- ☑ mail.cco.com
- ☑ SP2003.cco.com

Note: If you do not see all of the computers you expect to see, you can obtain information on troubleshooting discovery issues at http://go.microsoft.com/fwlink/?LinkID=128940.

Management Server: OPSMGR.cco.com

Management Mode: Agent

FIGURE 23.7 Discovered computers.



Running tasks ...

Task Target	Status
archive.cco.com	Started
FILE.cco.com	Started
SP2003.cco.com	Started
mail.cco.com	Started

Task Output

You can close this dialog at any time. Doing so will not interrupt executing tasks. You can check the status of tasks in a task status view.

FIGURE 23.8 Agent installation progress.

Even if the window is closed before the installs complete, the results of the installs can be viewed in Task Status view in the Monitoring section of the Operations Console.

The agent deployment is very efficient and a large number of computers can be selected for deployment without any issues. The agents will start automatically and begin to be monitored as they are discovered.

After installation, it might be necessary to wait a few minutes before the information from the agents will be sent to the management server.

During the next few minutes after installation, the agent contacts the management server and establishes a mutually authenticated, encrypted communication channel with the assigned management server. If the agent was pushed through a software delivery system such as System Center Configuration Manager 2007 R2, the agent determines the management server through Active Directory–integrated discovery.

The agent downloads rules to discover the various applications and components it's hosting, allowing the correct application-specific management packs to be applied. This discovery process runs periodically to ensure the correct rules are always applied to the server.

Configuring Operations Manager 2007 R2

After installing the Operations Manager 2007 R2 infrastructure, several configuration steps should be taken to have the system monitor properly, generate Active Directory synthetic transactions, and send out email notifications of alerts.

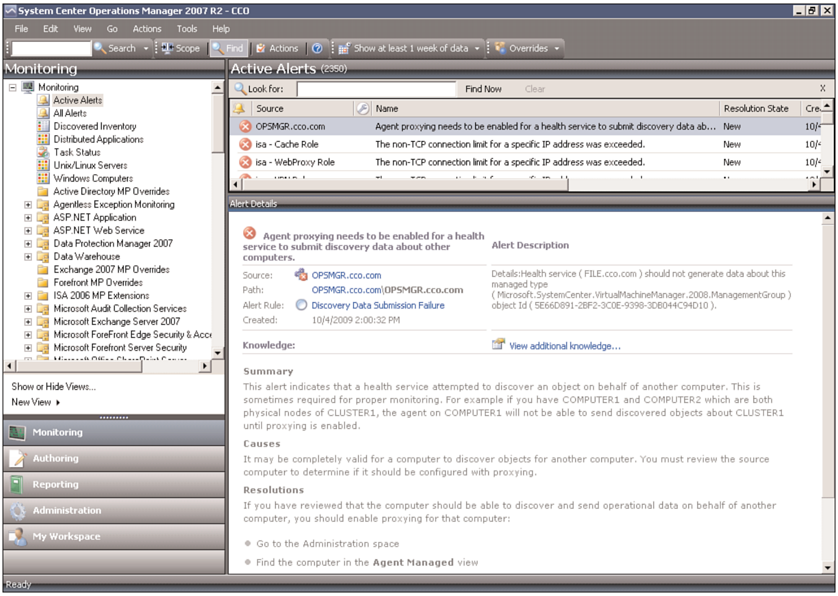
Agent Proxy Configuration

Operations Manager 2007 R2 has a variety of security measures built in to the product to prevent security breaches. One measure in particular is the prevention of impersonation of one agent by another. That is, an agent SERVER1 cannot insert operations data into the database about a domain controller DC1. This could constitute a security violation, where SERVER1 could maliciously generate fraudulent emergencies by making it appear that DC1 was having operational issues.

Although this is normally a good feature, this can be a problem if, in fact, SERVER1 is monitoring DC1 from a client perspective. The Operations Manager infrastructure would reject any information presented about DC1 by SERVER1. When this occurs, the system generates an alert to indicate that an attempt to proxy operations data has occurred. Figure 23.9 shows an example of the alert. In the normal course of events, this alert is not an indication of an attack but rather a configuration problem.

To get around this problem, Agent Proxy can be selectively enabled for agents that need to be able to present operational data about other agents. To enable Agent Proxy for a computer, run the following steps:

1. Open the Operations Manager 2007 R2 console.
2. Select the Administration section.
3. Select the Agent Managed node.


System Center Operations Manager 2007 R2 - CCO
File Edit View Go Actions Tools Help
Search Scope Find Actions Show at least 1 week of data Overrides
Monitoring
Monitoring
Active Alerts
All Alerts
Discovered Inventory
Distributed Applications
Task Status
Unix/Linux Servers
Windows Computers
Active Directory MP Overrides
Agentless Exception Monitoring
ASP.NET Application
ASP.NET Web Service
Data Protection Manager 2007
Data Warehouse
Exchange 2007 MP Overrides
Forefront MP Overrides
ISA 2006 MP Extensions
Microsoft Audit Collection Services
Microsoft Exchange Server 2007
Microsoft ForeFront Edge Security & Acce
Microsoft Forefront Server Security
Show or Hide Views...
New View
Monitoring
Authoring
Reporting
Administration
My Workspace
Ready
Active Alerts (2350)
Look for:
Find Now
Clear
Alert Details

Source	Name	Resolution State	Cre
OPSMGR.cco.com	Agent proxying needs to be enabled for a health service to submit discovery data ab...	New	10/
isa - Cache Role	The non-TCP connection limit for a specific IP address was exceeded.	New	10/
isa - WebProxy Role	The non-TCP connection limit for a specific IP address was exceeded.	New	10/

Agent proxying needs to be enabled for a health service to submit discovery data about other computers.

Source: OPSMGR.cco.com
Path: OPSMGR.cco.com\OPSMGR.cco.com
Alert Rule: Discovery Data Submission Failure
Created: 10/4/2009 2:00:32 PM

Alert Description

Details:Health service (FILE.cco.com) should not generate data about this managed type (Microsoft.SystemCenter.VirtualMachineManager.2008.ManagementGroup) object Id (5E66D891-2BF2-3C0E-9398-3DB044C94D10).

Knowledge: View additional knowledge...

Summary

This alert indicates that a health service attempted to discover an object on behalf of another computer. This is sometimes required for proper monitoring. For example if you have COMPUTER1 and COMPUTER2 which are both physical nodes of CLUSTER1, the agent on COMPUTER1 will not be able to send discovered objects about CLUSTER1 until proxying is enabled.

Causes

It may be completely valid for a computer to discover objects for another computer. You must review the source computer to determine if it should be configured with proxying.

Resolutions

If you have reviewed that the computer should be able to discover and send operational data on behalf of another computer, you should enable proxying for that computer:

- Go to the Administration space
- Find the computer in the **Agent Managed** view

FIGURE 23.9 Agent Proxy alert.

