

Infrastructure Planning  
and Design

Microsoft® System Center Operations   
Manager 2007

Version 2.1

Published: June 2008

Update: July 2010

For the latest information, please see [www.microsoft.com/IPD](http://www.microsoft.com/IPD)

Copyright © 2010 Microsoft Corporation. This documentation is licensed to you under the Creative Commons Attribution License.  To view a copy of this license, visit <http://creativecommons.org/licenses/by/3.0/us/> or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.  When using this documentation, provide the following attribution: Infrastructure Planning and Design is provided with permission from Microsoft Corporation.

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS". Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user’s particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation. Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet website references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, email addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, Active Directory, SharePoint, SQL Server, Visio, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries and regions.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

You have no obligation to give Microsoft any suggestions, comments or other feedback (“Feedback”) relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback. You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

[The Planning and Design Series Approach 1](#_Toc265590858)

[Introduction to the System Center Operations Manager 2007 Guide 2](#_Toc265590859)

[System Center Operations Manager 2007 in Microsoft Infrastructure Optimization 5](#_Toc265590860)

[System Center Operations Manager 2007 Design Process 6](#_Toc265590861)

[Step 1: Define the Scope of the System Center Operations Manager 2007 Project 10](#_Toc265590862)

[Step 2: Identify Necessary Management Packs and Product Connectors 15](#_Toc265590863)

[Step 3: Determine How Monitoring Will Be Implemented 18](#_Toc265590864)

[Step 4: Determine the Number of Management Groups 21](#_Toc265590865)

[Step 5: Determine the Agent Security Model 25](#_Toc265590866)

[Step 6: Design and Place the System Center Operations Manager Server 2007 Roles 28](#_Toc265590867)

[Step 7: Design the OperationsManager Database, ACS Database, and AEM File Share 35](#_Toc265590868)

[Step 8: Design the Notification System 40](#_Toc265590869)

[Step 9: Determine Whether to Implement Reporting 42](#_Toc265590870)

[Step 10: Design the Data Warehouse, Reporting Server, and Service Level Dashboard 44](#_Toc265590871)

[Step 11: Design the Network Connections 47](#_Toc265590872)

[Conclusion 49](#_Toc265590873)

[Appendix: Job Aids 51](#_Toc265590874)

[Version History 59](#_Toc265590875)

[Acknowledgments 60](#_Toc265590876)

# 

# The Planning and Design Series Approach

This guide is one in a series of planning and design guides that clarify and streamline the planning and design process for Microsoft® infrastructure technologies.

Each guide in the series addresses a unique infrastructure technology or scenario. These guides include the following topics:

* Defining the technical decision flow (flow chart) through the planning process.
* Describing the decisions to be made and the commonly available options to consider in making the decisions.
* Relating the decisions and options to the business in terms of cost, complexity, and other characteristics.
* Framing the decision in terms of additional questions to the business to ensure a comprehensive understanding of the appropriate business landscape.

The guides in this series are intended to complement and augment the product documentation.

## Benefits of Using This Guide

Using this guide will help an organization to plan the best architecture for the business and to deliver the most cost-effective Microsoft System Center Operations Manager 2007 technology.

Benefits for Business Stakeholders/Decision Makers:

* Most cost-effective design solution for an implementation. Infrastructure Planning and Design (IPD) eliminates over-architecting and overspending by precisely matching the technology solution to the business needs.
* Alignment between the business and IT from the beginning of the design process to the end.

Benefits for Infrastructure Stakeholders/Decision Makers:

* Authoritative guidance. Microsoft is the best source for guidance about the design of Microsoft products.
* Business validation questions to ensure the solution meets the requirements of both business and infrastructure stakeholders.
* High integrity design criteria that includes product limitations.
* Fault-tolerant infrastructure, where necessary.
* Proportionate system and network availability to meet business requirements. Infrastructure that is sized appropriately to meet business requirements.

**Benefits for** Consultants or Partners:

* Rapid readiness for consulting engagements.
* Planning and design template to standardize design and peer reviews.
* A “leave-behind” for pre- and post-sales visits to customer sites.
* General classroom instruction/preparation.

Benefits for the Entire Organization:

Using this guide should result in a design that will be sized, configured, and appropriately placed to deliver a solution for achieving stated business requirements, while considering the performance, capacity, manageability, and fault tolerance of the system.

# Introduction to the System Center Operations Manager 2007 Guide

This guide leads the reader through the process of planning a System Center Operations Manager 2007 (Operations Manager 2007) infrastructure. The process in this guide applies to both Operations Manager 2007 and Operations Manager 2007 R2, except where content that is new in R2 is explicitly indicated. The guide addresses the following fundamental decisions and tasks:

* Identifying which services, applications, and infrastructure need to be monitored.
* Determining the resources needed to employ Operations Manager 2007 to monitor the selected resources.
* Designing the components, layout, security, and connectivity of the Operations Manager 2007 infrastructure.

Business objectives should be prioritized at the start of the project so that they are clearly understood and agreed upon by IT and business managers. Certain features require additional licensing or infrastructure costs; before adding those features, planners should inform the business of the extra costs involved.

## What’s New in System Center Operations Manager 2007 R2

This guide has been revised to include these new enhancements in System Center Operations Manager 2007 that may, or may not, affect the infrastructure choices and design:

* UNIX and Linux monitoring. Agents are now available to discover, monitor, and manage a number of UNIX and Linux platforms.
* Integrated and customizable service level tracking. The Operations Manager 2007 Data Warehouse database includes all of the customization required for service level tracking and is ready to provide data to the Service Level Dashboard (available as a Solution Accelerator).
* Enhanced synthetic monitoring. The scale of the existing URL monitoring has been increased and is easier to set up. Management packs are available for monitoring Microsoft Exchange Server and SQL Server® transaction performance and availability.
* Process monitoring. This detects whether desired or undesired processes are running and, if they are, how many are running. In addition, it provides monitoring of the CPU and memory being consumed by processes.
* Notifications. This provides a mechanism to set up Simple Mail Transfer Protocol (SMTP) more easily and to subscribe to notifications to events.
* Run As capability. Provides improved granularity and control of security settings.
* Import Management Packs Wizard. This wizard can be used to import management packs and updates to them, either from a local or network disk or directly from the management pack catalog on the Internet.
* Update to Visio export. The Microsoft Visio® exports that are obtained from Operations Manager 2007 R2 now include the metadata that is necessary for future versions of Microsoft SharePoint® and Visio to query the OperationsManager database and update the status of exported objects in the diagram.
* Maintenance mode. The process of placing a computer and all its related objects into maintenance mode has been streamlined.
* UI performance and usability. The Operations console performance has been greatly improved.

## Assumptions

To limit the scope of material in this guide, the following assumptions have been made:

* This design is for use in a production environment. It is expected that a test environment will also be created to mirror the configuration of the production environment.
* The reader is familiar with Microsoft infrastructure solutions. This guide does not attempt to educate the reader on the features and capabilities of Microsoft products. The product documentation covers that information.

## Feedback

Please direct questions and comments about this guide to [satfdbk@microsoft.com](mailto:satfdbk@microsoft.com?subject=IPD%20-%20System%20Center%20Operations%20Manager%202007).

We value your feedback on the usefulness of this guide. Please complete the following **Solution Accelerators Satisfaction Survey**, available at <http://go.microsoft.com/fwlink/?LinkID=132579>, and help us build better guidance and tools.

# 

## IPD in Microsoft Operations Framework (MOF 4.0)

Microsoft Operations Framework (MOF) offers integrated best practices, principles, and activities to assist an organization in achieving reliable solutions and services. MOF provides guidance to help individuals and organizations create, operate, and support technology services, while helping to ensure the investment in technology delivers expected business value at an acceptable level of risk. MOF’s question-based guidance helps to determine what is needed for an organization now, as well as providing activities that will keep the organization running efficiently and effectively in the future.

Use MOF with IPD guides to ensure that people and process considerations are addressed when changes to an organization’s technology services are being planned.

* Use the Plan Phase to maintain focus on meeting business needs, consider business requirements and constraints, and align business strategy with the technology strategy. IPD helps to define an architecture that delivers the right solution as determined in the Plan Phase.
* Use the Deliver Phase to build solutions and deploy updated technology. In this phase, IPD helps IT pros design their technology infrastructures.
* Use the Operate Phase to plan for operations, service monitoring and control, as well as troubleshooting. The appropriate infrastructure, built with the help of IPD guides, can increase the efficiency and effectiveness of operating activities.
* Use the Manage Layer to work effectively and efficiently to make decisions that are in compliance with management objectives. The full value of sound architectural practices embodied in IPD will help deliver value to the top levels of a business.



Figure 1. The architecture of Microsoft Operations Framework (MOF) 4.0

# System Center Operations Manager 2007 in Microsoft Infrastructure Optimization

The Infrastructure Optimization (IO) Model at Microsoft groups IT processes and technologies across a continuum of organizational maturity. (For more information, see <http://www.microsoft.com/infrastructure>.) The model was developed by industry analysts, the Massachusetts Institute of Technology (MIT) Center for Information Systems Research (CISR), and Microsoft's own experiences with its enterprise customers. A key goal for Microsoft in creating the Infrastructure Optimization Model was to develop a simple way to use a maturity framework that is flexible and can easily be applied as the benchmark for technical capability and business value.

IO is structured around three information technology models: Core Infrastructure Optimization, Application Platform Optimization, and Business Productivity Infrastructure Optimization. According to the Core IO Model, Operations Manager 2007 can be used to move an organization from a Standardized to a Dynamic level of maturity. At a Standardized level, monitoring may occur for 80 percent or more of critical servers. At the Rationalized level, service level agreement (SLA) monitoring of mission-critical servers and IT service level reporting would occur. A Dynamic level of maturity requires service level monitoring of desktops, servers, and applications.

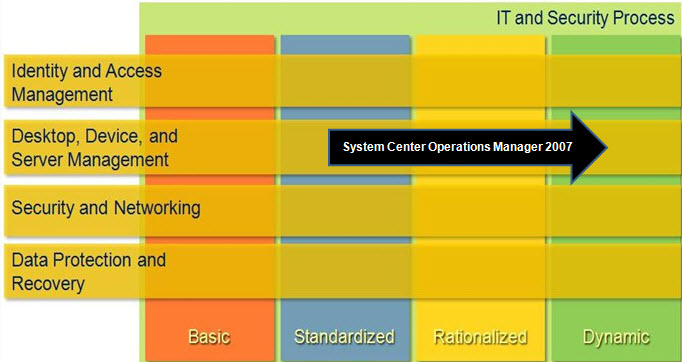


Figure 2. Mapping System Center Operations Manager 2007 into the Core Infrastructure Model

# System Center Operations Manager 2007 Design Process

The goal of the System Center Operations Manager 2007 Infrastructure Planning and Design Solution Accelerator is to guide users through the information gathering, decisions, options, and tasks required to create and design an Operations Manager 2007 infrastructure. The objective is an infrastructure that is sized, configured, and appropriately placed to deliver the stated business benefits, while considering the user experience, security, manageability, performance, capacity, and fault tolerance of the system. The guide addresses the scenarios most likely to be encountered by someone designing an Operations Manager 2007 infrastructure. Customers should consider having their architecture reviewed by Microsoft Customer Service and Support prior to implementation as that organization is best able to comment on the supportability of a particular design.

Figure 3 illustrates the relationship between the components that can work together to deliver a monitoring solution with Operations Manager 2007. Note that the components can be designed in many different ways; Figure 3 shows them in a particular implementation for illustrative purposes only.

