Symantec™ IT Management Suite 8.5 powered by Altiris™ technology Planning for Implementation Guide

Symantec™ IT Management Suite 8.5 powered by Altiris™ technology Planning for Implementation Guide

Legal Notice

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

https://www.symantec.com

Symantec Support

All support services will be delivered in accordance with your support agreement and the then-current Enterprise Technical Support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Contents

Chapter 1

Introducing IT Management Suite

This chapter includes the following topics:

About IT Management Suite

Note: Current documentation applies to the most recent version of the product.

IT Management Suite (ITMS) combines client and server configuration management with IT asset and service management. It promotes effective service delivery and helps reduce the cost and complexity of managing corporate IT assets. These assets may include desktops, laptops, thin clients, and servers in heterogeneous environments running Windows, Linux, UNIX, or Mac operating systems. You can manage all of the features of the suite through a central console on a common platform: the Symantec Management Platform. This common platform integrates management functions to accelerate automation for better service, value, and IT efficiency.

See "What you can do with IT Management Suite" on page 9.

IT Management Suite comprises of the following management capabilities:

- Server management
  The server management incorporates a variety of wizards and other features that let you automate configuration, stage tasks, and create policies to manage your servers. The server management capabilities support Windows, UNIX, and Linux operating systems. In

addition, the same management disciplines are applied to both physical systems and virtual systems, including both Microsoft Hyper-V and VMware.

- Client management
  The client management helps you discover the resources in your network, and lets you check their state. The reporting tools help you identify problems and take immediate action to fix them. The client management capabilities support Windows, Linux, UNIX, and Mac operating systems.
- IT asset management
  IT asset management builds upon solid inventory foundations for configuration management. It helps you accurately value both your discoverable and non-discoverable assets, and tracks your assets and your asset-related information. You can manage contracts, software license compliance, and procurement processes as well as the configuration items that are associated with your assets.

See "What you can do with IT Management Suite" on page 9.

See "How IT Management Suite works" on page 10.

What you can do with IT Management Suite

IT Management Suite (ITMS) helps you improve service delivery, increase efficiency, and reduce costs.

You can do the following with IT Management Suite:

- Manage from a central console.
  You can centrally manage heterogeneous client and server endpoints.
- Manage remotely.
  One-to-one remote-management capabilities let you avoid desk-side or server-side visits.
- Automate tasks.
  The task engine lets you perform multiple remote-management tasks simultaneously.
- Automate policy enforcement.
  The policy engine lets you detect and remediate automatically, without human involvement.
- Automate processes.
  The workflow engine lets you automate human and system interactions to eliminate latency errors and omissions.
- Create self-service.
  The service catalog lets you avoid calls or requests entirely with best-practice self-service.
- Centrally manage software.
  Software management includes software inventory, patching, delivery, and license management.

See “About IT Management Suite” on page 8.

How IT Management Suite works

IT Management Suite (ITMS) is a bundling of Symantec products and software. IT Management Suite helps you deploy, manage, support, and retire the various computers, devices, servers, and IT assets in your organization. IT Management Suite includes IT asset management and client and server configuration management.

See “About IT Management Suite” on page 8.

IT Management Suite has the following key features and functions:

- Centralized management platform

  All of the parts of IT Management Suite are built on a common foundation that is called the Symantec Management Platform. The Symantec Management Platform is a set of core services that all of the parts of IT Management Suite share. These services can include aspects such as security, reporting, communications, and data storage.

  IT Management Suite introduces an improved management interface that gets you where you want to be faster. Common concepts such as managing computers, delivering software, and managing licenses and deployment are consolidated into an integrated experience. When you click on a computer, resource management details are immediately visible. Powerful search features help you drill down and build filters in a short period of time. You can quickly save the searches for future use.

- Common database and management console

  The different parts of the platform can read and write from a common database. The database is called the Configuration Management Database (CMDB). Even though IT Management Suite covers a wide variety of IT-related capabilities, you interact with all of its technologies through a common Web-based user interface. This interface is called the Symantec Management Console.

- Management agent and management server

  IT Management Suite can discover the computers that are present in your environment. You can install the Symantec Management Agent on these computers. The agent lets you gather very detailed information about them. It regularly sends information about the computer to a management server computer called Notification Server. Notification Server processes the information about your computers and stores it in a common database. The Symantec Management Agent gives you robust control and visibility into the hardware and software on your managed computers and servers. It helps you to maintain your corporate standards and policies remotely from the Web-based Symantec Management Console.

- Asset Management

  You can use the data in the CMDB to manage your assets more efficiently. For example, you can use this information with reports and filters to gain visibility into and track metrics on the assets in your environment

- License management

  License management and asset management and usage are tightly integrated. Within the software display is an at-a-glance view of the current deployments and cost details. These details are based on the current installations and the purchasing details. A graphic can help you to determine if a software product is over-deployed or under-deployed, and evaluate its current usage. It gives visibility into the financial implications of a product. You can see the potential savings from harvesting licenses, and you can see the cost effect when a product is over-deployed.