4. Right-click the agent in the right pane and select Properties.
5. Click the Security tab.
6. Check the Allow This Agent to Act as a Proxy and Discover Managed Objects on Other Computers check box.
7. Click OK to save.

Repeat this for all agents that need to act as proxy agents.

NOTE

Because the alerts generated by this condition are rule-based and not monitor-based, the alert needs to be manually resolved by right-clicking on it and selecting Close Alert.

Active Directory Client Monitoring Configuration

Although monitoring performance of Active Directory services is done by the domain controllers using a variety of measures, sometimes what really matters is how clients perceive the performance of the domain services. To measure that, the Windows Server 2008 Active Directory management pack can generate synthetic transactions from selected client systems. These transactions include ADSI bind and search times, LDAP ping and bind times, global catalog search times, and PDC ping and bind times. The clients execute tests and log the results, as well as alert on slow performance.

The Active Directory Server Client object discovery is disabled by default. The object discovery has to be overridden to discover objects that will then run the rules. To selectively override the Active Directory Server Client object discovery, run the following steps:

1. Open the Operations Manager 2007 R2 console.
2. Select the Authoring section.
3. Expand the Management Pack Object node.
4. Select the Object Discoveries node.
5. Select View, Scope.
6. In the Look For field, type `Client Perspective`. This narrows down the selections.
7. Check the Active Directory Client Perspective target and click OK.
8. Right-click the AD Client Monitoring Discovery and select Overrides, Override the Object Discovery, and For a Specific Object of Class: Windows Computer.
9. A list of Windows Computer objects will be displayed. Select the computer that will act as an Active Directory client and click OK.

NOTE

The selected Windows Computer should not be a domain controller.

10. Check the Override box next to Enabled and set the value to True.
11. In the Select Destination Management Pack pull-down menu, select the appropriate override management pack. If none exists, create one for the Active Directory management pack by clicking New.

NOTE

Never use the Default Management Pack for overrides. Always create an override management pack that corresponds to each imported management pack.

12. Click OK to save the override.
13. Repeat for each Windows computer that will be an Active Directory Server Client agent.

After a period of time, the selected agents will begin to generate Active Directory client perspective data and alerts. As a best practice, key Exchange servers are often selected as Active Directory Server Client agents. It is also a best practice to select at least one agent in each location to be an Active Directory Server Client agent as well.

Active Directory Replication Monitoring Configuration

The Active Directory management pack can monitor the replication latency between domain controllers in Active Directory. It uses sources and targets domain controllers, where the source domain controllers create objects in the OpsMgrLatencyMonitors container. These objects are read by the targets, which log performance data in the OpsMgr databases. There will be a replication counter for each domain partition, for the DomainDNSZones partition, and for the ForestDNSZones partition between each source and target pair. There will also be a counter for minimum replication latency and average replication latency.

The Active Directory management pack has the sources and targets disabled by default due to the number of counters that can potentially be created. Overrides need to be created for each source and each target domain controller to get the replication monitoring to function.

It is a best practice to reduce the number of sources and targets to a minimum, due to the number of counters that get created. An example of a source-target model might be to make all branch offices sources and a single central office DC as the target. Another example might be to pick a single DC in each site to be in both the source and target groups, assuming there are a limited number of sites.

The steps to set the source overrides are as follows:

1. Launch the Operations Manager 2007 R2 console.
2. Select the Authoring section.
3. Expand the Management Pack Objects node.
4. Ensure that the console is not scoped for any objects.
5. Select the Rules node.
6. In the Look For field, enter `sources` and click Find Now.
7. Select the rule “AD Replication Monitoring Performance Collection (Sources)” in the “Type: Active Directory Domain Controller Server 2008 Computer Role”.
8. Right-click the rule and select Overrides, Override the Rule, and For a Specific Object of Class: Active Directory Domain Controller Server 2008 Computer Role.
9. The Select Object window opens and shows matching objects. Select the domain controller that will be the source and click OK.
10. Check the Override box next to Enabled and set the value to True.
11. In the Select Destination Management Pack pull-down menu, select the appropriate override management pack. If none exists, create a new management pack named “Active Directory MP Overrides” by clicking New.

NOTE

Never use the Default Management Pack for overrides. Always create an override management pack that corresponds to each imported management pack.

12. Click OK to save the override.
13. Repeat for each domain controller that will be a source.

The steps to set the target overrides are as follows:

1. Launch the Operations Manager 2007 R2 console.
2. Select the Authoring section.
3. Expand the Management Pack Objects node.
4. Ensure that the console is not scoped for any objects.
5. Select the Rules node.
6. In the Look For field, enter `targets` and click Find Now.
7. Select the rule "AD Replication Monitoring Performance Collection (Targets)" in the "Type: Active Directory Domain Controller Server 2008 Computer Role".
8. Right-click the rule and select Overrides, Override the Rule, and For a Specific Object of Class: Active Directory Domain Controller Server 2008 Computer Role.
9. The Select Object window opens and shows matching objects. Select the domain controller that will be the source and click OK.
10. Check the Override box next to Enabled and set the value to True.
11. In the Select Destination Management Pack pull-down menu, select the appropriate override management pack. Use the same one from the previous steps when selecting the sources.
12. Click OK to save the override.
13. Repeat for each domain controller that will be a target.

After a period of time, monitoring will begin. Counters will be measuring the replication latency between the partitions. In addition, replication latency alerts will be triggered if latency falls below the predefined thresholds.

This sets the sources and targets for Windows Server 2008 domain controllers. For other versions such as Windows Server 2003 and Windows 2000 Server domain controllers, the overrides need to be created for those domain controllers separately. Also, the replication latency mechanism does not support cross-version replication latency measurement.

NOTE

It might be tempting to make all domain controllers both sources and targets. Each domain controller would then be connected to every other domain controller. This is also known as a full mesh. However, the problem is that the number of connections grows as a power of 2. The general function for the number of connection in a full mesh is:

f(x)= (x^2-x)/2

where x is the number of domain controllers and f(x) is the number of connections.

This means that 2 DCs will have 1 connection, 3 DCs will have 3 connections, 4 DCs will have 6 connections, and so on. By the time you get to 20 domain controllers, you have 190 connections. The connections are bidirectional and there are at least 5 counters that are collected per source-target pair, so for 20 DCs in a full mesh, there would be 1,900 performance counters (190 connections x 2 bidirectional x 5 counters) gathering data. Full mesh is bad!

Agent Restart Recovery

Agents will heartbeat every 60 seconds by default, contacting their management server to check for new rules and upload data. On the Root Management Server, there is a Health Service Watcher corresponding to each managed agent. If the Health Service Watcher for an agent detects three missed heartbeats in a row (that is, 3 minutes without a heartbeat), the Health Service Watcher executes a pair of diagnostics:

- First, the Health Service Watcher attempts to ping the agent.
- Second, the Health Service Watcher checks to see if the Health Service is running on the agent.