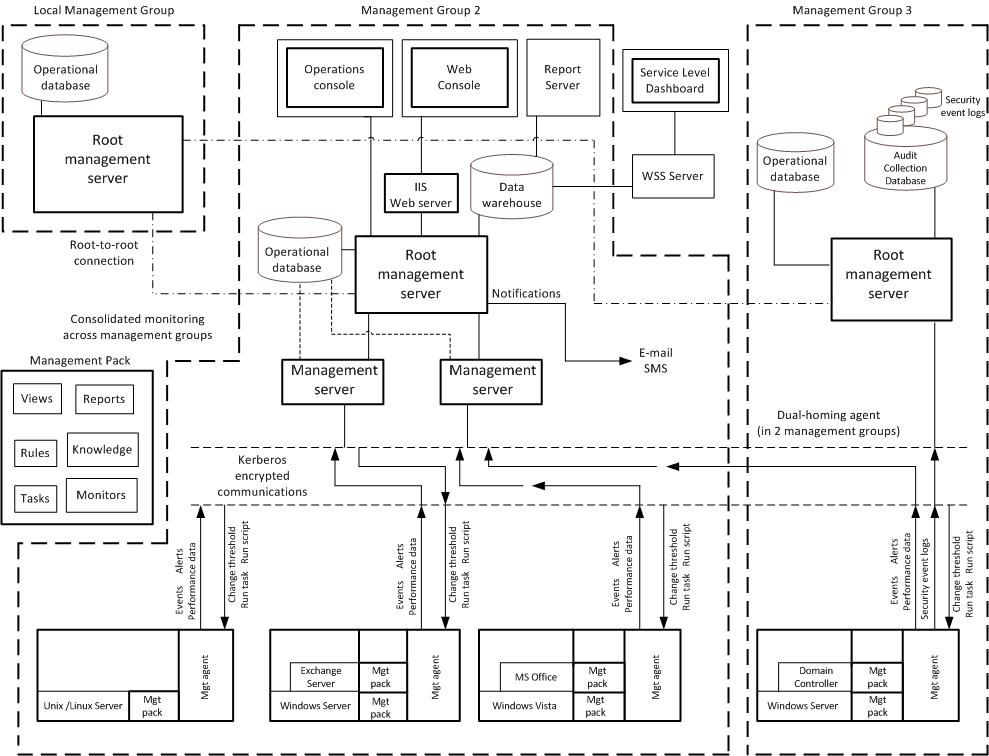


Figure 3. System Center Operations Manager 2007 architecture

## Decisions

This guide addresses the following decisions and activities that need to occur in planning for Operations Manager 2007. The 11 steps that follow represent the most critical design elements in a well-planned Operations Manager 2007 design:

* Step 1: Define the Scope of the System Center Operations Manager 2007 Project
* Step 2: Identify Necessary Management Packs and Product Connectors
* Step 3: Determine How Monitoring Will Be Implemented
* Step 4: Determine the Number of Management Groups
* Step 5: Determine the Agent Security Model
* Step 6: Design and Place the System Center Operations Manager 2007 Server Roles
* Step 7: Design the OperationsManager Database, ACS Database, and AEM File Share
* Step 8: Design the Notification System
* Step 9: Determine Whether to Implement Reporting
* Step 10: Design the Data Warehouse, Reporting Server, and Service Level Dashboard
* Step 11: Design the Network Connections

Some of these items represent decisions that must be made. Where this is the case, a corresponding list of common response options will be presented.

Other items in this list represent tasks that must be carried out. These types of items are addressed because their presence is significant in order to complete the infrastructure design.

## Decision Flow

Figure 4 provides a graphic overview of the steps involved in designing an Operations Manager 2007 infrastructure.

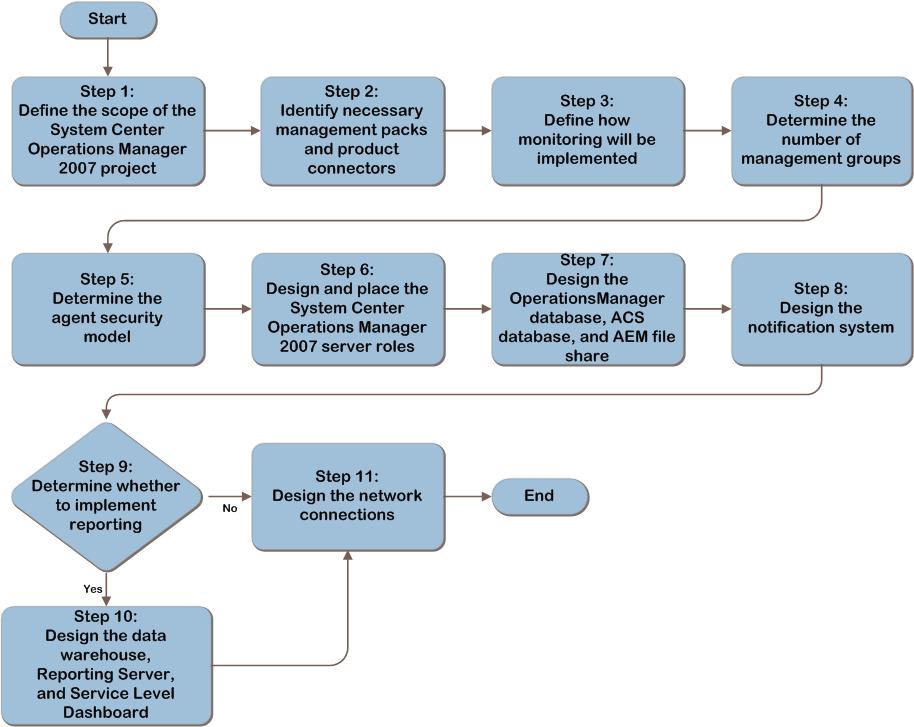


Figure 4. The System Center Operations Manager 2007 infrastructure decision flow

## Applicable Scenarios

This guide addresses the planning and design decisions involved in creating a successful Operations Manager 2007 infrastructure. It has been written to address the needs of the following groups:

* Organizations with no monitoring solution that are planning to monitor services, applications, and infrastructure with Operations Manager 2007.
* Organizations presently using another monitoring solution that are planning to move to Operations Manager 2007.
* Organizations that are consolidating multiple monitoring solutions to Operations Manager 2007.
* Organizations with multi-forest environments where Operations Manager 2007 will be employed to monitor and manage resources that span Microsoft Active Directory® Domain Services (AD DS) forest boundaries.
* Organizations that have distributed environments with systems separated by wide area network (WAN) links.
* Organizations with services in perimeter networks separated by firewalls.
* Organizations interested in implementing centralized Security event log collection and reporting to meet internal audit or regulatory compliance requirements.
* Organizations upgrading from Microsoft Operations Manager 2005 to Operations Manager 2007.
* Organizations requiring coexistence with existing management systems.

## Out of Scope

This guide does not address the following:

* Multi-tenancy. Service provider scenarios incorporating Operations Manager 2007 or Microsoft System Center Essentials 2007 functionality.
* System Center Essentials. System Center Essentials is a separate product designed for midmarket businesses.
* OEM management packs. Original equipment manufacturer (OEM) management packs have varying resource and security requirements. Necessary resources should be obtained from the OEM vendor offering the management pack.
* Management pack development. Creation of custom management packs.

# Step 1: Define the Scope of the System Center Operations Manager 2007 Project

Because technical decisions must align with organizational objectives, it is important to clearly define the scope of any IT project. The business requirements will be used to determine the technical requirements of the solution in subsequent tasks and will reflect appropriate trade-offs in feature usage, fault tolerance, capacity, and performance.

The process in this guide applies to both Operations Manager 2007 and Operations Manager 2007 R2, except where content that is new in R2 is explicitly indicated.

This step identifies the functional requirements of the business and the budgetary resources available to meet them. This information will enable the creation of a design that meets functional requirements within the project’s defined resource constraints.

Step 1 contains the following tasks:

* Identify business requirements.
* Create a component map for services identified as in scope for monitoring.
* Identify resources in scope for monitoring.
* Identify in-place monitoring and administrative processes.

The outputs of this step will be a detailed list of resources in scope for monitoring, coexistence requirements with any existing management systems, as well as any IT support requirements affecting the Operations Manager 2007 infrastructure design. The information collected in Step 1 will be used in Step 2 to identify required management packs, in Step 3 to determine how certain components or business services will be monitored, and in Steps 5, 6, 7, and 10 to design the Operations Manager 2007 server infrastructure.

## Task 1: Identify Business Requirements

In this task, the functional requirements for business stakeholders are documented. When the requirements and budget are known, accurate technical decisions can be made on how to best meet solution requirements.

Below is a list of key data-collection tasks and descriptions of how the information will be used in later steps. Before proceeding to the next step, document all of the following information in the order listed:

1. Identify business services in scope for monitoring. Determine which business services (for example, customer relationship management applications or e-commerce websites) should be monitored. This information makes it possible to identify the dependent applications, servers, and devices, as well as the underlying technologies that they depend (for example, SQL Server and AD DS) that must be considered for monitoring in Task 3.

Using Table A-1 “Sample Business Service Inventory” in the Appendix: “Job Aids,” document a list of business services for which monitoring is required. In the job aid, document the service owner, a description of service function, whether application performance and availability must be monitored, and whether reports will be required by the business. Also request and document the description of a sample transaction in the field provided.

1. Identify reports expected for service owners and stakeholders. Ask business stakeholders about the reports they expect to receive. Record this information for each business service in the field provided in Table A-1. Understanding the specific reports required for each business service uncovers any need for reporting as well as the need for certain types of monitoring to collect the data necessary to generate these reports.

For example, if a service has a response time SLA, synthetic transaction monitoring will be necessary to provide performance data for the expected reports.

1. Identify service level requirements for the monitoring infrastructure. Ask stakeholders for their service level requirements and weigh these expectations against the cost of implementing them. Record these findings in Table A-1. This will drive fault-tolerance decisions when the server and storage infrastructure is designed in later steps.
2. Identify regulatory compliance or internal audit requirements. Obtain answers to the following questions before proceeding:

* Does the organization have any external or internal requirements for security auditing?
* If so, has the organization implemented a security auditing solution that satisfies these requirements?

External regulations, such as the Sarbanes Oxley (SOX) Act or the Health Insurance Portability and Accountability Act (HIPAA) might require implementation of Audit Collection Services (ACS) if a security-auditing solution is not currently in place. Likewise, internal security policies mandating a security audit can also create a need for ACS. If security logs must be recorded and stored centrally, record in Table A-1 in the Appendix whether security logs should be retained and how long they must be stored.

1. Identify the available budget for the project. The planner should design the most effective solution and then adapt it to the available budget, if necessary. Obtain this figure before continuing Step 1.

## Task 2: Create a Component Map for Services Identified As In Scope for Monitoring

For each business service for which monitoring is required, create a component map that documents the applications, subservices, servers, and devices on which the service runs or depends. This information may be obtained from the business service owner and the application owners; it may also be available from system and network architects. Be sure to note whether the service has business-critical components on client computers (for example, bank teller workstations). This information will be used in the next task to determine and prioritize which underlying services should be monitored. It will also enable the monitoring infrastructure to deliver rapid problem isolation in the event of service degradation. Finally, it will be used to identify the management packs, product connectors, and product features required in Steps 2 and 3 and will help determine server infrastructure sizing and licensing requirements in Steps 6, 7, 10, and 11.

A sample component map showing monitoring requirements for an organization that uses a time-tracking application to gather hours worked on customer projects is illustrated in Table A-2 “Sample Business Service Component Map” in the Appendix.

The bullet points below list the type of information included in a component map:

* The organization’s time-tracking software depends on AD DS for authentication.
* The data for the application is stored in a SQL Server database.
* Clients accessing both the service and AD DS depend on Domain Name System (DNS) for name resolution.
* These services are hosted on Windows Server® 2008, which depends on its server hardware.
* Server and client network connectivity are dependent on the network switches to which they are connected.

For your project, document the list of dependent components for each business service identified in Task 1 using Table A-2 in the Appendix. This list of the components and dependencies for each business service will be available for use in Task 3.

## Task 3: Identify Resources In Scope for Monitoring

For each component map created in Task 2, use Table A-2 in the Appendix to record the priority of monitoring for each component, including workstation clients. Prioritize each of these components based on their effect on overall functionality, using the monitoring priority scale shown in the table below as a guide. If a component is determined to be low priority for monitoring, decide whether it should remain in scope for the project. Refer to Table A-1, to understand whether the availability and performance of the business service will be reported, and use that to determine whether the availability and performance of each of the components must be monitored. That will require the use of synthetic transaction monitoring. This information will be used in Step 2 to determine management pack requirements as well as Operations Manager 2007 server sizing and placement in Steps 6, 7, 8, and 11.

Table 1. Monitoring Priority Scale for Components of Business Services

| Impact of component failure on business service | Component priority | In scope |
| --- | --- | --- |
| Service outage | Critical | Yes |
| Service operates, but at substantially reduced functionality or capacity | High | Yes |
| Service operates with full functionality, but at reduced capacity | Medium | Yes |
| Service operates with full functionality and capacity | Low | No |

Record the monitoring priority in the column provided in Table A-2 in the Appendix. Repeat this process for each component map created in Task 2.

## Task 4: Identify In-Place Monitoring and Administrative Processes

Not every Operations Manager 2007 project will be a new implementation. Many organizations will have monitoring and management systems already in place, deployed in a way best suited to meet the organization’s administrative model. Before moving to Step 2, it is crucial to identify whether coexistence with existing management systems is required. Determining whether Operations Manager 2007 is expected to coexist with, or replace, these systems will affect selection of management packs and monitoring methodology in Steps 2 and 3, as well as infrastructure sizing and placement decisions in Steps 6, 7, 8, and 11.

Discuss the need for coexistence and its expected duration with service owners of existing monitoring and trouble ticket systems. The results of these discussions will drive the decision about whether to replace existing systems or to plan for coexistence.

There are several circumstances that require coexistence:

* When continuous monitoring is necessary during Operations Manager 2007 deployment.
* During an upgrade, when systems are operating in a side-by-side configuration with elements of Microsoft Operations Manager 2007.
* When other System Center products are used that require interface with Operations Manager 2007 (for example, System Center Virtual Machine Manager uses the Operations Manager 2007 Reporting Server role to generate reports).
* When some existing monitoring systems are controlled by autonomous IT units that are not adopting Operations Manager 2007.
* If an integrated solution that provides a single console for help desk or other IT support functions is required.
* If automated ticket generation to a help desk ticketing system is required.

Record the information for this task in Table A-3 “Sample Monitoring and Administrative Process Analysis” in the Appendix.