- Software Management

  You can see what software is installed, how often it is used, and how many licenses for it you have purchased. This type of information can help you determine the IT assets you need to purchase. You can also use this information to determine how to maximize your software investment and when to replace or decommission software. In addition, you can use IT Management Suite to take action on the information that it gathers. For example, IT Management Suite may discover that certain software is installed and licensed but is not used. You can configure the suite to remove the unused software.

  In IT Management Suite, the Software Catalog interface is streamlined and redesigned. Any software that is found is stored in the newly discovered list. From this list you can quickly determine whether you want to make the identified software a managed product. If not, you can assign it to unmanaged software. After you identify software as a managed software product, you can manage all elements of it in a single interface. Inventory, metering, delivery, and license tracking are all presented in a single interface.

  The Managed Delivery feature separates the schedule for delivery and the schedule for execution. You can first stage packages in advance, and then later schedule the execution.

- Task and policy engines

  Notification Server has two components that are called the task engine and the policy engine. These components let you do work on your managed computers. You can use policies to maintain consistent standards, and you can use tasks to execute sequential steps. Policy-based management can allow the managed computer autonomy whether it is in a connected or disconnected state. Task-based management follows the traditional server to client communications paradigm.

- Managed computers

  Managed computers have the management agent installed. They regularly communicate with the Notification Server computer. When a managed computer contacts Notification Server, it checks to see if you have configured any work for it to do.

  The agent can check to see if the computer on which it is installed is compliant with a policy. For example you can set up a policy to ensure that all of your managed computers have the latest version of software. If it is not compliant, then the agent can download and install the software according to your settings. When software is remotely executed on target computers with Notification Server, this software is called a software package.

- Patch Management

You can use IT Management Suite to keep your computers secure, patched, and compliant. IT Management Suite lets you manage all aspects of applying Microsoft Windows security updates and patches.

- Provisioning

  You can remotely provision and deploy standardized operating system images to your computers. This functionality includes bare-metal deployment and re-imaging computers to return them to known-good states.

- Migration and deployment

  Deployment Solution is natively integrated with the Symantec Management Platform. Consequently, you work with Deployment Solution and Symantec Management Platform through a single console, database, and agent. IT Management Suite provides many enhancements to the Deployment Solution console.

  The DeployAnywhere capability supports all plug-and-play driver types for hardware-independent imaging. This addition complements the support for hardware abstraction layers (HAL), network interface cards, and mass-storage-controller drivers to provide a complete hardware-independent imaging solution. Management for the driver database is now available through the console. You can consolidate driver management because both imaging and scripted operating system installations consume the drivers in the DeployAnywhere database.

  Ghost imaging supports multicasting. PC transplant supports Microsoft Office 2010 (32-bit and 64-bit).

  Enhanced Virtual Machine Management capabilities streamline configuration and extend the virtual machine creation wizard. The wizard can execute any Deployment Solution job as part of the virtual machine creation process. This ability lets you leverage existing server provisioning jobs and apply them to virtual server provisioning.

- Server health monitoring

  IT Management Suite also lets you monitor and maintain the health of your servers. You can monitor key metrics and indicators of your server health performance. These metrics can be viewed in real time. With the task engine, you can proactively manage your servers. For example, you can automate complex sequences of fail-safe measures such as provisioning a backup server in the event that a server crashes. You can configure the system to alert you if a specific metric starts to indicate a potential problem. You can then resolve that problem so that it does not manifest in the future.

- Workflow engine

  IT Management Includes a workflow engine that lets you automate human and system interactions. You can set up robust workflows to automatically complete many of the sequential tasks that are required for efficient service management.

  In addition to form builders, you can use the full component generator capability for access to third-party technologies. These technologies include HR or finance systems, and the Workflow portal. The Workflow portal lets you track the overall process as a workflow moves through the various stages.

- Advanced reporting and IT Analytics

  The executive dashboard and trend analysis give you a representative view of your IT assets. Key performance indicators let you measure critical success factors for your organization and quickly assess trends of how these measures change over time. You can use ad-hoc data mining to construct pivot table reports. The reports are based on predefined measures and dimensions. The functionality allows for easy manipulation of the data so you do not have to be a SQL expert to access the information you need. Multidimensional analysis and robust graphical reporting are incorporated to help you arrive at your answers with very little customization and without waiting.

  The MultiCMDB feature provides global IT Analytics reporting across multiple CMDBs without the need to replicate large amounts of data.

See “What you can do with IT Management Suite” on page 9.

Understanding the components of IT Management Suite

This chapter includes the following topics:

About the Symantec Management Platform

Note: Current documentation applies to the most recent version of the product.

The Symantec Management Platform provides a set of services that IT-related solutions can leverage. Solutions plug into the platform and take advantage of the platform services, such as security, reporting, communications, package deployment, and Configuration Management Database (CMDB) data. Because solutions share the same platform, they can share platform services as well as data. Shared data is more useful than data that is only available to a single solution. For example, one solution collects data about the software that is installed on company computers and another solution uses the data to manage software licenses. A third solution can also use this data to help you update software. This close integration of solutions and the platform makes it easier for you to use the different solutions because they work in a common environment and are administered through a common interface.