An alert is then generated for each of the diagnostics if they failed. If the agent is reachable via ping but the Health Service is stopped, there is a recovery to restart the Health Service. This allows the agent to recover automatically from stopped agent conditions.

The Restart Health Service Recovery is disabled by default. To enable the functionality, an override can be created for the Health Service Watcher objects. To enable the recovery, execute the following steps:

1. Open the Operations Manager 2007 R2 console.
2. Select the Authoring space.
3. Expand the Management Pack Objects node.
4. Select the Monitors node.
5. Select View, Scope.
6. Type `health service watcher` in the Look For field and click the View All Targets option button.
7. Select the Health Service Watcher target. Don't pick the ones with additional information in parentheses.
8. Click OK.
9. Type `Heartbeat Failure` in the Look For field and click Find Now.
10. Right-click the Health Service Heartbeat Failure aggregate rollup node and select Overrides, Override Recovery, Restart Health Service, and For All Objects of Class: Health Service Watcher.
11. Check the Override box next to Enabled and set the value to True.
12. In the Select Destination Management Pack pull-down menu, select the appropriate override management pack. If none exists, create a new management pack named "Operations Manager MP Overrides" by clicking New.

NOTE

Never use the Default Management Pack for overrides. Always create an override management pack that corresponds to each imported management pack.

13. Click OK to save the override.

Now if the Health Service is stopped on an agent, the Root Management Server will automatically attempt to restart it.

Notifications and Subscriptions

When alerts are generated in the console, there is a wealth of information available about the nature of the problem and how to troubleshoot and resolve it. However, most administrators will not be watching the console at all times. Operations Manager has a sophisticated notification mechanism that allows alerts to be forwarded to email, SMS, IM, or even a command-line interface. The most common method of alert notification is email.

However, Operations Manager generates a lot of alerts. If each one of these alerts were forwarded, this would overwhelm the average administrator's Inbox and prove totally useless. Operations Manager has two alert parameters to help categorize the alerts. Each alert has two parameters that help guide the notification process, severity and priority.

Alert Severity is the first and main parameter. There are three severity levels:

- **Critical (2)**—These alerts indicate that there is a problem that needs to be fixed immediately and is directly actionable (that is, there is something that can be done).
- **Warning (1)**—These alerts indicate that there is a problem, but that it might not be immediately impacting the environment or might not be directly actionable.
- **Information (0)**—These alerts indicate that there is something that is good to know, but might not be a problem nor is actionable.

By the nature of things, there are a lot more warning alerts generated than critical alerts. In general, notifications should only be sent out for critical alerts. That is, there should never be an email sent for a warning or informational alert.

Alert Priority is the second parameter that qualifies the alert status. The priority allows management pack authors to make some alerts more important than others. There are three levels of priority as well:

- High
- Medium
- Low

In general, a high-priority, critical severity alert is very important. This includes events like an agent down or a security breach. A medium-priority, critical severity alert is important. Both are generally actionable.

The best practice is to create two SMTP channels to deliver the alert notification emails, which are as follows:

- **SMTP (High Priority)**—High-priority email to an SMTP gateway
- **SMTP (Regular Priority)**—Regular email to an SMTP gateway

Then, create two notification subscriptions that use the Severity and the Priority to select the emails to be sent:

- Notification for All Critical Severity High-Priority Alerts
- Notification for All Critical Severity Medium-Priority Alerts

This provides a configuration that will deliver the very important alerts (high-priority critical severity alerts) via high-priority email and important alerts (medium-priority critical severity alerts) via regular email. All other alerts will be available in the console and no emails will be sent to notify of them.

The next sections will set up the notification infrastructure described previously.

The first step is to set up a channel, that is, how the emails will be sent. The steps are as follows:

1. Launch the Operations Manager 2007 R2 console.
2. Select the Administration space.
3. Select the Channels node.
4. Right-click the Channels node and select New Channel, E-Mail (SMTP).
5. Enter `SMTP Channel (High Priority)` for the channel name and click Next.
6. Click the Add button, enter the FQDN of the SMTP server, and click OK.
7. Enter a return SMTP address and click Next.
8. Change the Importance to High and click Finish. Click Close to close wizard.
9. Right-click the Channels node and select New Channel, E-Mail (SMTP).
10. Enter `SMTP Channel (Normal Priority)` for the channel name and click Next.
11. Click the Add button, enter the FQDN of the SMTP server, and click OK.
12. Enter a return SMTP address and click Next.
13. Leave the Importance at Normal and click Finish. Click Close to close wizard.

The second step is to set up the subscriber, that is, to whom the emails will be sent. The steps are as follows:

1. Launch the Operations Manager 2007 R2 console.
2. Select the Administration space.
3. Select the Subscribers node.
4. Right-click the Subscribers node and select New Subscriber.
5. Click the "…" button and select a user or distribution group. Click OK.
6. Click Next.
7. Click Next to always send notifications.
8. Click the Add button.
9. Type `Email` for the address name and click Next.
10. Select the Channel Type as E-Mail (SMTP) and enter the delivery email address.
11. Click Finish.
12. Click Finish again to save the subscriber. Click Close to exit the wizard.

NOTE

It is a best practice to use distribution lists rather than user email addresses for subscribers.

The last step is to set up the subscriptions, that is, what to notify on. The steps are as follows:

1. Launch the Operations Manager 2007 R2 console.
2. Select the Administration space.
3. Select the Subscriptions node.
4. Right-click the Subscriptions node and select New Subscription.
5. Enter `Notification for All Critical Severity High Priority Alerts` for the subscription name and click Next.
6. Check the Of a Specific Severity and the Of a Specific Priority check boxes.
7. In the Criteria Description pane, click the "Specific Severity" link, check the Critical check box, and click OK.
8. In the Criteria Description pane, click the "Specific Priority" link, check the High check box, and click OK.
9. Click Next.
10. Click the Add button, click Search, select the subscriber, click the Add button, and click OK.
11. Click Next.
12. Click the Add button, click Search, select the SMTP Channel (High Priority) channel, click the Add button, and click OK.
13. Click Next and then click Finish.
14. Right-click the Subscriptions node and select New Subscription.
15. Enter `Notification for All Critical Severity Medium Priority Alerts` for the subscription name and click Next.
16. Check the Of a Specific Severity and the Of a Specific Priority check boxes.
17. In the Criteria Description pane, click the "Specific Severity" link, check the Critical check box, and click OK.
18. In the Criteria Description pane, click the "Specific Priority" link, check the Medium check box, and click OK.
19. Click Next.
20. Click the Add button, click Search, select the subscriber, click the Add button, and click OK.
21. Click Next.
22. Click the Add button, click Search, select the SMTP Channel (Normal Priority) channel, click the Add button, and click OK.
23. Click Next and then click Finish.