## Step Summary

Aligning technical decisions with business requirements is a critical component of a successful project. Failure to clearly identify the functional requirements of the business and the budgetary resources available to meet them can result in a design that fails to meet requirements within the resource constraints defined for the project.

In Step 1, the following determinations were made:

* Business requirements for the Operations Manager 2007 solution.
* Business services in scope for monitoring with Operations Manager 2007.
* Individual components that contain the resources that must be monitored.
* Coexistence and interoperability requirements for Operations Manager 2007 with existing management systems (monitoring or ticketing systems) if other solutions exist and will continue to be present.

The output of Step 1 is a detailed list of the resources in scope for monitoring, coexistence requirements with any existing monitoring systems, and any IT support requirements affecting the Operations Manager 2007 infrastructure design. This information was recorded in Tables A-1, A-2, and A-3 in the Appendix.

This information will be used in Step 2 to identify required management packs, in Step 3 to determine how some components or business services will be monitored, and in Steps 5, 6, 7, and 10 to design the Operations Manager 2007 server infrastructure.

## Additional Reading

Operations Manager 2007 R2 Design Guide: <http://technet.microsoft.com/en-us/library/dd789005.aspx>

# Step 2: Identify Necessary Management Packs and Product Connectors

In Operations Manager 2007, management packs deliver the monitoring rules for a given application or device. When the business services and their required components that will be monitored have been identified, the management packs necessary to deliver the required monitoring rules must be selected. If a requirement for communication with existing monitoring systems was identified in Step 1, a product connector for establishing communication will be required as well.

Step 2 focuses on:

* Selection of the required management packs. Native management packs offered by Microsoft will be selected from the catalog of available management packs published by Microsoft. If no native management pack is available from Microsoft, an alternative will be required, which may incur an additional cost to license third-party management packs or for development of custom management packs.
* Selection of product connectors. Product connectors are available for several, but not all enterprise monitoring platforms, so availability of a connector must also be explored.

The outputs of this step will be a list of required native management packs, a list of third-party management packs for other operating systems and third-party line-of-business (LOB) application monitoring, and a list of product connectors required to connect Operations Manager 2007 with existing management systems.

This information will be used in Step 6, during the design of the Operations Manager 2007 server infrastructure.

## Task 1: Determine Which Management Packs Are Required

Native management packs released by Microsoft are available for download at no charge from the System Center Operations Manager 2007 Catalog on the Microsoft website. Identify which native management packs are required by using the information in Table A-2 in the Appendix, documented in Step 1.

To select the native management packs needed to monitor the components identified in Step 1, do the following:

1. Using the Business Service Component Map completed in Step 1, Task 2, compare the components that are in scope for monitoring to the list of available management packs in the System Center Management Pack Catalog page at <http://pinpoint.microsoft.com/en-US/systemcenter/managementpackcatalog>.
2. Make a list of the native management packs that will be required. This list should include management packs that monitor the component’s health as well as those that monitor its availability and performance through the use of synthetic transactions. (Synthetic transactions are the best way of monitoring availability of any system or system component, since they measure its ability to deliver in response to user requests.)

Document the selected management packs in Table A-2 in the Appendix before moving to the next task.

## Task 2: Determine How Third-Party Devices and Third-Party Applications Will Be Monitored

Operations Manager 2007 includes some native facilities for monitoring third-party devices, such as through Simple Network Management Protocol (SNMP) or Syslog. The decision of how operating systems, network devices, and applications from third parties will be monitored brings with it additional software, time, and infrastructure costs. To select the best options, answer the following questions for each type of third-party server or device and each third-party application contained in the original component map:

* Does the third-party vendor offer a management pack either for a fee or free?
* Are there in-house IT resources with the skills to develop a custom management pack?
* Could the development of a custom management pack be outsourced to a specialist vendor?

Document the answers in Table A-3 in the Appendix. If no commercially available management pack can be identified to meet the requirement, determine whether development of a custom management pack is practical, or whether it is more practical to exclude the devices or applications from the scope of the project.

## Task 3: Determine Which Product Connectors Are Required

Product connectors send and receive data between Operations Manager 2007 and other management systems, such as those that monitor third-party computers or those that create trouble tickets. The connector may be implemented to integrate monitoring at the component level or to integrate a trouble ticketing system with Operations Manager 2007 systems that are monitoring one or more business services. There is a list of available product connectors in the System Center Operations Manager 2007 Catalog on the Microsoft website. Microsoft offers product connectors for several popular management systems at no charge; other product connectors are available from independent software vendors (ISVs) for a fee.

If coexistence with existing management systems was documented as a requirement in Step 1, perform the following steps to acquire appropriate product connectors:

1. Review the list of available product connectors in the System Center Management Pack Catalog at <http://go.microsoft.com/fwlink/?LinkId=121514>.
2. Ask the vendor of the management system for a product connector.
3. If a connector is not available, consider developing a custom connector using the System Center Operations Manager 2007 R2 software development kit (SDK), available at <http://msdn.microsoft.com/en-us/library/cc268402.aspx>.

Identify and document the list of product connectors and accompanying download links in Table A-3 in the Appendix before proceeding to Step 3. This information will be used in Step 6, Task 1, to determine the server role distribution in each management group.

## Step Summary

Step 2 focuses on selecting required native management packs, determining how third-party applications will be monitored, and selecting appropriate product connectors.

The outputs of this step are:

* A list of required native management packs.
* A list of third-party management packs for monitoring third-party LOB applications.
* A list of product connectors required to connect Operations Manager 2007 with existing management systems.

All of the information gathered in this step was recorded in Table A-2 and Table A-3 in the Appendix. This information will be incorporated in Step 6 when designing the Operations Manager 2007 server infrastructure.

## Additional Reading

“Connecting to External Systems by Using Operations Manager Connectors”: [http://msdn2.microsoft.com/en‑us/library/bb437511.aspx](http://msdn2.microsoft.com/en-us/library/bb437511.aspx)

# Step 3: Determine How Monitoring Will Be Implemented

When the list of in-scope resources is completed, it can be used to create a plan for implementing synthetic transaction monitoring and client workstation monitoring (if those management packs are required). This step is important because it allows planners to determine which methods of monitoring to use for the components that were identified as in scope for monitoring in Table A-2 in the Appendix.

Note   Monitoring options such as management packs will not be covered here as their use does not have a direct bearing on infrastructure planning at this stage.

Step 3 focuses on:

* Developing a strategy for synthetic monitoring. Synthetic transaction monitoring can be conducted for in-scope business services in order to monitor availability and performance against established SLAs.
* Developing a client workstation monitoring strategy. Because client workstations typically greatly outnumber server computers, the license cost and additional resource load and licensing imposed on the Operations Manager 2007 server infrastructure may not justify (or allow) monitoring of all client computers.

The outputs of this step will be a sampling strategy for synthetic monitoring as well as a client monitoring sampling strategy that strikes a balance in delivering the maximum benefits with minimal resource consumption. This information will be recorded in the job aids referenced in each task. Data from this step will be used in Steps 6, 7, and 8 during the design and sizing of the Operations Manager 2007 server and database infrastructure.

## Task 1: Determine a Synthetic Transaction Monitoring Strategy

A business service can be considered available only if a transaction can be completed successfully. Synthetic transaction monitoring is a way of testing transaction processing.

Using the information captured in Step 1, determine the following for the business services components that are in scope for synthetic transaction monitoring:

* Correct location of watcher nodes
* Transaction load on the watcher node
* Fault tolerance for watcher nodes
* Number of watcher nodes that should be deployed to run a given transaction

The placement of watcher nodes should mirror the locations from which the application is used. This can provide the greatest insight into the source of service performance and availability issues, quickly highlighting those that are specific to a certain location.

Although there is no single correct sampling method for synthetic transaction monitoring, performing the following activities can help define the best strategy for the organization:

* Determine watcher node location. The ideal synthetic transaction implementation would involve placing a monitoring workstation physically next to each user workstation to accurately measure and monitor the availability of the transaction from that user’s perspective. However, this is not practical, so synthetic transaction workstations must be placed in sample locations that best represent the typical user population for the service.

The exact number of locations should be determined by considering the cost and overhead of maintaining them and the granularity of the measurement that they provide. Refer to any specific requirements that the business may have regarding points from which to monitor. In the absence of that information, plan to place a watcher node in all high-priority user locations and in each branch office or other remote location.

* Determine whether dedicated or shared watcher nodes are required. Servers that are performing other functions may be used as watcher nodes. However, in areas of e-commerce or other applications that affect revenue, plan for dedicated watcher nodes. This precaution will help prevent any unforeseen resource issues that could interfere with the execution of the synthetic transaction and accurate recording of transaction response time, or with the business system that runs on the server.   
  If dedicated server hardware is not available, using virtual machines (VMs) as dedicated watchers should work equally well.
* Determine the number of watcher nodes for each location. Consider fault-tolerance requirements for watcher nodes and the aggregate load of all synthetic transactions running from watcher nodes for a specific location. For example, if synthetic transaction monitoring from a certain location must continue in the event of a watcher node outage, then two watcher nodes should be assigned to that location. If the number of synthetic transactions running for business services is greater than one node can support, then the sample transactions should be distributed across two or more watcher nodes.
* Determine repeat frequency for synthetic transactions. The repeat interval for each synthetic transaction must strike a balance between timely notification and resource load. Start by using a repeat interval that is equal to the time within which operations staff expects to be notified of a failure in the application.
* Determine the load on watcher of the synthetic transaction. Using the Windows® Performance Monitor tool, measure the load of each transaction on a computer at rest to determine the resource requirements of each transaction, and then size watcher node hardware accordingly.
* Determine the network load of a single transaction. In cases where transactions involve significant amounts of data or images, the impact on network bandwidth may become a concern. If a transaction consumes excessive bandwidth, it may be necessary to avoid performing synthetic transaction monitoring over WAN links. This will require measuring or estimating the bandwidth consumption of a given transaction and comparing it to available network bandwidth.

Record this information in Table A-4 “Sample Synthetic Monitoring Implementation Planner” in the Appendix, and then move to the next task. This information will be used in Step 6 during the design and sizing of the server infrastructure.

## Task 2: Determine the Client Workstation Sampling Strategy for Monitoring

The goal of this task is to determine whether client workstations that are in scope for monitoring must be monitored individually.

For each of the workstations identified as in scope for monitoring, record whether it is business-critical (for example, automated teller machines) and, if so, implement monitoring using the appropriate management packs.

If a client workstation is in scope but not business critical, determine whether a representative sample of similar workstations could be monitored, and then whether that monitoring could be aggregated using Collective Client Monitoring.

Record this information in Table A-5 “Sample Client Monitoring Implementation Planner” in the Appendix before moving to the next step. This information will be used in Steps 6, 7, and 8 during the design and sizing of the Operations Manager 2007 server infrastructure.

## Step Summary

Step 3 focused on determining:

* A plan for synthetic transaction monitoring.
* A sampling strategy for client monitoring.

The outputs of this step will be a strategy for synthetic transaction monitoring and a client computer monitoring strategy that strikes a balance in delivering the maximum benefits with minimal resource consumption. This information was recorded in Tables A-4 and   
A-5, referenced in each task. This information will be used in Steps 6, 7, and 8 during the design and sizing of the Operations Manager 2007 server and database infrastructure.

## Additional Reading

Client Monitoring with Microsoft Operations Manager 2007: <http://go.microsoft.com/fwlink/?LinkId=121515>

# Step 4: Determine the Number of Management Groups

A management group is the basic functional unit of an Operations Manager 2007 implementation that can perform monitoring. Each management group contains a Microsoft SQL Server database server to host the OperationsManager database, a root management server (RMS), one or more Operations consoles, and the agents and other resources that are managed. It can also contain additional management servers and gateway servers, as well as ACS components.

The goal of this step is to determine the smallest number of management groups necessary to meet the organization’s monitoring objectives. The exact number will depend on the organization’s business and technical requirements. These requirements are not mutually exclusive, so the planner will need to iterate through all of them.

The output of this task is a document listing the number of management groups required and the justification and function of each. This will be used in Step 6 to help determine the number and sizing of Operations Manager 2007 server roles and the distribution of these roles across servers. This information also determines how many iterations of Steps 6, 7, and 8 are necessary to complete all management group infrastructure planning activities.

## Task 1: Determine the Number of Management Groups Required to Meet the Organization’s Size, Location, and Security Requirements

Begin this task with a design that includes one production management group, and then justify each additional management group according to the list of criteria that dictate the need for additional management groups.

The primary technical considerations in determining the number of management groups required are:

* The number of resources in scope for monitoring.
* The location of these resources.
* The IT groups responsible for monitoring the resources.

Answer the following questions based on the criteria provided for each question. Any question with a yes answer indicates the need for additional management groups.