The platform provides the following services:

- Role-based security
- Client communications and management
- Execution of scheduled or event-triggered tasks and policies
- Package deployment and installation
- Reporting
- Centralized management through a single, common interface
- Configuration Management Database (CMDB)
- Software Management Framework

When you install a solution or suite, the platform is also installed if it is not already installed.

See "Components of the Symantec Management Platform" on page 16.

Core architectural components of Symantec Management Platform

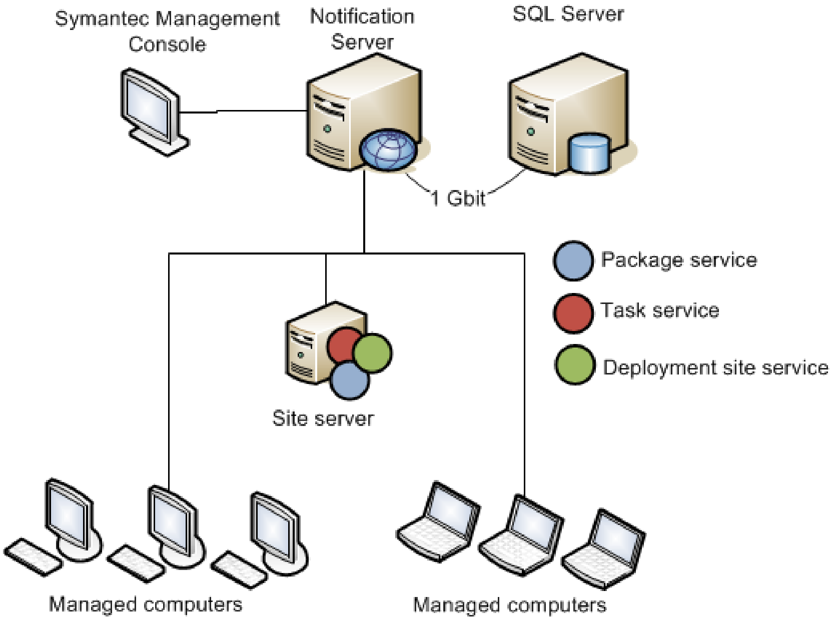
Symantec Management Platform has four main architectural components.

See "IT Management planning considerations" on page 28.

They are as follows:

- Notification Server and its Web-based Symantec Management Console
- SQL Server
- Site servers
  Site servers can include task servers, package servers, network boot servers, and monitor service.
- Managed computers

Figure 2-1 Core architectural components of Symantec Management Platform



Components of the Symantec Management Platform

Table 2-1 Components of the Symantec Management Platform

Component	Description
Notification Server and Symantec Management Console	The Symantec Management Platform service that processes events, facilitates communications with managed computers, and coordinates the work of the other Symantec Management Platform services. The console is the Notification Server computer's Web-based user interface that lets you manage the platform and its solutions.
Configuration Management Database (CMDB)	The database that stores all of the information about managed computers.
Site servers	The Symantec Management Platform can host several types of middleware components, such as package services, task services, and network boot services. The official name for a middleware component is "site service." Any component that hosts a site service is known as a site server. Site servers can host one or more of these services.

Table 2-1 Components of the Symantec Management Platform *(continued)*

Component	Description
Symantec Management Agent	The software that is installed on a computer to enable Notification Server to monitor and manage it. After the Symantec Management Agent is installed, that computer becomes a managed computer.
Software Management Framework	An interface that lets you create and manage the software resources that are in the Software Catalog. It also lets you manage the packages that are in the Software Library. The **Software** view provides a central location for initiating the software-related tasks that are performed in your organization.
Reports	A way to gather automated information. You can view reports for any managed computer from the Symantec Management Console.

See "About the Symantec Management Platform" on page 14.

Solutions of IT Management Suite

Table 2-2 IT Management Suite solutions and components

Suite/Platform	Solution/Component	Description
Asset Management Suite	Asset Management Solution	Asset Management Solution lets you set up and manage different asset management processes. It helps you accurately value your assets, track ownership, and maintain associations with related documents. Additionally, it aligns with ITIL standards.
	CMDB Solution	CMDB Solution lets you model configuration items, resources, and the relationships between them in a central database. It lets you facilitate the identification of all components and relationships, and instigate any required changes. The solution actively manages resources according to user-specified instructions in jobs, tasks, configuration policies, and custom CMDB rules.
Client Management Suite	Deployment Solution	Deployment Solution helps to reduce the cost of deploying and managing servers, desktops, and notebooks from a centralized location in your environment. It offers operating system deployment, configuration, personality migration of computers, and software deployment across different hardware platforms and operating systems.