Now, the subscribers will get email notifications for alerts based on the severity and priority. These severities and priorities are based on the judgments of the authors of the management packs, which might or might not be optimal for any given organization. Later in the chapter, the priority and severity of alerts will be used to tune the management packs to reduce alert noise.

Monitoring DMZ Servers with Certificates

Servers in an organization's demilitarized zone (DMZ) are usually not domain members and, thus, cannot do automatic mutual authentication with the OpsMgr server. However, these servers are the most exposed in the organization and, thus, critical to be monitored. Thankfully, there is a well-defined process for using certificates to handle the mutual authentication.

NOTE

This topic also applies to machines that are workgroup servers or servers that are members of domains where there is no trust to the OpsMgr domain.

Monitoring servers in the DMZ requires an install of certificate-based mutual authentication. This process has a lot of steps, but is straightforward. To install and configure certificates to allow the DMZ servers to use mutual authentication, the following five major tasks need to be completed:

1. Create a certificate template to issue the correct format of X.509 certificates for Operations Manager to use for mutual authentication.
2. Request the root CA certificate to trust the CA and the certificates it issues. This is done for each DMZ server and possibly for the management servers if not using an enterprise CA.
3. Request a certificate from the root CA to use for mutual authentication. This is done for each DMZ server and for each management server.
4. Install the Operations Manager agent manually. This is done for each DMZ server.
5. Configure the agent to use the certificate. This is done for each DMZ server and for each management server.

These various X.509 certificates are issued from a certificate authority, which could be a Windows Server 2008 R2 CA.

Creating a Certificate Template

This step creates a certificate template named Operations Manager that can be issued from the Windows Server 2008 R2 certification authority web enrollment page. The certificate template will support Server Authentication (OID 1.3.6.1.5.5.7.3.1) and Client Authentication (OID 1.3.6.1.5.5.7.3.2) as well as allow the name to be manually entered rather than autogenerated from Active Directory because the DMZ server will not be an Active Directory domain member.

The steps to create the security template are as follows:

1. Log on to the CA, which is DC1.companyabc.com in this example.
2. Launch Server Manager.
3. Expand Roles, Active Directory Certificate Services, and select Certificate Templates (*fqdn*).
4. Right-click the Computer template and select Duplicate Template.
5. Leave the version at Windows 2003 Server, Enterprise Edition and click OK.
6. On the General tab in the Template Display Name field, enter `Operation Manager`.
7. Select the Request Handling tab and mark the Allow Private Key to Be Exported option.
8. Select the Subject Name tab and select Supply in the Request option. Click OK at the warning.
9. Select the Security tab, select Authenticated Users, and check the Enroll right.
10. Click OK to save the template.
11. Select the Enterprise PKI to expose the CA.
12. Right-click the CA and select Manage CA.
13. In the certsrv console, expand the CA, right-click Certificates Templates, then select New, Certificate Template to Issue.
14. Select the Operations Manager certificate template and click OK.

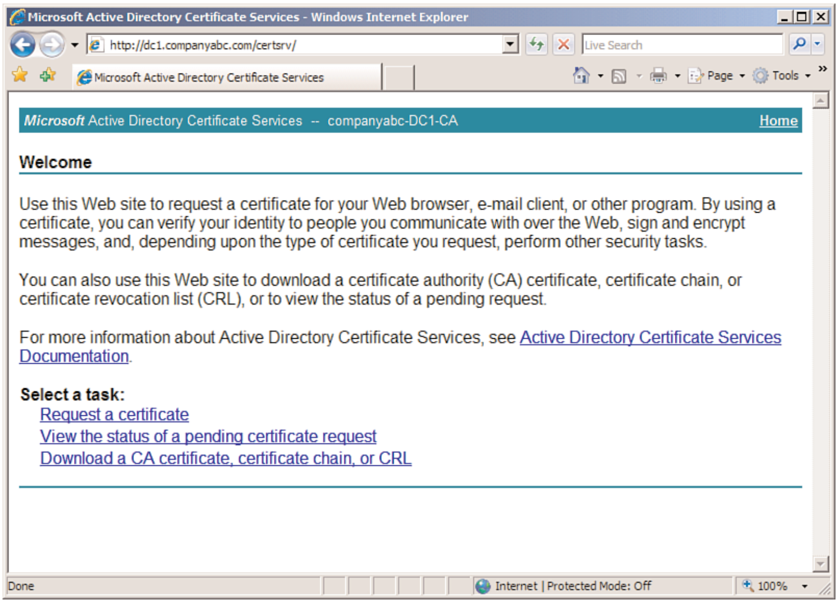
The new Operations Manager template will now be available in the Windows Server 2008 R2 web enrollment page.

Requesting the Root CA Server Certificate

This allows the DMZ server to trust the Windows Server 2008 R2 CA. This does not need to be done on the OpsMgr management servers, as the Windows Server 2008 R2 CA is an enterprise CA and all domain members automatically trust it. If the CA is not an enterprise CA, the steps need to be completed for the management servers as well.

To request and install the root CA certificate on the DMZ server, execute the following steps:

1. Log on to a DMZ server with local administrator rights.
2. Open a web browser and point it to the certificate server, in this case https://dc1.companyabc.com/certsrv. Enter credentials if prompted.
3. Click the Download a CA Certificate, Certificate Chain, or CRL link (shown in Figure 23.10).
4. Click the Download CA Certificate link. Note: If the certificate does not download, add the site to the Local Intranet list of sites in Internet Explorer.
5. Click Open to open the CA certificate.
6. Click Install Certificate to install the CA certificate.


Microsoft Active Directory Certificate Services - Windows Internet Explorer
http://dc1.companyabc.com/certsrv/
Live Search
Microsoft Active Directory Certificate Services
Page
Tools
Done
Internet | Protected Mode: Off
100%

Microsoft Active Directory Certificate Services -- companyabc-DC1-CA Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

FIGURE 23.10 Downloading a root CA certificate.

7. At the Certificate Import Wizard screen, click Next.
8. Select Place All Certificates in the Following Store option button.
9. Click Browse.
10. Click the Show Physical Stores check box.
11. Expand the Trusted Root Certification Authorities folder and select the local computer store.
12. Click OK.
13. Click Next, Finish, and OK to install the CA certificate.
14. Close any open windows.

Repeat for all DMZ servers. Now the DMZ servers will trust certificates issued by the certification authority. The next step is to request the certificates to use for the mutual authentication for all servers.

Requesting a Certificate from the Root CA Server

Each of the management servers and the servers in the DMZ will need to be issued certificates to use for communication.

The steps to request a certificate are as follows:

1. Log on as an administrator, then open a web browser and point it to the certificate server (in this case, https://dc1.companyabc.com/certsrv).
2. Click the Request a Certificate link.