* Does the number of monitored resources require multiple management groups? While there is no programmed limit for the number of agents that can be managed within a single management group, information from live environments has established certain limits. Recommended scale limits for Operations Manager 2007 R2 are published under the “Monitored Item Capacity” section of *Operations Manager 2007 R2 Supported Configurations* at <http://go.microsoft.com/fwlink/?LinkId=121517>.
* Are agents separated from their management server by WAN-speed network links? Slow network links may require separate management groups. Use the data in the “Minimum Network Connectivity Speeds” section o*f Operations Manager 2007 R2 Supported Configurations*at <http://go.microsoft.com/fwlink/?LinkId=121517> to calculate the network bandwidth that would be required to support the agents in the remote location.

If the required bandwidth exceeds what will be available on the network link, there are two options:

* Plan for an additional management group in that location. This will incur additional infrastructure and support costs.
* Upgrade the bandwidth, at additional cost.
* Do administration or security requirements within the organization require separate management groups? The Operations Manager 2007 Administrator role maintains full control of all resources in the management group and cannot be limited in the resources it controls. If the organization has multiple autonomous IT support units that are unwilling or unable to share administrative control of the Operations Manager 2007 infrastructure, then additional management groups are required.
* Is a view of AD DS topology required across multiple forests? The AD DS management pack does not provide out-of-forest topology monitoring, so unless a cross-forest trust is in place, a separate management group must be designed for each forest in which AD DS topology function is needed.

Record each management group identified and the reason required in Table A-6 “Same Management Group Requirements” in the Appendix, and then proceed to the next task.

## Task 2: Determine the Number of Management Groups Necessary to Meet the Organization’s Testing, Auditing, and Localization Needs

For each of the management groups identified in Task 1, answer the following questions to decide whether additional management groups must be planned:

* **Are separate production and preproduction management groups necessary?** Microsoft recommends that organizations maintain a separate preproduction management group for tuning and testing management packs. In this preproduction environment, a copy of the default management packs can be unsealed and thresholds adjusted to match local standards. This management group’s infrastructure does not have to be of the same physical scale as the production management group.
* Is a dedicated ACS management group required? If regulatory compliance or internal security policies require that administration of Security event log data must be separated from management of operational events and alerts, add an ACS management group for each management group identified in Task 1.
* Is support for multiple languages needed? The localization of all Operations Manager 2007 server roles must match that of the root management server (RMS). For example, suppose an organization has offices and IT support staff located on multiple continents. If multiple languages must be supported for Operations Manager 2007 server roles, an additional management group would be necessary for each language used by Operations Manager 2007 operators.

Use Table A-6 in the Appendix to record each management group needed to meet the above criteria and the reason required, and then proceed to the next task.

## Task 3: Determine the Number of Management Groups Required to Meet the Organization’s Disaster Recovery and Reporting Needs

The availability requirements of the Operations Manager 2007 monitoring infrastructure may vary based on the location and the resources being managed. In addition, when multiple management groups are used in an environment, the organization may desire a single view of the monitoring and alert data. Both of these areas may influence the number of management groups in the design.

For each management group identified in tasks 1 and 2, answer the following questions regarding the creation of additional management groups:

* Is disaster recovery functionality required? If the organization’s service level requirements for the Operations Manager 2007 infrastructure include disaster recovery functionality, a dedicated failover management group can be created. SQL Server log shipping can be used to send SQL Server logs to another SQL Server-based computer, and the logs can be applied to a copy of the OperationsManager database in the failover management group.

If the RMS or OperationsManager database becomes unavailable because of a disaster, management servers can then be redirected to the failover SQL Server-based computer. This setup could be used to facilitate continued management group availability in the event of failure of a database server, or even failure of a physical location.

* Are consolidated views of connected management groups required in Operations Manager 2007? An additional local management group can be used to provide a centralized management view and to centrally connect to other event and alert management systems.

A centralized management model with large remote locations works best with a management group in each region and a local management group (which provides a consolidated view of alerts and status) in the parent location. In this case, the centralized management group connects through the SDK and functions as an additional console on each of the connected management groups. Note that performance data cannot be viewed from the local management group. There is no official sizing guidance on how many connected management groups to which a local management group may connect.

* **Will Operations Manager 2007 Reports be integrated into the System Center Virtual Machine Manager (VMM) console?** VMM uses the Operations Manager 2007 Connector Framework to connect to a single Operations Manager 2007 management group, so the Reports tab in the VMM console can display only the reporting data that is within the scope of that management group. This means that if two different VMM hosts are in different Operations Manager 2007 management groups, two VMM instances will be required in order to provide reporting integration in the VMM console. Each VMM instance will then only provide reports for the management group to which it is connected.

This may prompt the planner to design fewer Operations Manager 2007 management groups. Alternatively, side-by-side use of the VMM and Operations consoles may be sufficient, without their integration.

Record any additional management groups that are required in Table A-6 in the Appendix.

## Step Summary

The goal of this step was to determine the number of management groups necessary to meet the organization’s monitoring objectives. Infrastructure and environment data from Step 1 was compared to the criteria for multiple management groups to determine the need for additional management groups.

The output of this task is a list of required management groups (recorded in Table A-6) and the justification and function of each. This information is used in Step 6 as an aid in decision making about server size, count, and Operations Manager 2007 server role distribution. This information also determines how many times Steps 6, 7, and 8 must be repeated to complete all infrastructure planning activities required for each management group.

## Additional Reading

* Operations Manager 2007 R2 Design Guide: <http://technet.microsoft.com/en-us/library/dd789005.aspx>
* Operations Manager 2007 Deployment Guide: <http://go.microsoft.com/fwlink/?LinkId=121518>
* Operations Manager 2007 R2 Supported Configurations: <http://go.microsoft.com/fwlink/?LinkId=121517>
* System Center Operations Manager 2007 R2 SDK: <http://go.microsoft.com/fwlink/?LinkID=108753>

# Step 5: Determine the Agent Security Model

Operations Manager 2007 requires mutual authentication between management servers and agents. This can be achieved using one of the following methods:

* Kerberos authentication,which is available to all computers within the same AD DS forest and computers outside the forest that have established AD DS forest trust or domain trust relationships.
* Certificate authentication, which uses x.509 digital certificates to mutually authenticate agents and management servers across trust boundaries, such as workgroup computers or those in a separate AD DS forest.

If all computers defined as in scope for monitoring in Step 1 are located within trust boundaries and that is not expected to change, skip this step and move to Step 6.

If computers in scope for monitoring are located beyond trust boundaries, decision makers must evaluate the readiness of the organization to support mutual authentication between Operations Manager 2007 server and agent roles. If the necessary infrastructure does not exist, a design will be created in this step.

## Decision Flow

Figure 5 illustrates the decision flow for designing an infrastructure that provides mutual authentication with agents that are beyond the trust boundary of the Operations Manager 2007 management server. The planner will need to use this flow for each group of agents beyond the trust boundary that will connect to each management group.

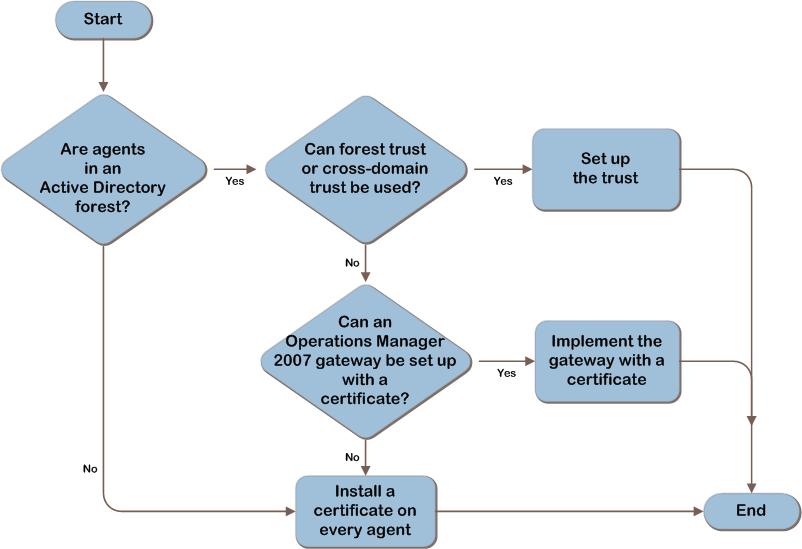


Figure 5. Decision flow to design mutual authentication

### Decision 1: Are Agents in An AD DS Forest?

Kerberos authentication is possible only between computers located within the same trust boundary. The trust boundary can be extended to include agents beyond the trust boundary, provided that those agents are in an AD DS forest. So the first thing to determine is whether the agents are in an AD DS forest.

#### Option 1: Yes

If the agent computers are in an AD DS forest, proceed to the next decision.

#### Option 2: No

If the agent computers are not in an AD DS forest, proceed to Task 1 to deploy a certificate on each agent computer.

### Decision 2: Can a Forest Trust or Cross-Domain Trust Be Used?

The trust boundary can be extended to include agent computers that are in a different AD DS forest. Extension would require agreement from the group responsible for security in that forest.

#### Option 1: Yes

If a trust relationship can be established, extending the trust boundary of the management server beyond the forest in which it resides will require a decision to be made between a cross-forest trust and a cross-domain trust. For additional information, refer to the *Infrastructure* *Planning and Design for Windows Server 2008 Active Directory Domain Services* guide at [www.microsoft.com/IPD](http://www.microsoft.com/IPD), and then set up the trust.

#### Option 2: No

If a trust cannot be used, proceed to the next decision.

### Decision 3: Can an Operations Manager 2007 Gateway Be Set Up with a Certificate?

If a trust cannot be used, it will be necessary to implement certificate authentication. The management overhead and cost of this may be minimized by implementing a gateway in the other forest and deploying a certificate to that gateway. The gateway server and the management server to which it will connect must both be issued certificates by the same trusted certification authority (CA).

#### Option 1: Yes

If a gateway can be set up in the other forest and if that gateway can authenticate with the agents, it can be used as an authentication concentrator. In this case, implement the gateway in the other forest and deploy a certificate to it, as well as to the management server that it will connect to.

#### Option 2: No

If a gateway cannot be deployed into the other forest, proceed to Task 1 to deploy a certificate on each agent computer.

For each group of agents beyond the trust boundary, record how they will connect to each management group in Table A-7 “Mutual Authentication Decisions” in the Appendix.

## Task 1: Deploy a Certificate to Every Computer Beyond the Trust Boundary

If the computers outside the AD DS forest that hosts Operations Manager 2007 are not within a trusted forest or are in a workgroup configuration, a certificate will have to be deployed to each computer to provide mutual authentication. In this case, the planner must determine whether the organization’s public key infrastructure (PKI) meets Operations Manager 2007 requirements. The PKI requirements for the Operations Manager 2007 infrastructure can be met by one of the following:

* A Windows Server 2003 or Windows Server 2008 stand-alone CA.
* A Windows Server 2003 or Windows Server 2008 enterprise CA running on Windows Server 2003 Enterprise Edition.
* A third-party CA that supports the certificate template that Operations Manager 2007 requires. (For a copy of this template, see <http://blogs.technet.com/momteam/archive/2007/10/03/cerificate-template-for-third-party-ca.aspx>.)

Note   A Windows Server 2003 enterprise CA running on Windows Server 2003 Standard Edition does not meet Operations Manager 2007 requirements because certificates based on version 2 certificate templates cannot be issued to computers from an enterprise CA running on this version of the Windows Server 2003 operating system.

If no PKI infrastructure exists in the organization, the organization can either design and deploy a PKI or purchase digital certificates from a third-party provider. To determine which option is best, compare the cost of certificates for computers outside the trust boundary with the cost of server hardware and Windows licensing to establish an internal PKI infrastructure.

Repeat this decision-making process for each management group that includes resources beyond its AD DS trust boundary.

## Step Summary

Step 5 determined the readiness of the organization to support mutual authentication between Operations Manager 2007 server and agent roles. The decisions in this step were recorded in Table A-7 in the Appendix.

The output of this step is a strategy that supports mutual authentication between Operations Manager 2007 components across trust boundaries.

## Additional Reading

* *Infrastructure Planning and Design for Windows Server 2008 Active Directory Domain Services:* [www.microsoft.com/IPD](http://www.microsoft.com/IPD)
* Operations Manager 2007 R2 Design Guide: <http://technet.microsoft.com/en-us/library/dd789005.aspx>
* Operations Manager 2007 Deployment Guide: <http://go.microsoft.com/fwlink/?LinkId=121518>
* Operations Manager 2007 R2 Supported Configurations: <http://go.microsoft.com/fwlink/?LinkId=121517>

# Step 6: Design and Place the System Center Operations Manager Server 2007 Roles

Step 4 focused on establishing the required number of management groups. The goal of Step 6 is to determine the appropriate sizing and distribution of Operations Manager 2007 server roles within each management group. This decision depends on both the number of monitored objects and the fault-tolerance requirements of the organization served by that management group. Proceed through this entire step once for each management group that was defined in Step 4.

Determining appropriate size, placement, and distribution of server roles is an important element in delivering the required monitoring functionality at a level of performance and fault tolerance expected by the organization.