Table 2-2 IT Management Suite solutions and components *(continued)*

Suite/Platform	Solution/Component	Description
	Inventory Solution	Inventory Solution lets you gather inventory data about the computers, users, operating systems, and installed software applications in your environment. You can collect inventory data from the computers that run Windows, UNIX, Linux, and Mac. After you gather inventory data, you can analyze it using predefined or custom reports.
	IT Analytics	IT Analytics Solution software complements and expands upon the traditional reporting that is offered in most Altiris solutions. It brings exciting new features and capabilities to Notification Server because it incorporates multi-dimensional analysis and robust graphical reporting and distribution features. This functionality allows users to explore data on their own, without advanced knowledge of databases or third-party reporting tools. It empowers users to ask and answer their own questions quickly, easily, and effectively.
	Patch Management Solution	Patch Management Solution for Windows lets you scan Windows computers for the updates that they require, and view the results of the scan. The system lets you automate the download and distribution of software updates. You can create filters of the computers and apply the patch to the computers that need it. Patch Management Solution for Linux lets you scan Red Hat and Novell Linux computers for security vulnerabilities. The solution then reports on the findings and lets you automate the download and distribution of needed errata, or software updates. The solution downloads the required patches and provides wizards to help you deploy them. Patch Management Solution for Mac lets you scan Mac computers for the updates that they require. The solution then reports on the findings and lets you automate the downloading and distribution of needed updates. You can distribute all or some of the updates.
	Symantec Remote Access Connector	Symantec Remote Access Connector is an IT Management Suite functionality that lets you configure and integrate a third-party remote connection tool such as Microsoft® Remote Desktop Connection or Bomgar™ Remote Support Solution with IT Management Suite.

Table 2-2 IT Management Suite solutions and components *(continued)*

Suite/Platform	Solution/Component	Description
	Real-Time System Manager	Real-Time System Manager provides you detailed real-time information about a managed computer, and lets you remotely perform different administrative tasks in real time. Real-Time System Manager also lets you run some of the management tasks on a collection of computers. You can run the tasks immediately, or on a schedule.
	Software Management Solution	Software Management Solution provides intelligent and bandwidth-sensitive distribution and management of software from a central Web console. It leverages the Software Catalog and Software Library to ensure that the required software gets installed, remains installed, and runs without interference from other software. Software Management Solution also lets users directly download and install approved software or request other software.
	Workflow Solution	Symantec Workflow is a security process development framework that you can use to create both automated business processes and security processes. These processes provide for increased repeatability, control, and accountability while reducing overall workload. The Symantec Workflow framework also lets you create Workflow processes that integrate Symantec tools into your organization's unique business processes. Once deployed, Workflow processes can respond automatically to environmental variables. Workflow processes can also allow for human interface points when a process calls for someone to make a decision with accountability.
Server Management Suite	Deployment Solution	Deployment Solution helps to reduce the cost of deploying and managing servers, desktops, and notebooks from a centralized location in your environment. It offers operating system deployment, configuration, personality migration of computers, and software deployment across different hardware platforms and operating systems.
	Inventory Solution	Inventory Solution lets you gather inventory data about the computers, users, operating systems, and installed software applications in your environment. You can collect inventory data from the computers that run Windows, UNIX, Linux, and Mac. After you gather inventory data, you can analyze it using predefined or custom reports.

Table 2-2 IT Management Suite solutions and components *(continued)*

Suite/Platform	Solution/Component	Description
	Inventory Pack for Servers	Inventory Pack for Servers gathers server-based inventory data from servers. It runs on top of Inventory Solution and uses the same Inventory plug-ins, tasks, and wizards.
	IT Analytics	IT Analytics Solution software complements and expands upon the traditional reporting that is offered in most Altiris solutions. It brings exciting new features and capabilities to Notification Server because it incorporates multi-dimensional analysis and robust graphical reporting and distribution features. This functionality allows users to explore data on their own, without advanced knowledge of databases or third-party reporting tools. It empowers users to ask and answer their own questions quickly, easily, and effectively. Altiris IT Analytics Symantec Endpoint Protection Pack is also included in this solution.
	Monitor Solution	Monitor Solution for Servers lets you monitor various aspects of computer operating systems, applications, and devices. These aspects can include events, processes, and performance. This ability helps you ensure that your servers and your devices work and reduces the costs of server and network monitoring.
	Monitor Pack for Servers	Monitor Pack for Servers works with the Monitor Solution core components of the Symantec Management Platform. It lets you monitor operating system performance, services, and events of your Windows, UNIX, and Linux server environment.
	Patch Management Solution	Patch Management Solution for Windows lets you scan Windows computers for the updates that they require, and view the results of the scan. The system lets you automate the download and distribution of software updates. You can create filters of the computers and apply the patch to the computers that need it. Patch Management Solution for Linux lets you scan Red Hat and Novell Linux computers for security vulnerabilities. The solution then reports on the findings and lets you automate the download and distribution of needed errata, or software updates. The solution downloads the required patches and provides wizards to help you deploy them. Patch Management Solution for Mac lets you scan Mac computers for the updates that they require. The solution then reports on the findings and lets you automate the downloading and distribution of needed updates. You can distribute all or some of the updates.