3. Click the Advanced Certificate Request link.
4. Click the Create and Submit a Request to This CA link.
5. In the Type of Certificate Template field, select Operations Manager.
6. In the Name field, enter the FQDN (fully qualified domain name) of the target server.

NOTE

Go to the actual server to get the name! On the server, go to Computer Properties, Computer Name. Copy the full computer name and paste it into the Name field of the form.

7. Click Submit.
8. Click Yes when you get the warning pop-up.
9. Click Install This Certificate.
10. Click Yes when you see the warning pop-up. The certificate is now installed in the user certificate store.

NOTE

The certificate was installed in the user certificate store, but needs to be in the local computer store for Operations Manager. The ability to use web enrollment to directly place the certificate into the local computer store was removed from the Windows Server 2008 web enrollment, so the certificate needs to be moved manually.

11. Select Start, Run and then enter `mmc` to launch an MMC console.
12. Select File and Add/Remove Snap-In.
13. Select Certificates and click the Add button.
14. Select My User Account and click Finish.
15. Select Certificates again and click the Add button.
16. Select Computer Account and click Next.
17. Select the local computer, click Finish, and then click OK.
18. Expand the Certificates – Current User, Personal, and select the Certificates folder.
19. In the right pane, right-click the certificate issued earlier and select All Tasks, Export. The certificate can be recognized by the certificate template name Operations Manager.
20. At the Certificate Export Wizard, click Next.
21. Select Yes, Export the Private Key. Click Next.
22. Click Next.
23. Enter in a password and click Next.

24. Enter in a directory and filename and click Next.
25. Click Finish to export the certificate. Click OK at the pop-up.
26. Expand the Certificates (Local Computer), Personal, and select the Certificates folder.

NOTE

If this is the first certificate in the local computer store, the Certificates folder will not exist. Simply select the Personal folder instead and the Certificates folder will be created automatically.

27. Right-click in the right pane and select All Tasks, Import.
28. At the Certificate Import Wizard, select Next.
29. Click Browse to locate the certificate file saved earlier. Change the file type to Personal Information Exchange (`.pfx`) to see the file. Click Next.
30. Enter in the password used earlier, select the Mark This Key as Exportable, and click Next.
31. Click Next.
32. Click Finish and then click OK at the pop-up to complete the import.

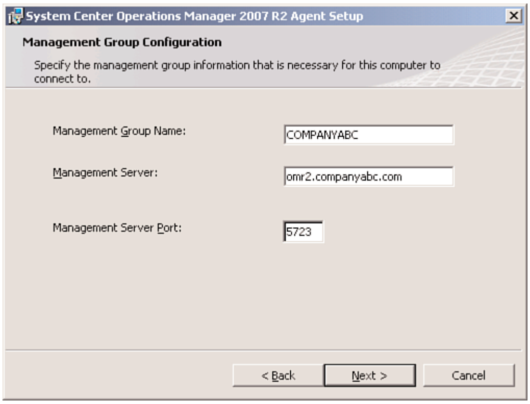
The preceding steps need to be completed for each DMZ server and for each management server.

Installing the Agent on the DMZ Server

The agent needs to be installed manually on each DMZ server. Normally, agents would be pushed by the Operations Manager console, but DMZ servers typically reside in the DMZ and are not members of the domain.

The steps to manually install the agent are as follows:

1. Log on as an administrator and insert the OpsMgr 2007 R2 installation media.
2. At the AutoPlay menu, select Run SetupOM.exe.
3. Select Install Operations Manager 2007 R2 Agent from the menu.
4. Click Next.
5. Click Next to accept the default directory.
6. Click Next to specify management group information.
7. Type in the management group name and FQDN of the management server. Keep the default management server port as 5723. The example shown in Figure 23.11 has `COMPANYABC` as the management group name and `omr2.companyabc.com` as the management server.



Management Group Configuration

Specify the management group information that is necessary for this computer to connect to.

Management Group Name: COMPANYABC

Management Server: omr2.companyabc.com

Management Server Port: 5723

FIGURE 23.11 Manually entered management group information.

8. Click Next.
9. Click Next at the Agent Action Account page to leave the local system as the action account.
10. Click Install to complete the installation.
11. When the installer is finished, click Finish.

The preceding steps need to be completed for each DMZ server.

The agent is installed, but will not communicate correctly with the management server. This is because the agent has not been configured to use the certificate for mutual authentication. This will be done in the next section.

Configuring the Agent to Use the Certificate

After the agent is installed, the agent still needs to be configured to use the correct certificate. The OpsMgr installation includes a utility called `MOMCertImport.exe` that configures the agent to use certificates for authentication and specifies which certificate in the local computer store to use. The tool does not do any validation checking of the certificate itself, so care needs to be taken that the correct certificate is selected.

The steps to configure the agent to use a certificate are as follows:

1. Log on as an administrator on the DMZ server and insert the OpsMgr 2007 R2 installation media.
2. At the AutoPlay menu, select Run SetupOM.exe.
3. Select Browse This CD from the menu.
4. Select the SupportTools directory and then the AMD64 directory.

NOTE

Windows Server 2008 R2 is a 64-bit operating system, so the AMD64 is the correct folder for the 64-bit binaries. If the procedure is being run for 32-bit servers, select the appropriate directory for the binaries such as i386.

5. In the directory, double-click `MOMCertImport.exe`.
6. In the pop-up window, select the certificate issued previously and click OK. The View Certificate button can be used to view the certificate details if the correct certificate is not obvious.

The Operation Manager service will restart automatically to have the certificate selection take effect. The preceding steps need to be repeated for each DMZ server and for each management server.

The Operations Manager event log can be viewed with the Windows Event Viewer. It is named Operations Manager and is located in the Applications and Services Logs folder in the tool. Any problems with the certificate will be shown in the log immediately following the start of the System Center Management service.

Using Operations Manager 2007 R2

After Operations Manager 2007 R2 has been installed and configured, ongoing work needs to be done to ensure that the product performs as expected. The two primary activities are to, first, tune the management packs to ensure that alerts are valid for the environment and that alert noise is reduced and, second, produce reports of the information that Operations Manager 2007 R2 is collecting.

Alert Tuning

After deploying Operations Manager 2007 R2, there are frequently complaints about the number of alert notifications that get generated. This can cause organizations to decommission the product, ignore the emails, or generally complain about what a bad product it is. In reality, the Operations Manager alert notifications just need to be tuned.

The following process will help you tune the management packs quickly and effectively to reduce alert and email noise. This is done by adjusting parameters on the rules (Enable/Disable, Severity, and Priority) using overrides.

Alert Severity is the first parameter to be tuned. There are three levels:

- Critical (2)
- Warning (1)
- Information (0)

The numeric value of the severity is given as well, as some rules and monitors will show the severity as a value rather than as text.