Step 6 focuses on:

* Determining the appropriate number and distribution of root management servers, management servers, and gateway servers to support agent load.
* Deciding the location and size of IIS servers to support web consoles for administration.
* Determining the number of management servers needed to support the organization’s Agentless Exception Monitoring (AEM) and Audit Collection Services (ACS) needs.
* Reviewing the network topology to determine whether additional gateway servers are needed to optimize bandwidth utilization in instances of poor connectivity or trust boundary issues.
* Designing server configurations to meet the organization’s fault-tolerance requirements.
* Determining the hardware specifications for each server.

This information is used in Step 7 to determine the size and placement of the OperationsManager database, ACS database, and AEM file share. The design for Operations Manager 2007 server roles will also be considered during design of the network connections in Step 11.

The official infrastructure sizing tool for Operations Manager 2007 R2 is the Sizing Helper, available for download at <http://blogs.technet.com/momteam/archive/2009/08/12/operations-manager-2007-r2-sizing-helper.aspx>.

## Decision Flow

Figure 6 provides an overview of the steps to determine the Operations Manager 2007 management server infrastructure.

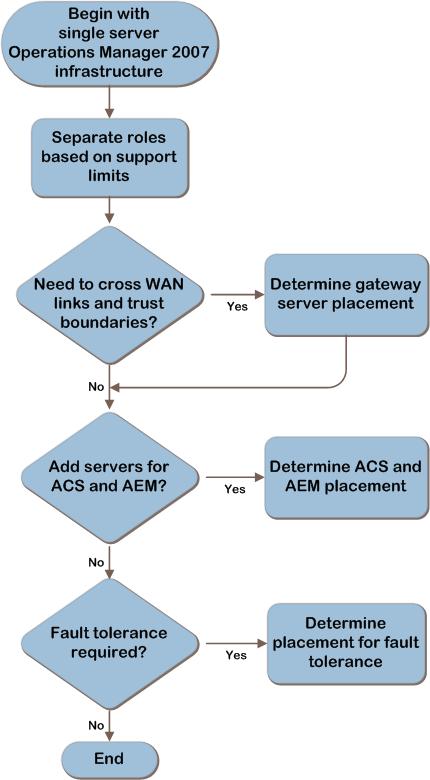


Figure 6. Determining server size, role distribution, and placement

## Planning Limitations

Ideally, the architectural design of the server roles would be based on the following information about each role:

* Integration (where this role fits relative to other roles)
* Capacity requirements
* Performance characteristics
* Unit sizing and volume expectations for data being sent and received by the role

As of this writing, this data is not available for Operations Manager 2007.

Simulation of the load on the server environment from the expected number of agents might be another way to approach this, but no such load simulators are available.

The official infrastructure sizing tool for Operations Manager 2007 R2 is the Sizing Helper, available for download at <http://blogs.technet.com/momteam/archive/2009/08/12/operations-manager-2007-r2-sizing-helper.aspx>.

Support limitations are published by the Operations Manager 2007 product group: <http://go.microsoft.com/fwlink/?LinkId=121517>. Note that these limits are based on testing that the product group has performed on R2. Testing was performed with all of the Microsoft standard management packs deployed in the environment.

Additional guidance is available from the product group on hardware form factors: <http://blogs.technet.com/momteam/archive/2008/04/10/opsmgr-2007-hardware-guidance-what-hardware-do-i-buy.aspx>. This guidance was published before the release of Operations Manager 2007 R2. Note that no architectural justification is offered to support these configurations.

## Planning Approach

A number of factors need to be considered when sizing and placing the server roles:

* **The management packs that will be loaded.** Each additional management pack creates additional load on the server environment.
* **The number of agents.** This determines the load from incoming events, alerts, and performance data.
* **The number of concurrently working consoles.** Each console places a load on the root management server.
* **The number of web consoles.** Each web console places a load on the RMS.

An examination of the supported configurations shows that:

* As the number of agents increases, a scale-out strategy, deploying additional servers, is recommended.
* As the number of ACS forwarders or AEM workstations increases, a scale-up strategy, to larger servers, is recommended.

No guidance is available for situations where supporting agents, ACS, and/or AEM are used together in the same management group.

Using this information, proceed with caution to design an implementation that is initially small, but capable of growth. Deploy on an increasingly larger scale and measure, learn, and adjust at each deployment.

## Task 1: Determine Root Management Server and Management Server Role Distribution

In this task, the expected agent load and console connections in each management group are used as criteria in determining how the core Operations Manager 2007 server roles (root management server and management servers) will be distributed to one or more servers.

Decide whether the root management server (RMS) and management server roles will be run on a single server, or whether the roles will be split across more servers, and then for each server document the applicable information in Table A-8 “Sample Server Infrastructure Requirements” in the Appendix. The server roles and configuration information recommended here are used in Tasks 2, 3, and 4 to decide whether to implement additional Operations Manager 2007 servers in order to optimize performance and adjust for load and fault tolerance.

## Task 2: Design the Gateway Server Deployment Strategy

The focus of this task is to determine the need for gateway servers. This involves examining agent location and network connectivity to determine where the core server infrastructure of each management group should be augmented. The goal is to optimize performance in the following key scenarios:

* Agents across trust boundaries necessitate administrative overhead because certificate authentication is required.
* Agents located across WAN links consume network bandwidth, potentially affecting service delivery to and from the remote location.
* Agents behind a firewall require multiple “allow” rules to permit agent traffic to pass through the firewall, raising potential security concerns.

A gateway server forwards data from its connected agents to an upstream management server, which then inserts the data into the OperationsManager database. Gateway servers can act as a point of consolidation for agents to minimize the number of points of outbound traffic for environments separated by a firewall; they can also consolidate communications, which results in reduced WAN link traffic.

Gateway servers are useful in a number of scenarios. The Operations Manager 2007 product group suggests that more than 10 agents in a single location outside a trust boundary or across a WAN connection may be grounds for use of a gateway. The benefits of a gateway must be balanced with the cost of administrative overhead, bandwidth utilization, hardware, and software. If minimizing bandwidth utilization or administrative overhead is a high priority, the gateway server scenario is optimal. For example:

* If a number of agent-managed computers are located on the opposite end of a low-speed WAN connection, a gateway could be used to reduce bandwidth utilization.
* If agent-managed computers are located in a separate AD DS forest, a gateway server can be justified to minimize the need for certificate authentication because only the gateway and upstream management server will require certificates.

However, if reducing hardware and software costs is the highest priority, gateway servers become a less attractive option. Recommended hardware sizing for the gateway server is identical to that of the management server role.

## Task 3: Determine Additional Hardware Requirements for AEM and ACS

The focus of Task 3 is to determine the number of management servers required to service the load generated by AEM and ACS.

### Agentless Exception Monitoring

When an application error occurs in a Windows operating system, the Dr. Watson service can capture the details so that they can be used to diagnose the cause of the problem. When Agentless Exception Monitoring (AEM) is enabled, those details can be forwarded to a management server and aggregated. They can then be used in centralized error analysis and diagnosis.

Decide whether AEM will be used and, if so, whether it will be implemented on dedicated server hardware.

### Audit Collection Services

Audit Collection Services (ACS) collects security event data from domain controllers, member servers, and client computers. Its use enables central security monitoring and reporting.

If ACS will be used in the management group, decide whether additional servers will be required for it, and add those servers as new rows in Table A-8 in the Appendix. This data will be used to help determine fault-tolerance configurations in Task 5.

## Task 4: Size and Place Web Console Servers

Operations Manager 2007 provides a web console that enables the environment to be administered from a web browser. The console is delivered by a Microsoft Internet Information Services (IIS) server, which is connected to the RMS.

Decide whether the web console will be used and, if so, whether additional servers will be required for it and add those servers as new rows in Table A-8 in the Appendix. This data will be used to help determine fault-tolerance configurations in Task 5.

## Task 5: Determine Server Fault-Tolerance Requirements

If fault tolerance was named as a requirement during Step 1, determine the need for fault tolerance in each server role based on the criticality of the resources being monitored.

The following table shows the fault-tolerance options for Operations Manager 2007 server roles. They are listed in order of importance to the Operations Manager 2007 infrastructure.

Table 2. Fault-Tolerance Methods for Operations Manager 2007 Server Roles

|  |  |  |
| --- | --- | --- |
| Role | Fault tolerance options | Failover type |
| Root management server | Failover cluster | Automatic |
| Management server promotion to RMS. Achieved by promoting a redundant management server with no allocated agents to take over the RMS role. | Manual |
| Management server | Redundant management server (deploy in pairs)  Note   Failover behavior is configured at the agent or in global settings, depending on how the agent was deployed. Microsoft Failover Cluster is not supported for management servers. | Automatic |
| Gateway server | Redundant gateway server (deploy in pairs)  Note   Failover must be configured using a Windows PowerShell command. Configure agents with a failover gateway and gateways with a failover management server. The gateways and management servers themselves are not load balanced or clustered. | Manual |
| AEM | Microsoft Failover Cluster | Automatic |
| ACS | Redundant ACS collectors.  Note   Agents configured to automatically fail over from one ACS collector to another. | Automatic |

If fault-tolerance options will be deployed, the hardware should be configured so that it will not be overloaded while operating in a fault-tolerant state.

Document any additional servers that are required for fault tolerance in Table A-8 in the Appendix. The output of this task is a list of the infrastructure necessary to meet the fault-tolerance requirements of the organization.

## Task 6: Select a Form Factor for the Servers

The goal of this task is to determine the most appropriate type of hardware on which to deploy the RMS, management servers, and gateway roles. Form factor in this guide refers to the combination of the servers’ characteristics including:

* Processor architecture (32-bit versus 64-bit).
* Number of CPUs and their speed.
* Amount of memory installed.
* Disk subsystem design.

Since there is no specific architectural information available to determine the optimal form factor for the servers, this guide cannot make any specific recommendations for configurations.

The product group provides some information on hardware form factors at <http://blogs.technet.com/momteam/archive/2008/04/10/opsmgr-2007-hardware-guidance-what-hardware-do-i-buy.aspx>.

Document the selected form factor for the servers in Table A-8 in the Appendix.

### **Use of Virtual Machines**

It is possible to use virtual machines (VMs) as an alternative to multiple physical systems, and this is supported as documented in*Operations Manager 2007 R2 Supported Configurations* at <http://go.microsoft.com/fwlink/?LinkId=121517>.

If used, document the selected form factor for VMs in Table A-8 in the Appendix, and then proceed to the next step.

## Step Summary

Step 6 involved:

* Determining the appropriate number and distribution of management servers and gateway servers to support agent load.
* Reviewing the network topology to determine whether additional gateway servers are needed to optimize bandwidth utilization where poor connectivity exists.
* Determining server configurations to meet the fault-tolerance requirements of the organization.
* Selecting hardware specifications for each server to be implemented.

The outputs of this step are:

* A detailed design for the Operations Manager 2007 management server infrastructure.
* A list of hardware and software specifications to implement the design.
* A diagram detailing Operations Manager 2007 server role placement in the network topology.

Operations Manager 2007 server sizing and placement must be performed for each management group determined in Step 4. Repeat the infrastructure design activities completed in this step for each management group. All data gathered in this step was recorded in Table A-8 in the Appendix.

This information is used in Step 7 during OperationsManager and ACS database sizing and placement. The design for Operations Manager 2007 server roles will also be considered in Step 11 during the design of network connections.

## Additional Reading

* Operations Manager 2007 R2 Design Guide: <http://technet.microsoft.com/en-us/library/dd789005.aspx>
* Operations Manager 2007 R2 Supported Configurations: <http://go.microsoft.com/fwlink/?LinkId=121517>

# Step 7: Design the OperationsManager Database, ACS Database, and AEM File Share

The goal of this step is to create infrastructure designs for the OperationsManager database, ACS database, and the AEM file share. The designs must reflect organizational requirements for performance, capacity, and fault tolerance. This step is important because OperationsManager database design has a direct bearing on console performance. An inadequately sized ACS database infrastructure will result in queuing at the ACS collector; this will cause delays in insertion of Security event log events and denial of connections from ACS forwarders. Capacity shortage in the AEM file share will result in the inability of AEM to collect events.

Determinations made in Steps 2 and 3 will be used to size the databases and the file share. Data collected in Step 1 regarding the expectations for fault tolerance is used to assess the need for creating a fault-tolerant SQL Server configuration using failover clusters or SQL Server mirroring technologies. The resources identified in Step 1 for inclusion in ACS and AEM are used as input in estimating the ACS database size and the AEM file share size.

The number of management groups required, identified in Step 4, determines the number of times this step must be completed.

Step 7 focuses on the following:

* Design of the OperationsManager database infrastructure
* Design of the ACS database infrastructure
* Design of the AEM file share infrastructure

The design process for these three items includes specifications for hardware sizing, form factor, and fault-tolerance configuration options.

The official infrastructure sizing tool for Operations Manager 2007 R2 is the Sizing Helper, available for download at <http://blogs.technet.com/momteam/archive/2009/08/12/operations-manager-2007-r2-sizing-helper.aspx>.

The outputs of this step are infrastructure design hardware specifications and fault-tolerance configurations for the OperationsManager database, ACS database, and the AEM file share. This information will be used in Step 11 to design the network connections for the Operations Manager 2007 infrastructure.