Table 2-2 IT Management Suite solutions and components *(continued)*

Suite/Platform	Solution/Component	Description
	Real-Time System Manager	Real-Time System Manager provides you detailed real-time information about a managed computer, and lets you remotely perform different administrative tasks in real time. Real-Time System Manager also lets you run some of the management tasks on a collection of computers. You can run the tasks immediately, or on a schedule.
	Software Management Solution	Software Management Solution provides intelligent and bandwidth-sensitive distribution and management of software from a central Web console. It leverages the Software Catalog and Software Library to ensure that the required software gets installed, remains installed, and runs without interference from other software. Software Management Solution supports software virtualization technology, which lets you install software into a virtual layer on the client computer. Software Management Solution also lets users directly download and install approved software or request other software.
	Virtual Machine Management	Virtual Machine Management is a component of Server Management Suite that lets you perform the virtualization process on your network. You can create virtual environments of servers, storage devices, and network resources on a single physical server. Virtualization enhances the efficiency and productivity of the hardware resources and helps to reduce administrative costs.
	Workflow Solution	Symantec Workflow is a security process development framework that you can use to create both automated business processes and security processes. These processes provide for increased repeatability, control, and accountability while reducing overall workload. The Symantec Workflow framework also lets you create Workflow processes that integrate Symantec tools into your organization's unique business processes. Once deployed, Workflow processes can respond automatically to environmental variables. Workflow processes can also allow for human interface points when a process calls for someone to make a decision with accountability.

See “About IT Management Suite” on page 8.

About the Symantec Management Agent communication using persistent connection

Persistent connection in IT Management Suite enables real time data transfer from and to Symantec Management Agent and lets you perform tasks on client computers in real time. For example, you can gather inventory on client computers in real time to validate the current hardware or software state.

Persistent connection in IT Management Suite uses a WebSocket communication protocol. WebSocket operates over HTTPS and uses standard HTTPS port (443) for communication. It does not require keeping additional ports open on the servers or on the client computers. It also uses existing SSL certificates for communication.

Persistent connection supports all applicable settings that are configured in the communication profile. For example, persistent connection uses proxy settings and alternative HTTPS hostname settings if they are configured in a communication profile.

All IT Management Suite infrastructure components (including Internet gateway and remote Task Server) support persistent connection. Also, Windows (Windows 7 and above, Windows Server 2008 and above), Mac, and Linux agents support persistent connection.

When the persistent connection is enabled, all Symantec Management Agents regardless of their location (intranet and Internet) use persistent connection for communicating with Notification Server and site servers.

When the persistent connection is enabled for Notification Server, site servers and all required agents, it is used for all management traffic: registrations, sending NSEs, policy downloads, etc. Note that the WebSocket protocol is not used for package downloads.

If persistent connection is disabled or terminated by an intermediate hardware, the communication reverts to using legacy HTTP or HTTPS protocols.

About Cloud-enabled Management

Cloud-enabled Management lets you manage client computers over the Internet even if they are outside of the corporate environment and cannot access the management servers directly. The managed computers do not need to use a VPN connection to your organization's network.

You can apply Cloud-enabled Management in the following scenarios:

- An organization with many employees traveling or working outside the office (outside the corporate intranet).
- A managed service provider (MSP) managing external companies.
- Highly distributed companies with many small offices or employees working from home.

When you implement Cloud-enabled Management, the Notification Server computer and site servers are not directly exposed to the Internet. Therefore, Symantec Management Agent communicates with the Notification Server computer and the site servers through an Internet gateway. Usually, two or more Internet gateways should be available to maintain reliable management of cloud-enabled client computers and to provide failover options. Each Internet gateway can support routing to multiple independent Notification Servers.

To use cloud-enabled management, you must install an Internet gateway server. The Internet gateway works as a tunneling proxy. It ensures the privacy and safety of the data that is passed between an agent and a management server with HTTPS communications. The Internet gateway is located in a demilitarized zone (DMZ) between two firewalls. It accepts incoming connections from authorized client computers on the Internet and forwards them to the appropriate Notification Servers and site servers inside your network. The Internet gateway blocks any connection attempts by unauthorized client computers.

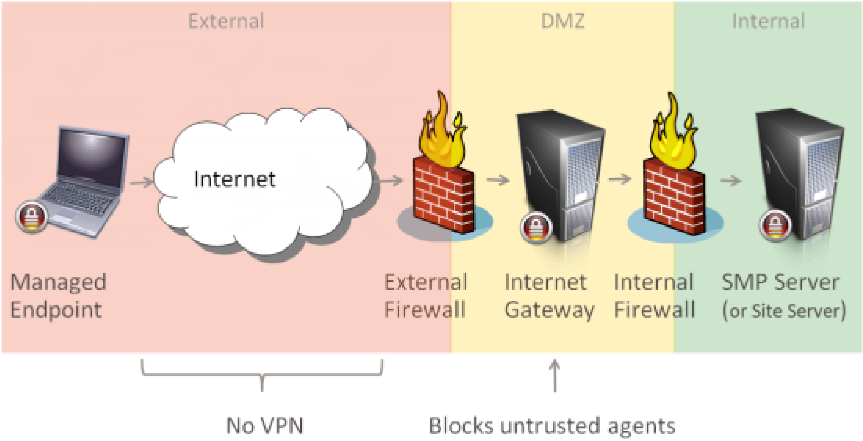
The Symantec Management Agent automatically determines whether routing the communication through the Internet gateway is needed or not. If a cloud-enabled computer has direct access to the local network using VPN, the agent automatically switches to a direct communication with Notification Server. If a cloud-enabled computer is outside the corporate network, the agent routes all communication on the Internet to Notification Server through the Internet gateway.