Alert Priority is the second parameter to be tuned. There are three levels of priority as well:

- High
- Medium
- Low

These tuning procedures assume that the notification subscriptions were created that were outlined in the "Notifications and Subscriptions" section earlier in the chapter. These notification subscriptions are as follows:

- Notification for All Critical Severity High-Priority Alerts
- Notification for All Critical Severity Medium-Priority Alerts

When you get an email from an alert that you don't want, you need to tune the management pack monitor or rule. The basic decision tree is as follows:

A. **Disable the Alert?** If yes, create an override to disable the rule for either the instance of the object, the class of objects, or a group of the objects. This prevents the alert from being generated, so no console alerts and definitely no emails are generated. This would be done if the alert does not reflect a real problem.

B. **Change Severity?** If yes, create an override to change the alert severity to Warning. This keeps the alert in the console as a warning, but does not generate an email. This would be done if the alert is real, but is not actionable.

C. **Change Priority?** If yes, create an override to change the alert priority to low. This keeps the alert as a critical alert, but prevents an email from being generated. This would be done if the alert is real, but is not resolvable in the immediate future.

D. **Change Threshold?** For performance-based alerts, there is the option to change the trigger threshold to a different value. This would be done if the problem is real and actionable, but the alert is firing too soon.

These options can be taken for all objects of the target class, for just the specific instance that generated the alert, or for a group. The group would have to be created in advance and would have to contain objects of the type targeted by the monitor or rule generating the alert.

For example, let's say there is an Application of Group Policy critical alert that is occurring frequently in the environment. It is occurring on a number of Windows Server 2008 R2 servers and is generating a lot of email notifications. This alert is valid, but does not require immediate action. The alert needs to be tuned to change the severity from critical to warning. The steps to tune the alert are as follows:

1. Open the Operations Manager 2007 R2 console.
2. Select the Monitoring space.
3. Select the Active Alerts view.
4. Locate and select the Application of Group Policy alert that is to be tuned.

5. Right-click the alert and select Overrides, Override the Monitor, and For All Objects of Class: Group Policy 2008 Runtime. This overrides the alert for all objects of that class.

NOTE

The alert is to be tuned for all objects, rather than any specific instances. If the alert is to be tuned for the specific instance that raised the alert, the For the Object option should be chosen. If it is a group of the objects, the For a Group option should be chosen. The group would have to be precreated and be a group of the target objects.

6. Check the Override box next to Alert Severity and set the value to Warning.
7. In the Select Destination Management Pack pull-down menu, select the appropriate override management pack. If none exists, create a new override management pack named "Group Policy MP Overrides" by clicking New.

NOTE

Never use the Default Management Pack for overrides. Always create an override management pack that corresponds to each imported management pack.

8. Click OK to save the override.

Now the next time the monitor triggers an alert, it will be of warning severity and will not generate a notification email. However, the alert can still be reviewed in the console.

This approach to tuning will address 90% of the noisy alerts that you get. To target the noisiest alerts, see the report Most Common Alerts in the next section. This helps identify the alerts that are responsible for the most noise. You'll frequently find that 50% of your alerts are coming from less than five rules or monitors. Tuning those will give you the most bang for your buck.

Scheduling Reports

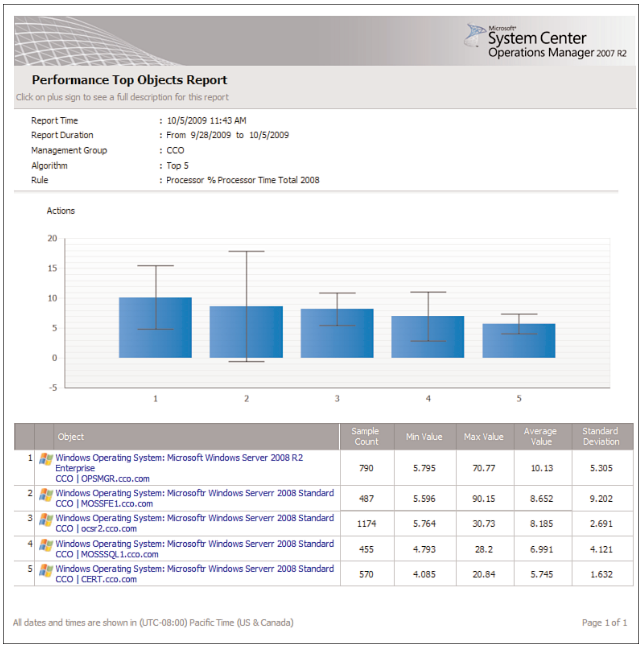
The Operations Manager 2007 R2 infrastructure collects many Windows Server 2008 R2 data points. This information can be presented in reports, which can be generated ad hoc or scheduled. The scheduling option is very useful, as it reduces the need to actively open the console and instead the reports are delivered via email.

Performance Reports

When managing a number of agents, it can be difficult to pinpoint the problem systems. For example, which systems are the most heavily utilized? A report showing a graph of all the resources would be very messy and difficult to read even in a medium-sized organization with a number of servers. Operations Manager 2007 R2 has a set of reports that address this specific concern, the Performance Top Objects and Performance Top

Instances. These reports take data from performance collection rules, perform some statistical analysis, and list the top systems.

For example, Figure 23.12 shows the top five systems with the most processor utilization. It is based on the “Processor % Processor Time Total 2008” rule. It shows the top five heaviest processor utilization systems for the previous week.



Performance Top Objects Report

Click on plus sign to see a full description for this report

Report Time	: 10/5/2009 11:43 AM
Report Duration	: From 9/28/2009 to 10/5/2009
Management Group	: CCO
Algorithm	: Top 5
Rule	: Processor % Processor Time Total 2008

	Object	Sample Count	Min Value	Max Value	Average Value	Standard Deviation
1	Windows Operating System: Microsoft Windows Server 2008 R2 Enterprise CCO | OPSMGR.cco.com	790	5.795	70.77	10.13	5.305
2	Windows Operating System: Microsoftr Windows Serverr 2008 Standard CCO | MOSSFE1.cco.com	487	5.596	90.15	8.652	9.202
3	Windows Operating System: Microsoftr Windows Serverr 2008 Standard CCO | ocsr2.cco.com	1174	5.764	30.73	8.185	2.691
4	Windows Operating System: Microsoftr Windows Serverr 2008 Standard CCO | MOSSSQL1.cco.com	455	4.793	28.2	6.991	4.121
5	Windows Operating System: Microsoftr Windows Serverr 2008 Standard CCO | CERT.cco.com	570	4.085	20.84	5.745	1.632

All dates and times are shown in (UTC-08:00) Pacific Time (US & Canada)

Page 1 of 1

FIGURE 23.12 Top five processor utilization report.

This report is one of the reports in the Microsoft Generic Report Library and can be used against any performance counter. The report can pick the top (the default) or bottom objects, as well as vary the number of objects to return (the default is five).