## Planning Limitations

Ideally, the architectural design of the database roles would be based on the following information about each role:

* Integration (where this role fits relative to other roles)
* Capacity requirements
* Performance characteristics
* Unit sizing and volume expectations for data being stored by and retrieved from the role

As of this writing, none of this data is available for Operations Manager 2007.

Simulation of the load on the server environment from the expected number of agents might be another way to approach this, but no such load simulators are currently available.

Support limitations are published by the Operations Manager 2007 product group at <http://go.microsoft.com/fwlink/?LinkId=121517>. Note that these limits are based on testing performed by the product group. Testing was performed with all of the Microsoft standard management packs deployed in the environment.

Additional guidance is available from the product group on hardware form factors at <http://blogs.technet.com/momteam/archive/2008/04/10/opsmgr-2007-hardware-guidance-what-hardware-do-i-buy.aspx>. Note that no architectural justification is offered to support these configurations.

## Planning Approach

A number of factors need to be considered when trying to size and place the database roles:

* **The management packs that will be loaded.** Each additional management pack creates additional load on the server environment.
* **The number of agents.** This determines the load from incoming events, alerts, and performance data.
* **The number of concurrently working consoles.** Each console places a read load on the databases.
* **The number of web console users.** Each web console user places a load on the databases.

An examination of the supported configurations shows that:

* As the number of agents increases, a scale-out strategy, deploying additional servers, is optimal.
* As the number of ACS forwarders or AEM workstations increases, a scale-up strategy, to larger servers, is optimal.

No guidance is available for situations where supporting agents, ACS, and/or AEM are used together in the same management group.

Using this information, proceed with caution to design an implementation that is initially small, but capable of growth. Deploy on an increasingly larger scale and measure, learn, and adjust at each deployment.

## Task 1: Determine Resource Requirements for the OperationsManager Database Server

The OperationsManager database contains the configuration for the management group as well as all the recent operational data (event, alert, performance, and state data) collected from agent computers. Performance of the OperationsManager database role is one of the primary determinants in the performance of the Operations console.

The goal of this task is to determine the resource requirements (CPU, memory, and disk) for the OperationsManager database role.

The OperationsManager database size and load are based on two primary factors:

* The rate of data collection, which varies by the number of monitored devices and the management packs deployed.
* The rate of instance space change, which is the rate of change for the data that Operations Manager 2007 maintains to describe all the monitored computers, services, and applications in the management group. Updates to this data are expensive (in terms of performance) compared to writing new operational data.

The Operations Manager 2007 product group recommends that the size of the OperationsManager database should be kept below 50 GB for optimal database indexing and query performance. This is handled automatically by the grooming processes in Operations Manager 2007, which maintains a 7-day rolling dataset by clearing older data as part of a nightly maintenance process. A preconfigured alert will be sent when the free space in the OperationsManager database falls below 40 percent. This provides an opportunity to adjust retention settings to maintain adequate free space.

Document the resource requirements for the OperationsManager database server in Table A-9 “Sample Database Infrastructure Requirements” in the Appendix, and then move to Task 2.

## Task 2: Determine Resource Requirements for the ACS Database Server

The ACS database houses the central archive of security events collected from agent-managed computers enabled as ACS forwarders. When an organization has either large numbers of computers with audit requirements, aggressive security audit policies, or both, this database role will be very busy and the database can grow quickly.

The goal of this task is to determine the resource requirements for the ACS database role. Because the ratio of ACS collector servers to ACS database servers is 1:1, the number of ACS databases required is understood based on the decisions reached in Step 6.

### Sizing the Disk Subsystem

A process to estimate the requirements for the disk subsystem in terms of storage space, disk performance, and physical disks needed to meet the expected load has been discussed on the Operations Manager 2007 team blog at <http://blogs.technet.com/momteam/archive/2008/07/02/audit-collection-acs-database-and-disk-sizing-calculator-for-opsmgr-2007.aspx>.

This is based on the number of events per second generated on the computers on which ACS is enabled, along with the number of days data will be retained. The number of events per second can be estimated using the process that is in the Operations Manager Performance and Scalability Guide, available at <http://download.microsoft.com/download/d/3/6/d3633fa3-ce15-4071-be51-5e036a36f965/om2007_perfscal.doc>.

## Task 3: Determine Resource Requirements for the AEM File Share

Agents configured to participate in agentless exception monitoring upload exception data in .cab file format to a management server configured to host the AEM file share. The goal of this task is to determine the storage requirements of management servers hosting the AEM file share.

Determine the storage requirementsfor AEM and document findings in Table A-9 in the Appendix.

## Task 4: Determine Fault-Tolerance Configuration for the Database Roles and File Share

The OperationsManager database contains the configuration of the management group and all operational data used to populate the Operations console. Because there is only one OperationsManager database in a management group, it must be available for the management group to function. Fault-tolerant configurations can be used to provide service data redundancy in order to eliminate the OperationsManager database as a single point of failure.

The ACS database stores collected audit information and is critical to organizations that need to maintain complete audit data. Fault-tolerant configurations can ensure that recording and access to audit data continues uninterrupted.

The goal of this task is to determine the appropriate fault-tolerance configuration for the OperationsManager database, ACS database servers, and AEM file share. Fault-tolerance options for the databases are:

* **Failover cluster**. A server cluster provides service redundancy. The cluster can sustain a failure of one server and fail over to the remaining server without user intervention, resulting in only a brief interruption. Only active-passive cluster configurations are supported. A server cluster does not provide data redundancy as only one instance of the OperationsManager database is present on the server.
* SQL Server log shipping. Log shipping provides data redundancy. It is the process of automating the backup of database and transaction log files on a production SQL Server-based computer, and then restoring them onto a standby server.

Although the OperationsManager database can be recovered, the process is not completely automatic. Management server settings must be updated and services restarted on each management server to redirect them to the standby copy of the OperationsManager database after it is online. This could be scripted, but would involve some effort.

Note   While there is no reason why it should not work, database mirroring has not been tested and is currently not supported by the product team. Therefore, database mirroring is not recommended as a fault-tolerance measure for the OperationsManager database.

The AEM file share can be made fault tolerant by storing the file on a file server that is in a failover cluster. See Infrastructure Planning and Design Guide for Windows Server 2008 File Services at <http://www.microsoft.com/IPD>.

Document fault-tolerance configuration decisions for both the OperationsManager database and the ACS database infrastructures, using Table A-9 in the Appendix before proceeding to the next step.

The output of this step is the fault-tolerance approach for the OperationsManager database, the ACS database, and the AEM file share. This information will be used in Task 5 during determination of the appropriate server form factor for each of the database servers.

## Task 5: Select a Form Factor for the OperationsManager Database and ACS Database Servers

The goal of this task is to determine the most appropriate type of hardware on which to deploy the OperationsManager database and ACS database servers.

Form factor in this guide refers to the combination of the servers’ characteristics including:

* Processor architecture (32-bit versus 64-bit).
* Number of CPUs and their speed.
* Amount of memory installed.
* Disk storage capacity and disk subsystem design.
* Number of network adapter ports configured.

Since there is no specific architectural information available to determine the optimal form factor for the servers, this guide cannot make any specific recommendations for configurations.

The product group provides some information on hardware form factors at <http://blogs.technet.com/momteam/archive/2008/04/10/opsmgr-2007-hardware-guidance-what-hardware-do-i-buy.aspx>.

Document the selected form factor for servers in Table A-9 in the Appendix.

### **Use of Virtual Machines**

It is possible to use virtual machines (VMs) as an alternative to multiple physical systems and this is supported as documented in *Operations Manager 2007 R2 Supported Configurations* at <http://go.microsoft.com/fwlink/?LinkId=121517>.

If used, document the selected form factor for VMs in Table A-9 in the Appendix, and then proceed to the next step.

## Step Summary

The outputs of Step 7 are an infrastructure design, hardware specification, and fault-tolerance configurations for the OperationsManager database, ACS database, and the AEM file share. The information gathered in this step was recorded in Table A-9. This information is used in Step 11 during design of the network connections.

## Additional Reading

* Operations Manager 2007 R2 Design Guide: <http://technet.microsoft.com/en-us/library/dd789005.aspx>
* Operations Manager 2007 R2 Supported Configurations: <http://go.microsoft.com/fwlink/?LinkId=121517>

# Step 8: Design the Notification System

The goal of this step is to design the infrastructure to provide timely notification of alerts that require attention by Operations staff members, even when they are not logged on to the Operations console. This step is crucial to ensuring that IT support staff members are notified, even if parts of the infrastructure become unavailable. Work through this step for each management group.

In this step, data collected on resources in scope for monitoring is used to identify which channels are necessary to ensure notification in a variety of circumstances. Additionally, the redundancy requirements from Step 1 are used to assess the need for redundancy in the notification infrastructure.

The output of this step is a design for the notification interface to the RMS. This will be used to determine necessary infrastructure additions to the Operations Manager 2007 environment to support the organization’s alert notification requirements.

## Task 1: Determine the Required Notification Channels

This task involves deciding which notification channels to use to meet the organization’s needs. Effective planning will ensure that alert notifications are delivered in a timely manner and in an easily consumable format.

To identify the infrastructure necessary for notification delivery, use the requirements from Step 1 to select which notification channels are appropriate for the organization. The following notification channels are available in Operations Manager 2007:

* Email. Uses any Simple Mail Transfer Protocol (SMTP) server, such as Microsoft Exchange Server, Windows Server, or a third-party server, to deliver alert notifications by email.
* Instant message. Uses a session initiation protocol (SIP) server, such as Microsoft Office Communications Server 2007, to deliver alert notifications by instant message.
* Short Message Service. Uses a global system for mobile (GSM) communications modem to deliver alert notifications. (When determining whether to use a GSM modem in a data center environment, be sure to validate that an adequate signal is available before determining the best solution for the organization.)
* Command. Executes response through a Windows Command Prompt window. (This can be used to execute any number of command-line utilities, including programs that could send email through a telephone modem.)

Record the desired notification channels in Table A-10 “Selected Notification Channels” in the Appendix. After these have been selected, the appropriate fault-tolerance strategy can be designed.

## Task 2: Determine the Fault-Tolerance Strategy in Notifications

The goal of this task is to establish the fault-tolerance strategy for the infrastructure used in delivering Operations Manager 2007 alert notifications. Notifications are generated by the RMS and then flow through the notification channel (email, instant message, Short Message Service). Any one of these can be a single point of failure.

Fault tolerance in notification can be achieved using the following techniques in combination with each other:

* Provide redundancy in the link from the RMS to the notification channel. The network link to the notification channel can be set to fail over to an alternate link in the event of a problem.
* Provide redundancy within the notification channel. The email and command channels are the only notification channels that allow redundant configuration. For email notification, this requires purchasing additional hardware if existing servers cannot be configured to function as SMTP servers.
* Use multiple notification channels. By using multiple channels (such as email and Short Message Service), notifications will still be received in the event one channel is unavailable, such as in the event of an Exchange Server outage.

Note   Configuring multiple SMTP servers does not guarantee timely notification in the event of a Microsoft Exchange Server 2003 or Microsoft Exchange Server 2007 messaging issue. For example, if Internet connectivity fails, notifications will be queued on the Exchange Server-based computer. The best way to guarantee notification when email is down is through use of multiple notification channels.

Record the fault-tolerance strategy in Table A-10 in the Appendix. This data is used in the implementation phase to make hardware purchases, if necessary, as well as in configuring the notification channels during installation.

## Step Summary

In this step, data collected in Step 1 on resources in scope for monitoring were used to identify which notification channels are appropriate to ensure notification. Additionally, the Step 1 data related to redundancy requirements is used in this step to assess the need for redundancy in the infrastructure used for sending notifications on alerts raised in Operations Manager 2007.

Step 8 involved:

* Determining which channels will be used for notification delivery.
* Deciding what fault tolerance in the infrastructure will be used to deliver the notifications.
* Recording the data collected and decisions made in Table A-10 in the Appendix.

The output of this step is a design for the notification infrastructure to be used by Operations Manager 2007.

# Step 9: Determine Whether to Implement Reporting

The goal of this step is to review the data collected in Step 1 to determine whether reporting—and thus the Operations Manager 2007 Reporting Server role and associated data warehouse—are necessary to the organization.

This step must be completed for each management group that was designed in Step 4.

Reporting stores monitoring and alerting data, aggregating the performance data on an hourly and daily basis. It enables reporting of long-term trends that the operational database cannot deliver because the operational database quickly fills with records from individual events, and so must be regularly groomed. The data warehouse that is used for reporting can also receive data from multiple management groups, which enables an aggregated view across resources in different management groups. Failure to plan for reporting can result in a significant failure on the part of IT to meet the needs of the organization, as well as its own needs in troubleshooting and forecasting activities.

The output of this step is a determination of whether to include reporting in the Operations Manager 2007 architecture.