See “Recommended Internet gateway hardware” on page 49.

Note: Cloud-enabled Management is supported on Microsoft Windows computers and Mac OS X computers.

Not all solutions in IT Management Suite support Cloud-enabled Management. For more information on Cloud-enabled Management support for a particular solution, refer to the solution documentation.

Figure 2-2 Cloud-enabled Management



To use the Cloud-enabled Management feature, you do the following:

- Set up the infrastructure and configure your servers and client computers to use SSL.
- Install and configure the Internet gateways, configure the Cloud-enabled Management policies, and set up the Symantec Management Agents to support the Cloud-enabled Management environment.
- (Optional) Perform troubleshooting and maintenance tasks.

Deploying software using Deployment Solution

Deployment Solution lets you create and deploy hardware-independent images, install operating systems, and manage them for client computers such as desktops, servers, and notebooks, from a centralized location. The solution also lets you capture and distribute personality, perform system configurations at run-time, and copy files or folders across computers. The application of the Deployment Solution functionality depends on the type of client computer that the solution manages. The client computer can be a bare metal computer, a predefined computer, or a managed computer. Most of the deployment-related functions rollout as tasks and are executed on the client computers. Deployment Solution is tightly coupled with the Symantec Management Platform and leverages the function of the site server components of SMP such as Package Server (PS) and Task Server (TS). The solution requires PS-specific and TS-specific deployment components to be deployed on the site servers for execution of deployment tasks. Moreover, to execute deployment tasks on the client computers, Deployment Solution requires operating system-specific Deployment plug-ins to be installed on them.

The Deployment Solution components that are required to execute deployment tasks are as follows:

- Deployment Solution Package Server component
- Deployment Solution Task Server component
- Deployment Solution plug-in for the following operating systems:
  - Windows
  - Linux
  - Mac

Setting up the preboot environment in Deployment Solution

Before you start execution of deployment tasks, you must create and set up the preboot configurations in Deployment Solution. The preboot configurations that are created are required to boot the client computers to execute the deployment tasks on them. In Deployment Solution, there are two types of preboot environments that you can configure whose details are as follows:

Table 2-3

Type of preboot configuration	Description
Pre-Boot Execution Environment (PXE)	In Deployment Solution, a Pre-Boot Execution Environment (PXE) is created using the **Preboot Configuration** and is distributed through the Network Boot Service (NBS), which is installed on a site server. The NBS component comprises of the PXE service, SymantecNetworkBootService(PXE and BSDP) and the TFTP service, SymantecNetworkBootServiceTftp. After a computer is added to a network, the PXE service boots the computer to the preboot environment using a preboot package of the supported operating system. Preboot package is also known as the PXE image. In Deployment Solution, you configure the preboot package and re-build the preboot environment before you roll out the configured preboot environment on the NBS site servers. A configured preboot package contains the OS-specific PXE environment files, the OS-specific agent, and the Deployment plug-in, which is also known as the Deployment agent. The OS-specific preboot packages that you can configure are as follows: ■ WinPE for Windows ■ LinuxPE for Linux ■ Netboot for Mac

Table 2-3 *(continued)*

Type of preboot configuration	Description
Automation environment	An automation environment is the configured preboot environment that is installed locally on the client computer. An automation environment installation lets you boot client computers to the preboot environment.. Similar to PXE environment, the automation environment too contains OS-specific preboot package that is installed on the client computers. The preboot package that is installed as a folder in the client computers is known as the automation folder. By default, for Windows, the automation folder is, PEInstall and for Linux computers the automation folder is, LinInstall folder is created on the client computer.

For more details about the PXE environment and Automation environment, refer to the *Deployment Solution User Guide*.

Methods of delivering preboot environments

Client computers boot to the preboot environment through the Network Boot Service (NBS) that is installed on the site server. Based on the type of client computer to boot, NBS must be configured. The types of client computers that Deployment Solution boots and manages are unknown computer, predefined computer, and managed computer. The configuration of NBS can be performed through the Symantec Management Console.

For more details about configuring types of client computers through NBS, refer to the *Deployment Solution User Guide*

Key Features of Deployment Solution

The two key features of Deployment Solution are as follows:

- Imaging functionality of Deployment Solution
  Deployment Solution lets you create an image of a client computer and deploy it on multiple client computers. When an image is created, a Symantec Management Platform resource for that image is also created. The resource is stored as a package on Notification Server and is distributed to all the package servers that are present in the network. The image resource is used when you build tasks to deploy the images. When a deploy image task is sent to a client computer it fetches the image from the package server that is closest to the client computer.
  You can create disk images and backup images of client computers. Deployment Solution provides Ghost and RapiDeploy tools to create images of client computers that are installed with Windows or Linux operating system and the symDeploMac tool to create image of for client computer installed with Mac operating system.
  For more details about creating and deploying images, refer to the *Deployment Solution User Guide*.