The best-practice recommendation is to generate daily reports spanning the previous week for the following rules:

- Processor % Processor Time Total 2008
- Page File Percentage Use 2008
- Memory % Committed Bytes in Use 2008
- Network Adapter Bytes Total per Second 2008
- % Logical Disk Free Space 2008

The Performance Top Objects report for each of these rules gives a good overview of the performance issues (or lack thereof) over the collection of all the monitored systems. These should be delivered on a daily basis in an email or to a share.

To schedule a report for email delivery, use the following steps:

1. Launch the Operations Manager 2007 R2 console.
2. Select the Reporting space.
3. Select the Microsoft Generic Report Library node.
4. Right-click the Performance Top Objects report and select Open.
5. In the From field, select Advanced.
6. Change the Offset to minus and the number of days to 7. Click the green check mark (OK) to save the selections. The From field will show "Today -7 day(s)".
7. Change both the From and the To times to 12:00 AM.
8. In the Rule field, click the Browse button.
9. In the Rule Name field, enter `Processor % Processor Time Total 2008` and click the Search button.
10. In the Available Items pane, select the rule and click OK.
11. Click Run and confirm that the report looks good.
12. Select File, Schedule.
13. In the Description, enter `Processor % Processor Time Total 2008 Report`.
14. In the Delivery Method field, select Email.
15. In the To field, enter the SMTP address of the recipient.
16. In the Subject field, replace @ReportName with `Processor % Processor Time Total 2008 Report`. The variable name is unfortunately very long and ugly, so it's best to replace it.
17. Click Next.
18. Change the schedule to Daily.
19. Change the time to be the time that the report should be generated on a daily basis, for example 6:00 a.m. Click Next.
20. Because the report was generated and all the parameters were selected initially, no parameters need to be changed. This method ensures that the email report will match expectations.
21. Click Finish to save the scheduled report.

The report will now be automatically generated every morning at 6:00 a.m. and delivered via email to the recipients. Additional reports can be created in exactly the same way for the recommended rules and any others that are needed. To review the schedules, go to the Scheduled Reports node in the Reporting space. The schedules can be adjusted as well.

NOTE

The performance rules are generally specific to each operating system. Thus, the reports are specific to each operating system. The rules in this section reflect Windows Server 2008 and Windows Server 2008 R2 performance data. If there are other operating systems such as Windows Server 2003, additional reports using those rules would need to be created.

OpsMgr 2007 R2 Maintenance Reports

There are also reports on Operations Manager 2007 R2 that should be generated to ensure that the health and performance of the infrastructure is good. The reports to generate are as follows:

- **Most Common Alerts—**This report is useful for determining what alerts are the noisiest and might be spamming the Inboxes of notification subscribers. The report shows which alerts are most common and gives additional statistical analysis.
- **Alert Logging Latency—**This report is useful for determining the health of the OpsMgr infrastructure, as measured by the time an event occurs on a managed computer to the time an alert is raised. If this is too long (that is, greater than 30 seconds), it indicates that there is a problem.
- **SQL Database Space report—**This report shows the database space and growth of SQL databases. This is generated against the OpsMgr databases to monitor the growth.

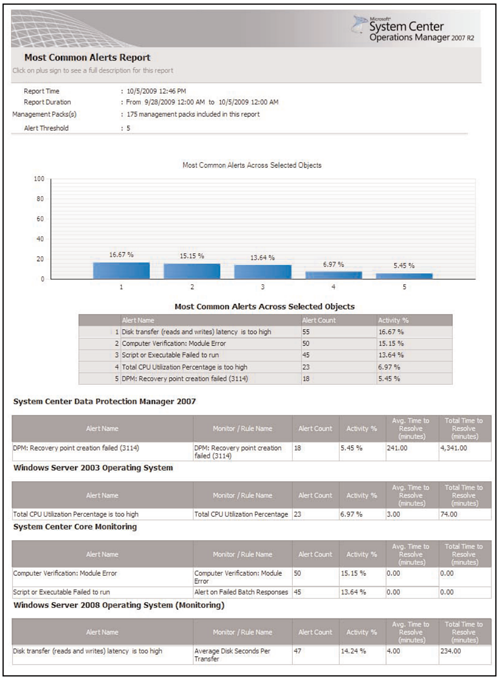
These reports should be generated on a weekly basis (for example, Monday at 6:00 a.m.) spanning the previous week and be sent to the Operations Manager administrators.

The Most Common Alerts report is based on the management packs that are installed. By default, the report selects all the installed management packs and shows the top five most common alerts. To schedule the Most Common Alerts report, execute the following steps:

1. Launch the Operations Manager 2007 R2 console.
2. Select the Reporting space.
3. Select the Microsoft Generic Report Library node.
4. Right-click the Most Common Alerts report and select Open.
5. In the From field, select Advanced.
6. Change the Offset to minus and the number of days to 7. Click the green check mark (OK) to save the selections. The From field will show “Today -7 day(s)”.
7. Change both the From and the To times to 12:00 AM.
8. Click Run and confirm that the report looks good.
9. Select File, Schedule.
10. In the Description, enter `Most Common Alerts Report`.
11. In the Delivery Method field, select Email.
12. In the To field, enter the SMTP address of the recipient.

13. In the Subject field, replace @ReportName with `Most Common Alerts Report`.
14. Click Next.
15. Change the schedule to Weekly and ensure that only Mon is checked.
16. Change the time to be the time that the report should be generated on a daily basis, for example 6:00 a.m. Click Next.
17. Because the report was generated and all the parameters were selected initially, no parameters need to be changed. This method ensures that the email report will match expectations.
18. Click Finish to save the scheduled report.

Figure 23.13 shows an example of the Most Common Alerts report. The most common alert for the previous week was the Disk Transfer Latency Is Too High, with 16.67% of alerts. This alert could be tuned to reduce the volume of alerts or the problem resolved.