## Task 1: Identify the Need for Reporting

The goal of this task is to identify the need for reporting in the Operations Manager 2007 solution architecture. Review the data collected in Step 1 to determine answers to the following questions:

* Does the organization require visibility across multiple management groups? The reporting data warehouse can store data forwarded by multiple management groups. This enables consolidated reporting across multiple management groups if the organization desires it.
* Does the organization need to measure service level compliance for business-critical applications? The Service Level Dashboard Solution Accelerator uses data from the data warehouse to generate web browser-based reports on adherence to service level commitments for line-of-business (LOB) applications. Further information on the Service Level Dashboard is available at <http://technet.microsoft.com/en-us/library/cc540485.aspx>.
* Does the organization expect performance, availability, or other reports for business services? Forcing business units to view this data through the Operations console or web console is less practical than a report in portable document format (PDF) or hypertext markup language (HTML) format delivered through email. Also, adding more console connections is more expensive in terms of server resources.
* Do any IT functions require long-term data collection for capacity planning, performance tracking, or trend analysis? The data required for these functions cannot be delivered through performance views in the Operations console. That is because the Operations console renders data from the OperationsManager database, which must be limited in size in order to maintain its write performance.
* Will Microsoft System Center Virtual Machine Manager be used in this environment, with reporting enabled? Reporting data from Operations Manager 2007 can be integrated into the Virtual Machine Manager (VMM) console. If this is done, the reporting data from the Operations Manager data warehouse appears under a tab in the VMM console. If this integration will be required in the VMM console, the Operations Manager 2007 data warehouse will need to be implemented as well as the Operations Manager 2007 virtualization management pack.

Review the answers to the questions in this task. If the answer was yesto any of the questions, an infrastructure design for Operations Manager 2007 reporting in Step 10 is required. If the answer was noto all questions, skip Step 10, and continue to Step 11.

## Evaluating the Characteristics

Technical criteria are not the only factors that should be considered when making an infrastructure design decision. The decision should also be mapped to appropriate operational criteria or characteristics. The following tables compare each option according to the characteristics that are applicable to this decision-making topic.

Table 3. Evaluate Characteristics

|  |  |  |
| --- | --- | --- |
| Complexity | Description | Rating |
| Implement reporting | Reporting requires that the data warehouse and Operations Manager 2007 Reporting Server be added to the design, which will increase the complexity. | ↑ |
| No reporting | If reporting is not implemented, the design will remain less complex. | → |
| Cost | Description | Rating |
| Implement reporting | The additional infrastructure required to deliver reporting will increase the cost of capital equipment, software, and support. | ↑ |
| No reporting | If reporting is not implemented, the cost will not increase. | → |

## Validating with the Business

Reporting is the Operations Manager 2007 component that is most likely to affect the business. Business stakeholders were consulted in Step 1 to determine the requirements for reporting. If it is decided that reporting is not required, re-confirm with those stakeholders that they do not need the reports that Operations Manager 2007 reporting can deliver.

## Step Summary

The goal of this step was to review data collected in Step 1 to determine whether reporting is necessary and thus to determine whether the Operations Manager 2007 Reporting Server role and associated data warehouse are necessary to the organization.

In this step, data collected on resources in scope for monitoring in Step 1 was used to identify the need for reporting in the organization. Step 1 data related to redundancy requirements was used to assess the need for redundancy in the reporting infrastructure.

The output of this step is a decision on whether to include reporting in the Operations Manager 2007 solution architecture.

This decision dictates the need to move to Step 10 to design the Operations Manager 2007 reporting infrastructure. If the answers to the questions in this step were no, skip Step 10 and move directly to Step 11.

## Additional Reading

* Reporting in Operations Manager 2007: <http://technet.microsoft.com/en-us/library/bb309653.aspx>
* Service Level Dashboard for Operations Manager 2007: <http://technet.microsoft.com/en-us/library/cc540485.aspx>

# Step 10: Design the Data Warehouse, Reporting Server, and Service Level Dashboard

In this step, data collected in Step 1 is used to design the data warehouse, the Operations Manager 2007 Reporting Server, and optionally, the server for the Service Level Dashboard.

Step 10 involves:

* Determining whether the data warehouse will be used to consolidate reporting data across management groups.
* Determining projected database size based on choices for the retention period.
* Determining redundancy requirements for Operations Manager 2007 reporting.
* Determining server size and role distribution based on database size and the architectural guidance in the Operations Manager 2007 R2 Design Guide.

The output of this step is the detailed infrastructure design for Operations Manager 2007 reporting, including server hardware specifications, role distribution, and any high-availability configurations. This data will be used in the implementation phase to build the Operations Manager 2007 reporting infrastructure.

## Task 1: Determine the Data Consolidation Strategy Across Management Groups

The data warehouse can be used to store data from different management groups; it can then provide reports on resources across those management groups.

Refer to the reporting requirements that were established in Step 1 and to the management group design that was generated in Step 4 to determine whether reporting is required across management groups and, if so, across which groups. Use this information to create a row for each data warehouse that will be required in Table A-11 “Sample Reporting Infrastructure Requirements” in the Appendix.

Proceed through the remaining tasks for each data warehouse instance.

## Task 2: Determine Data-Retention Requirements

The goal of this task is to figure out how long reporting data needs to be kept.

To identify the appropriate retention period, determine how far into the past (weeks or months) data is of interest to business units, as well as to IT. If this information is not already known, ask readers about reports in both the business units and IT. There may be regulatory requirements that will dictate how long data must be stored; these must be determined by consulting with departments responsible for regulatory compliance.

The output of this task is the required retention period for data housed in the reporting data warehouse. This will be used as input to design the data warehouse in the next task.

## Task 3: Determine Data Warehouse Size Requirements

It is possible to estimate the size of the data warehouse based on the data retention requirements documented in Task 2 and the number of devices in scope for monitoring. There are some tools available for arriving at this estimate.

The Operations Manager 2007 Database and Data Warehouse Size Calculator, available at <http://blogs.technet.com/momteam/archive/2007/10/15/opsmgr-2007-database-and-data-warehouse-size-calculator.aspx>, is based on data from Microsoft IT’s implementation and some customer sites. There are three inputs to this tool: the number of days that data should be retained, the number of servers, and the number of clients. All other values are constants. The degree to which it can be extrapolated to other environments is unknown, and it does not take into account the number of management packs that will be deployed. So it should be used as an estimator with caution.

Operations Manager 2007 R2 includes a report, the Data Warehouse Properties Report, that shows the average rate of data in flow (by type and by aggregation level) and predicts the size of the data warehouse when the number of days data held reaches the maximum data retention parameter. Of course, in order to generate this report, the data warehouse must already be deployed. So be prepared to use this tool, once Operations Manager 2007 is up and running, to adjust the size of the data warehouse on an ongoing basis.

Once the space requirement for the data warehouse has been estimated, add more storage space to provide 40 percent free space in the database, which will allow for efficient database maintenance and grooming operations. Divide the initial space estimate by 0.60 to arrive at this number.

The output of this task is the estimated amount of storage required to contain the data in the data warehouse. This will be used in Task 4 to identify the database size required.

## Task 4: Select a Form Factor for the Servers

The goal of this task is to determine the most appropriate type of hardware on which to deploy the following servers:

* The SQL Server-based server that is used to host the data warehouse.
* The SQL Server Reporting Services-based server that is used to create and deliver reports from the data warehouse.
* The Windows SharePoint Services-based server that is used by the Service Level Dashboard Solution Accelerator.

Use the reporting requirements that were determined in Step 1 to understand how many reporting users will be on the system concurrently and whether reports will be run on demand during peak hours or automatically published during off-peak hours. This will enable some understanding of whether the read load of reporting will run at the same time as the maximum write load into the data warehouse.

Refer to the Infrastructure Planning and Design: Microsoft SQL Server 2008 guide at [www.microsoft.com/IPD](http://www.microsoft.com/ipd), and review the guidance available from the product group on hardware form factors at <http://blogs.technet.com/momteam/archive/2008/04/10/opsmgr-2007-hardware-guidance-what-hardware-do-i-buy.aspx>. Then select a form factor for the servers running SQL Server for the data warehouse and the SQL Server Reporting Services.

It is possible to use virtual machines (VMs) as an alternative to multiple physical systems and this is supported as documented inOperations Manager 2007 R2 Supported Configurationsat <http://go.microsoft.com/fwlink/?LinkId=121517>**.**

Service Level Dashboard V2.0 uses a server running Windows SharePoint Services 3.0 to read, format, and display data directly from the Operations Manager 2007 R2 data warehouse. There is no specific architectural guidance available for the Windows SharePoint Services-based server form factor, so design the server following standard Windows SharePoint Services design guidance using memory that matches the organization’s standard form factor. The disk capacity required by the Windows SharePoint Services-based server must be sufficient to store the Service Level Dashboard configuration files.

The Windows SharePoint Services-based server could be run on the same server as SQL Reporting Services. As an alternative, it is also possible to run the Windows SharePoint Services-based server in a VM**.**

Document the selected form factors in Table A-11 in the Appendix, and then proceed to the next step.

## Task 5: Determine Fault-Tolerance Strategy

Based on data collected in Step 1, determine the redundancy expectations for reporting. If high availability is a requirement, the reporting data warehouse must be configured as a clustered SQL Server database. There is currently no high-availability configuration for SQL Server 2005 Reporting Services.

If the Service Level Dashboard will be designed and is required to be fault tolerant, design the Windows SharePoint Services-based server infrastructure using SharePoint product group guidance.

The output of this task is the fault-tolerance strategy for Operations Manager 2007 reporting. Record the decisions in Table A-11 in the Appendix.

## Step Summary

In this step, data collected in Step 1 was used to estimate growth and size of the reporting data warehouse.

The activities that were undertaken in this step are:

* Determination of projected database size based on database growth estimates and free space requirements for a given retention period.
* Determination of redundancy requirements for Operations Manager 2007 reporting.
* Determination of server size and role distribution based on the guidance in the Operations Manager 2007 R2 Design Guide at <http://technet.microsoft.com/en-us/library/dd789005.aspx>.

The output of this step is the detailed infrastructure design for Operations Manager 2007 reporting, including server hardware specifications, role distribution, and any high-availability configurations such as clustered SQL Server-based computers.   
The information gathered in this step was recorded in Table A-11 in the Appendix.   
This data is used in the implementation phase to build the Operations Manager 2007 reporting infrastructure.

# Step 11: Design the Network Connections

In this step, the following data will be used to determine network bandwidth and network port requirements:

* Data collected in Step 1 on network topology and inventory of resources in scope for monitoring.
* The management packs that will be deployed, as determined in Step 2.
* Server role distribution, determined in Step 6.
* Database role distribution, decided in Step 7.
* Reporting infrastructure requirements from Step 10.

This information is used in the implementation phase of the project to determine necessary changes in network firewalls as well as any network links requiring additional network bandwidth to support the minimum requirements of Operations Manager 2007.

## Task 1: Determine Where Additional Bandwidth Is Required

The goal of this task is to identify and record the network bandwidth required, as well as the bandwidth available, between each of the Operations Manager 2007 components. This information is recorded in Table A-12 “Sample Network Bandwidth and TCP/IP Port Requirements” in the Appendix.

To make these determinations, perform the following steps:

1. Use the output of Steps 6, 7, 8, and 10 to map the connections between the roles and the bandwidth requirements of each, using the Operations Manager 2007 R2 Supported Configurations document at <http://go.microsoft.com/fwlink/?LinkId=121517>. Record this information in Table A-12 in the Appendix.
2. Measure the available bandwidth on these connections by requesting the average available bandwidth during peak usage periods. Record this information in Table A-12 in the Appendix.
3. Compare the required bandwidth against the available bandwidth to determine whether additional bandwidth will be required, and record this in Table A-12 in the Appendix.

## Task 2: Determine Network Port Requirements

The goal of this task is to map the supported firewall scenarios to the locations of the roles in order to identify the network ports that must be opened. The network ports required for communication depend on the placement of server roles throughout the network.

To determine firewall port requirements, review server placement decisions from Steps 6 and 7 and compare them with the port requirements in Operations Manager 2007 R2 Supported Configurations at <http://go.microsoft.com/fwlink/?LinkId=121517>. This will establish which ports need to be opened on firewalls in the environment. Record the network port requirements in Table A-12 in the Appendix.

## Step Summary

The goals of this step are to ensure that network connectivity between server roles and between server roles and agents is sufficient in terms of network bandwidth and that the required firewall rules are in place to allow traffic to flow as necessary.

In this step, the following data was used to determine network bandwidth and network port requirements:

* Data collected in Step 1 on network topology and inventory of resources in scope for monitoring.
* Server role distribution, determined in Step 6.
* Database role distribution, decided in Step 7.
* Reporting infrastructure requirements from Step 10.

The output of this step was a table containing the bandwidth requirements between physical network sites as well as the network ports that must be opened through network firewalls. Table A-12 in the Appendix was used to record the information in this step.

This information is used in the implementation phase of the project to identify necessary changes in network firewalls as well as any network links requiring additional network bandwidth to support the minimum requirements of Operations Manager 2007.