- Install OS functionality of Deployment Solution

  Deployment Solution lets you install Windows, Linux, and Mac operating system on client computers. To install an operating system on the client computer you must first boot the client computer in the preboot environment of the operating system that you want to install on the client computer. Deployment Solution provides operating system-specific tasks to install operating system on the client computers.

  For Windows and Mac, the packages of the operating systems are added on Notification Server and from Notification Server they are distributed to all the package servers in the network. When an Install OS task is sent to a client computer it fetches the package from the package server that is closest to the client computer. For Linux, the operating system packages are placed on an anonymous HTTP or an FTP server.

  For more details about installing operating system, refer to the *Deployment Solution User Guide*.

Planning for IT Management Suite

This chapter includes the following topics:

IT Management planning considerations

Many factors and considerations may influence an implementation plan. To design your Symantec Management Platform infrastructure, you must assess your specific organizational features and requirements.

See "Core architectural components of Symantec Management Platform" on page 15.

Your requirements can include several variables. Some of these variables may include the following:

- The geographic implications of the environment.
  A centralized management design uses multiple Notification Server computers to support a variety of IT distribution models. For example, you can have central corporate office with thousands of managed computers as well as both large branches and small branches. The centralized design can be effective for managing global policies and tasks. If your IT organization is primarily centralized, then the Symantec Management Platform can be designed to support it. In such an environment, the platform may use a parent Notification

Server computer that is connected to additional child Notification Server computers in a hierarchy.

A decentralized management design consists of multiple dispersed sites and network segments that support subordinate sites and network segments. The decentralized design does not use hierarchy but instead it uses multiple Notification Server computers that operate independently.

- The future growth of the organization.

  The infrastructure design may require room for growth. If possible the architecture should reflect both the current organization and the vision for the organization in the coming years.

- The IT management team's distribution and its policies.

  The operations that IT manages centrally and locally influence design. Some IT tasks may need to be done from a central location or some tasks may need to be done from local sites. The security policies of the organization influence the design.

  Your organizational structure may determine the component placement and design of the infrastructure. How the organization’s staff works on a daily basis and how the business process is established influences the plan. Different branches of the organization, security requirements, or geographical requirements may all require separate Notification Server management domains. Different groups and roles managing endpoints may require Notification Server role and scope-based security. Role and scope-based security adds load on the Notification Server computer.

- The connectivity ranges of the environment.

  The connectivity ranges of the environment may determine the placement of components. For example, there may be a first-tier site that is well connected, but the second tier sites are poorly connected. Traveling users may dial in, use VPN, or may be connected using Cloud-enabled Management (CEM) from a remote location..

- How many of the IT Management Suite functions are used.

  The number of actively used functions influences the choice of hardware for Notification Server. For example, a server that only collects inventory demands less powerful hardware than a server with all of IT Management Suite functions used.

- The concurrent console usage and reporting needs.

  Concurrent use of the console can add additional processor utilization for heavy use of the Symantec Management Console. You can use the console to create custom reports to view information about the environment. Many custom reports are written with advanced Structured Query Language (SQL) statements that require significant database processing power. Having many users run these reports concurrently on the Notification Server computer can degrade its performance.

  If the organization requires heavy custom reporting, consider implementing a separate Reporting Notification Server. While it does mean that the organization needs to invest in an additional server, it provides for the separation of duties in the infrastructure. The Notification Server computer responsible for managing endpoints is able to dedicate its processing to that function. The Notification Server computer responsible for providing reports dedicates its process to that other function. With this configuration, you can use stand-alone replication to forward resource inventory information from the agent-facing Notification Server computer to the reporting Notification Server computer.

Another consideration is the memory cost of each of the concurrent console sessions from IIS on the Notification Server computer. You can calculate this memory requirement at approximately 20MB per console connection.

About planning your SQL Server configuration

The following information provides guidelines for SQL server configuration for a Symantec Configuration Management Database (CMDB) computer. You can follow these guidelines to tune the performance of the SQL Server computer that hosts the CMDB. These guidelines are not exclusive, and additional configuration options may be appropriate depending on the specifics of your environment. For detailed information about SQL Server configuration, refer to Microsoft’s documentation.

Many additional articles about SQL server setup, configuration, and maintenance are available on the Symantec Knowledge Base. The Symantec Knowledge Base is available at www.symantec.com/business/theme.jsp?themeid=support-knowledgebase.

Table 3-1 Considerations for planning your SQL Server configuration

Consideration	Description
Hardware	You can use recommended hardware guidelines to help tune the performance of your SQL Server computer.
Hard drive configuration	The way that you configure the hard drives of your SQL Server computer influences your overall performance. You can use disk configuration recommendations to maximize throughput and tune the performance of your SQL Server computer. See “About hard drive configuration for SQL Server” on page 31.
Database sizing	You can use database sizing guidelines to help tune the performance of your SQL Server computer. See “About database sizing for SQL Server” on page 32.
Memory management	You can use memory management guidelines to help tune the performance of your SQL Server computer. See “About memory management for SQL Server” on page 33.