Most Common Alerts Report

Click on plus sign to see a full description for this report

Report Time	: 10/5/2009 12:46 PM
Report Duration	: From 9/28/2009 12:00 AM to 10/5/2009 12:00 AM
Management Packs(s)	: 175 management packs included in this report
Alert Threshold	: 5

Most Common Alerts Across Selected Objects

	Alert Name	Alert Count	Activity %
1	Disk transfer (reads and writes) latency is too high	55	16.67 %
2	Computer Verification: Module Error	50	15.15 %
3	Script or Executable Failed to run	45	13.64 %
4	Total CPU Utilization Percentage is too high	23	6.97 %
5	DPM: Recovery point creation failed (3114)	18	5.45 %

System Center Data Protection Manager 2007

Alert Name	Monitor / Rule Name	Alert Count	Activity %	Avg. Time to Resolve (minutes)	Total Time to Resolve (minutes)
DPM: Recovery point creation failed (3114)	DPM: Recovery point creation failed (3114)	18	5.45 %	241.00	4,341.00

Windows Server 2003 Operating System

Alert Name	Monitor / Rule Name	Alert Count	Activity %	Avg. Time to Resolve (minutes)	Total Time to Resolve (minutes)
Total CPU Utilization Percentage is too high	Total CPU Utilization Percentage	23	6.97 %	3.00	74.00

System Center Core Monitoring

Alert Name	Monitor / Rule Name	Alert Count	Activity %	Avg. Time to Resolve (minutes)	Total Time to Resolve (minutes)
Computer Verification: Module Error	Computer Verification: Module Error	50	15.15 %	0.00	0.00
Script or Executable Failed to run	Alert on Failed Batch Responses	45	13.64 %	0.00	0.00

Windows Server 2008 Operating System (Monitoring)

Alert Name	Monitor / Rule Name	Alert Count	Activity %	Avg. Time to Resolve (minutes)	Total Time to Resolve (minutes)
Disk transfer (reads and writes) latency is too high	Average Disk Seconds Per Transfer	47	14.24 %	4.00	234.00

FIGURE 23.13 Most Common Alerts report.

The Alert Logging Latency report is based on the objects selected. The report does not include any objects by default, so the objects must be selected. It is a best practice to select the groups of agents, agentless, and agent watchers objects. To schedule the Alert Logging Latency report, execute the following steps:

1. Launch the Operations Manager 2007 R2 console.
2. Select the Reporting space.
3. Select the Microsoft Generic Report Library node.
4. Right-click the Alert Logging Latency report and select Open.
5. In the From field, select Advanced.
6. Change the Offset to minus and the number of days to 7. Click the green check mark (OK) to save the selections. The From field will show "Today -7 day(s)".
7. Change both the From and the To times to 12:00 AM.
8. Click the Add Group button.
9. In the Group Name field, enter `agent` and click the Search button.
10. Select the Agent Managed Computer Group, the Agentless Managed Computer Group, and the Microsoft.SystemCenter.AgentWatchersGroup and click the Add button.
11. Click OK to save the selections.
12. Click Run and confirm that the report looks good.
13. Select File, Schedule.
14. In the Description, enter `Alert Logging Latency Report`.
15. In the Delivery Method field, select Email.
16. In the To field, enter the SMTP address of the recipient.
17. In the Subject field, replace @ReportName with `Alert Logging Latency Report`.
18. Click Next.
19. Change the schedule to Weekly and ensure that only Mon is checked.
20. Change the time to be the time that the report should be generated on a daily basis, for example 6:00 a.m. Click Next.
21. Because the report was generated and all the parameters were selected initially, no parameters need to be changed. This method ensures that the email report will match expectations.
22. Click Finish to save the scheduled report.

The Alert Logging Latency report will now generate on a weekly basis and be emailed to the recipients. The report has two pages with lots of statistical analysis of the alert latency. It is one of the more complicated reports in the OpsMgr library of reports.

Finally, the SQL Database Space report is based on the databases. This report does not have any objects selected by default, so the Operations Manager database objects will need to be selected. To schedule the SQL Database Space report, run the following steps:

1. Launch the Operations Manager 2007 R2 console.
2. Select the Reporting space.
3. Select the SQL Server 2008 (Monitoring) node.
4. Right-click the SQL Database Space report and select Open.

5. In the From field, select Advanced.
6. Change the Offset to minus and the number of days to 7. Click the green check mark (OK) to save the selections. The From field will show “Today -7 day(s)”.
7. Change both the From and the To times to 12:00 AM.
8. Click the Add Object button.

NOTE

When the Add Object window appears, note that there is a caution triangle with the text “Filter Options Have Been Applied.” The objects returned will only be those that match the report criteria, in the case of SQL database objects. This is new to Operations Manager 2007 R2. Before this, all object classes would be returned and it was difficult to ensure that the correct objects were included in the report. Many times, reports would be returned without any data at all due to the incorrect objects being selected. This is a huge improvement in OpsMgr 2007 R2.

9. In the Object Name field, enter `Operations` and click the Search button.
10. Select all the OperationsManager databases and click the Add button.
11. Click OK to save the selections.
12. Click Run and confirm that the report looks good.
13. Select File, Schedule.
14. In the Description, enter `Operations Manager Database Space Report`.
15. In the Delivery Method field, select Email.
16. In the To field, enter the SMTP address of the recipient.
17. In the Subject field, replace @ReportName with `Operations Manager Database Space Report`.
18. Click Next.
19. Change the schedule to Weekly and ensure that only Mon is checked.
20. Change the time to be the time that the report should be generated on a daily basis, for example 6:00 a.m. Click Next.
21. Because the report was generated and all the parameters were selected initially, no parameters need to be changed. This method ensures that the email report will match expectations.
22. Click Finish to save the scheduled report.

The SQL Database Space report will be delivered every week on Monday at 6:00 a.m.

These three reports help ensure that the Operations Manager 2007 R2 infrastructure is healthy and performing well.

Summary

System Center Operations Manager 2007 is key to managing Windows Server 2008 R2. It can also be used in Windows 2003/2008 or mixed environments to provide for automated monitoring of all vital operating system, application, and network functionality. This type of functionality is instrumental in reducing downtime and getting the most out of a Windows Server 2008 R2 investment. In a nutshell, OpsMgr is an effective way to gain proactive, rather than reactive, control over the entire environment.

Best Practices

The following are best practices from this chapter:

- Deploy System Center Operations Manager 2007 R2 for monitoring Windows Server 2008 R2.
- Install the Windows Operating System, Active Directory, DNS, IIS, and Windows Server 2008 R2 management packs into OpsMgr to monitor network systems and applications that Windows Server 2008 R2 depends on.
- Deploy Operations Manager components on Windows 64-bit and SQL 64-bit for optimal performance.
- Create override management packs for each application management pack, such as the Windows Server 2008 R2 management pack. Don't use the Default Management Pack.
- Take future expansion and relevance of hardware into account when sizing servers for OpsMgr deployment.
- Keep the installation of OpsMgr on a separate server or set of separate dedicated member servers that do not run any other separate applications.
- Use SQL Server Reporting Services to produce custom reports using OpsMgr's reporting feature.
- Start with a single management group and add on additional management groups only if they are absolutely necessary.
- Use a dedicated service account for OpsMgr.
- Allocate adequate space for the databases depending on the length of time needed to store events and the number of managed systems.
- Monitor the size of the OpsMgr database to ensure that it does not increase beyond the bounds of acceptable size.
- Leverage the reporting database to store and report on data over a long period.

- Modify the grooming interval to aggressively address environmental requirements.
- When tuning, err on the side of fewer alerts. If nothing will be done about an alert, make sure it doesn't send a notification email.
- When tuning, use the Most Common Alerts report to see which alerts are the most valuable targets for tuning.
- Configure OpsMgr to monitor itself.