## Additional Reading

* Operations Manager 2007 R2 Supported Configurations: <http://go.microsoft.com/fwlink/?LinkId=121517>
* System Center Central home page: <http://www.systemcentercentral.com/>
* System Center Operations Manager 2007 R2 TechCenter home page: <http://technet.microsoft.com/en-us/opsmgr/dd239186.aspx>

# Conclusion

This guide has summarized the critical design decisions, activities, and tasks required to enable a successful design of System Center Operations Manager 2007. It focused on decisions involving:

* Which resources are to be monitored by Operations Manager 2007.
* The infrastructure necessary to employ Operations Manager 2007 to monitor the selected resources.
* The server roles, role placement, databases, and connectivity of the Operations Manager 2007 infrastructure.

This was done by leading the reader through the eleven steps in the decision flow to arrive at a successful design. Where appropriate, the decisions and tasks have been illustrated with typical usage scenarios.

The guide has discussed the technical aspects, service characteristics, and business requirements needed to complete a comprehensive review of the decision-making process.

As stated in the introduction, it is very important at the start of an Operations Manager 2007 project to have a full understanding of the business objectives for the project:

* What benefits does the business expect to achieve through the use of resource monitoring?
* What is the value of those benefits, and therefore the cost case for using Operations Manager 2007 to deliver those benefits?

The business objectives should be prioritized at the start of the project so that they are clearly understood and agreed upon between IT and the business.

When an architecture has been drafted, limited “pilot” tests should be conducted before a major rollout begins so that lessons learned can be incorporated back into the design.

This guide, when used in conjunction with product documentation, allows organizations to confidently plan the implementation of Operations Manager 2007.

## Feedback

Please direct questions and comments about this guide to [satfdbk@microsoft.com](mailto:satfdbk@microsoft.com?subject=IPD%20-%20System%20Center%20Operations%20Manager%202007).

We value your feedback on the usefulness of this guide. Please complete the following **Solution Accelerators Satisfaction Survey**, available at <http://go.microsoft.com/fwlink/?LinkID=132579>, and help us build better guidance and tools.

# 

# Appendix: Job Aids

Step 1. Use a job aid like the one shown below to record the business services that should be monitored by Operations Manager 2007.

Table A-1. Sample Business Service Inventory

| **Business service** | **Owner** | **Reports required** | **Service function** |
| --- | --- | --- | --- |
| CRM system | Sales | Monthly service availability report | Used to track potential and current customers, contact history and sales activities |

Table A-1. Sample Business Service Inventory (continued)

| **Description of a sample transaction** | **Service level requirements (SLAs)** | **Application performance or availability monitoring required?** | **Retain security logs?** |
| --- | --- | --- | --- |
| Sales representative logs into the CRM website, reviews calls for the day. Tasks are recorded in the customer or prospect record. Clicks Save to save. | Must be available from 7 A.M. to  9 P.M. | Yes, availability | Yes, for 2 years |

Steps 1 and 2. Use a job aid like the one shown below to record the components that business services (identified in Step 1) depend on, along with their relative priority for monitoring.

Table A-2. Sample Business Service Component Map

| **Service** | **Component** | **Requires synthetic transaction monitoring?** | **Monitoring priority** |
| --- | --- | --- | --- |
| Time Tracking | AD DS | No | Critical |
| SQL Server database | Yes | Critical |
| DNS | No | Critical |
| WINS | No | Low |
| Network switches | No | Medium |
| IIS servers | Yes | Medium |
| Linux file server | No | Medium |

Table A-2. Sample Business Service Component Map (continued)

| **Service** | **Dependent components** | **Management pack** |
| --- | --- | --- |
| Time Tracking | If AD DS fails, authorization in Time Tracking is unavailable. | Microsoft |
| All user input stored here. | Microsoft |
| Failure prevents client connections. | Microsoft |
| Used in client authentication, but handled by DNS if WINS fails. | Microsoft |
| Switches are redundant. Single switch failure would not cause outage. | Company X |
| Single switch failure would have little impact. Two or more failures would cause outage. | Microsoft |
| Single server failure would have little impact. Three or more failures would cause outage. | Microsoft |

Steps 1 and 2. Use a job aid like the one shown below to record the existing monitoring systems, monitoring gaps, and key details of administrative model.

Table A-3. Sample Monitoring and Process Analysis

| Objective | Answers/comments |
| --- | --- |
| Identify gaps in Operations Manager 2007 functionality versus resources in-scope for monitoring. |  |
| Determine if monitoring that is currently in place fills functionality gaps. |  |
| Identify and document the components and business services in the gap covered by existing systems. |  |
| What monitoring systems are currently in place? |  |
| Who uses monitoring consoles with existing systems? |  |
| What product connectors are required? Where can they be obtained? |  |
| Describe the administrative model of the organization.  Identify any security boundaries between autonomous support groups. |  |

Step 3. Use a job aid like the one shown below to record synthetic transaction monitoring requirements.

Table A-4. Sample Synthetic Monitoring Implementation Planner

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Business service** | **Client interfaces** | **Information flow in transaction** | **Locations using service** | **Watcher node location and number of watchers** |
| Inventory system | .NET Windows client | Client calls middle tier application server.  Middle tier retrieves data from SQL Server database called “inventory master” on production cluster. | Cleveland, Omaha, Orlando,  San Antonio | Omaha (4),  San Antonio (7) |
| **Recommended synthetic transactions** | | | | |
| Browser session accessing product inventory | | | | |
| Perform OLE database from middle tier | | | | |

Table A-4. Sample Synthetic Monitoring Implementation Planner (continued)

|  |  |  |  |
| --- | --- | --- | --- |
| **Load on watcher** | **Network load** | **Repeat frequency** | **Dedicated or shared** |
| 3% CPU, 40 MB, 20 IOps | 30 Kb/s | 15 mins | Dedicated |
| **Recommended synthetic transactions** | | | |
| Browser session accessing product inventory | | | |
| Perform OLE database from middle tier | | | |

Step 3. Use a job aid like the one shown below to record client monitoring requirements.

Table A-5. Sample Client Monitoring Implementation Planner

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Workstation name(s) | Business- critical? | Monitor as sample? | Client monitoring type | Comments |
| All cash registers | Y | N | Individual (Business-critical client) |  |
| All accounting, finance, and IT purchasing workstations | N | Y | Collective client |  |

**Step 4.** Use a job aid like the one shown below to record management group requirements.

Table A-6. Sample Management Group Requirements

|  |  |
| --- | --- |
| Management group descriptive name | Reason required |
| U.S. Production | Local management group for connected management groups |
| U.S. Pre-production | For management pack tuning prior to production release |
| APAC Production | Japanese language management group in Tokyo |
| APAC Pre-production | For management pack tuning (in APAC management group) prior to production release |

Step 5. Use a job aid like the one shown below to record mutual authentication decisions.

Table A-7. Mutual Authentication Decisions

|  |  |
| --- | --- |
| Decision | Response (Y or N) |
| Decision 1: Are agents in an AD DS forest? |  |
| Decision 2: Can a forest trust or cross-domain trust be used? |  |
| Decision 3: Can an Operations Manager 2007 gateway be set up with a certificate? |  |

Step 6. Use a job aid like the one shown below to record Operations Manager 2007 server infrastructure requirements.

Table A-8. Sample Server Infrastructure Requirements

|  |  |  |
| --- | --- | --- |
| Role | Location | Resource requirements and form factor |
| Management server | HQ data center | 1 x 2.8 GHz, 4 GB of RAM, 2-drive RAID 1  Form factor: HP DL380 or Dell 2950 |
| Gateway server | Toledo branch | 1 x 2.8 GHz, 2 GB of RAM, 2-drive RAID 1  Form factor: VM |

Step 7. Use a job aid like the one shown below to record OperationsManager database infrastructure requirements.

Table A-9. Sample Database Infrastructure Requirements

|  |  |  |
| --- | --- | --- |
| Role | Location | Resource requirements and form factors |
| OperationsManager database | HQ data center | 2 x 2.8 GHz, 8 GB of RAM, 2-drive RAID 1  SQL Server data: 4-drive RAID 0+1  SQL Server logs: 2-drive RAID 1  Form factor: 2 x HP DL380 or Dell 2950  Fault tolerance: Server cluster |
| ACS database | HQ data center | 2 x 2.8 GHz, 8 GB of RAM, 2-drive RAID 1  SQL Server data: 4-drive RAID 0+1  SQL Server logs: 2-drive RAID 1  Form factor: 1 x HP DL580 or Dell 6950  Fault tolerance: None |
| AEM file share | HQ data center | 200 GB on data center SAN |

Step 8. Use a job aid like the one shown below to record the selected notification channels.

Table A-10. Selected Notification Channels

|  |  |  |
| --- | --- | --- |
| Management group | Notification methods | Notification fault tolerance |
|  |  |  |
|  |  |  |

Step 10. Use a job aid like the one shown below to record Operations Manager 2007 reporting infrastructure requirements.

Table A-11. Sample Reporting Infrastructure Requirements

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Data warehouse instance name | Management groups providing data | How long data will be kept | Storage required | Location of data warehouse instance | Resource requirements and form factors |
| DW-1 | Ohio purchasing  Denver  Chicago sales | 120 days | 300GB | HQ data center | 2 x 2.8 GHz,  4 GB of RAM,  2-drive RAID 1  SQL Server-based server data:  4-drive RAID 0+1  SQL Server-based server logs:  2-drive RAID 1  Form factor:  HP DL580 or Dell 6950  Fault tolerance: None |

Table A-11. Sample Reporting Infrastructure Requirements (continued)

|  |  |  |  |
| --- | --- | --- | --- |
| Reporting Server name | Data warehouses providing data | Location of Reporting Server | Resource requirements and form factor |
| Report Server - 1 | DW-1 | Ohio | 2 x 2.8 GHz,  4 GB of RAM,  2-drive RAID 1  Form factor:  HP DL380 or Dell 2950  Fault tolerance: None |

Step 11. Use a job aid like the one shown below to record Operations Manager 2007 network bandwidth and TCP/IP port requirements.

Table A-12. Sample Network Bandwidth and TCP/IP Port Requirements

|  |  |  |  |
| --- | --- | --- | --- |
| **Source site** | **Destination site** | **Required bandwidth (k)** | **Available bandwidth (k)** |
| NYC hub | ATL branch | 832 | 1500 |
| NYC hub | BOI branch | 64 | 50 |
| NYC hub | PHX branch | 640 | 3000 |

Table A-12. Sample Network Bandwidth and TCP/IP Port Requirements (continued)

|  |  |  |
| --- | --- | --- |
| **Additional bandwidth required** | **Network port requirements** | **Comments (optional)** |
| N | 5723, 51909 | Gateway server, ACS collector to NYC hub |
| Y | 5723 | Gateway server to NYC hub |
| N | 5723 | 10 agents to management server at NYC hub |

# Version History

|  |  |  |
| --- | --- | --- |
| **Version** | **Description** | **Date** |
| 2.1 | Minor updates to this guide to reflect current IPD template. | July 2010 |
| 2.0 | Agents are now available to discover, monitor, and manage a number of UNIX and Linux platforms.  The Operations Manager 2007 Data Warehouse database includes all of the customization that is required for service level tracking, ready to provide data to the Service Level Dashboard.  The scale of the existing URL monitoring has been increased and is easier to set up. Management packs are available for monitoring Exchange Server and SQL Server transaction performance and availability.  Process monitoring: This detects whether desired and undesired processes are running, and if they are, how many of them are running. In addition, it provides monitoring of the CPU and memory being consumed by processes.  Notifications: This provides a mechanism to set up SMTP more easily and to subscribe to notifications to events.  Run As capability: Provides improved granularity and control of security settings.  Import Management Packs Wizard: This wizard can be used to import management packs and updates to them, either from a local or network disk or directly from the management pack catalog on the Internet.  Update to Visio Export: The Visio exports that are obtained from Operations Manager 2007 R2 now include the metadata that is necessary for future versions of Visio and SharePoint to query the OperationsManager database and update the status of exported objects in the diagram.  Maintenance mode: The process of placing a computer and all its related objects into maintenance mode has been streamlined.  UI Performance and Usability: The Operations console performance has been greatly improved. | October  2009 |
| 1.0 | First release. | June 2008 |

# Acknowledgments

The Solution Accelerators – Management and Infrastructure (SA-MI) team acknowledges and thanks the people who produced the Infrastructure Planning and Design Guide for Microsoft System Center Operations Manager 2007. The following people were either directly responsible for or made a substantial contribution to the writing, development, and testing of this guide.

Contributors:

* Jude Chosnyk – *GrandMasters*
* Joe Coulombe – Microsoft
* Charles Denny – Microsoft
* Michael Kaczmarek – Microsoft
* Robin Maher – *Microsoft*
* Fergus Stewart – Microsoft
* Melissa Stowe *– Microsoft*
* Pete Zerger – Studio B Productions

Reviewers:

* Tony Chou – Microsoft
* Fernando Gebara Filho – Microsoft
* John Joyner – ClearPointe
* Frank Koch – Microsoft
* Rob Kuehfus – *Microsoft*
* René Scholten – Capgemini
* Satya Vel – Microsoft

Editors:

* Laurie Dunham – *Microsoft*
* Dave Field – *Studio B Productions*
* Ruth Preston – *Volt Technical Services*
* Pat Rytkonen – *Volt Technical Services*