Table 3-1 Considerations for planning your SQL Server configuration *(continued)*

Consideration	Description
SQL maintenance plan	You can use maintenance plan recommendations to help tune the performance of your SQL Server computer. See "About maintaining SQL database" on page 34.
SQL failover clustering	You can use SQL failover clustering, a method of creating high availability for your Symantec Management Platform. See "About using Microsoft SQL failover clustering" on page 35.

About hard drive configuration for SQL Server

The throughput of the SQL Server is a primary consideration for Symantec Management Platform performance. The way that you configure your hard drives on SQL Server influences throughput. If you use spindle drives (HDD) or a Storage area network (SAN), consider performing detailed throughput analysis in making your decision between Solid-state drive (SSD) and other storage options.

SSD and high performance SAN are optimum for SQL performance. They can support greater than a million IOPS due to high IO bandwidth and low IO latency. Compare this to single HDDs that support 150-200 IOPS. If using HDD, high performance RAID configurations with multiple channels are recommended.

When you use traditional HDD in RAID configurations, RAID 10 and RAID 0+1 are considered high performance. RAID 5 is not a high performance configuration and is not recommended.

For the best performance, make sure that the operating system, SQL data file, TempDB database, and the log file each has a dedicated volume. To improve performance further, you can split the data file and the TempDB database across multiple volumes. The number of volumes that you use should match the number of processor cores in your SQL Server. A recommendation for high performance is to use parallelism with the same number of disk volumes as the number of logical processor cores. You can split the SQL data file and the transaction log file to match the number of processor cores.

The data file requires both high read-write performance and redundancy.

The TempDB database needs high read-write performance, but redundancy is not necessary. The TempDB database acts as a temporary working area for many processes. The TempDB database requires very high speed; however, it is not used for storage and it is cleared regularly.

The transaction log also requires high disk throughput for optimal system performance.

On-box configuration

A combined Notification Server and SQL database installation can be installed on HDD, solid-state drives, or a combination of the two. We recommend that you use mirrored HDD for the operating system and Notification Server, and SSD for the SQL database. This approach provides the best combination of performance, cost effectiveness, and ease of implementation.

See "Recommended configuration for Notification Server with locally installed SQL database" on page 49.

See "About planning your SQL Server configuration" on page 30.

About database sizing for SQL Server

You can use database sizing guidelines to help tune the performance of your SQL Server computer. A Symantec Management Platform installation with no solutions and no managed computers creates a database size of about 300 MB. An additional 500 managed computers can increase the size to approximately 500 MB. Databases also grow as solutions are introduced and used.

Allow between 750KB and 1 MB of space in the database for every managed computer. This sizing does not account for database fragmentation beyond initial creation. Actual sizes vary based on the solutions that are installed and the specific configuration of policies, tasks, and schedules. The database maintenance strategy that you use also influences your database size.

Autogrow is a SQL Server setting you can use to help with unexpected data growth. However, do not rely on autogrow to manage your database file sizes. You should monitor the files and re-size them according to your projected needs during maintenance.

To choose your autogrow setting, estimate the expected maximum sizes of the data file and the transaction log file. To estimate this size you can monitor the growth of these files in a pre-production environment. Set the autogrow increment for your data file and transaction log files to 10 to 20 percent higher than your initial estimate.

Do not use the autoshrink feature with the Symantec Management Platform. Auto shrink runs periodically in the background. It consumes CPU and I/O cycles which can cause unexpected performance degradation. Autoshrink can continually shrink and re-grow the data files. This process causes fragmentation of the database file. This fragmentation may degrade both sequential transfers and random accesses.

After you have estimated the approximate size of the database, you should create a database file of this size before you install Notification Server. This step ensures that adequate space is available. It also reduces negative performance from a database that continually grows. To further improve performance, you should defragment and re-index the database after its initial installation.

The CMDB SQL Server should not host additional third-party database applications because Symantec Management Platform has very high performance demands. However, additional CMDB databases can be hosted on the same SQL Server because each database has similar traffic requirements and hardware configuration needs.

You can have a single SQL instance that shares a single TempDB database, or multiple database instances can each have a dedicated TempDB database. Multiple database instances minimize risk for potential contention but require more disk arrays.

You may require the individual databases of each Notification Server computer to exist on a separate instance. They may need to be separate instances to avoid TempDB database contention.

See “About planning your SQL Server configuration” on page 30.

About memory management for SQL Server

Memory management is an important part of tuning SQL Server performance. Memory management is especially important when SQL is run locally on the Notification Server computer.

Table 3-2 Memory configuration options for SQL Server

Option	Description
Maximum server memory	This SQL setting limits the memory that SQL can consume. Set **Maximum server memory** value in the **Server memory options** page. Leave enough memory for the operating system and tools such as SQL Management Studio to run effectively. For example: around 4-6 GB less than the amount of RAM installed.
Windows memory usage	Set Windows memory usage to favor Programs over System Cache. SQL Server does its own data caching to improve performance.

Table 3-2 Memory configuration options for SQL Server *(continued)*

Option	Description
Enable the option to **Optimize for Ad hoc Workloads**	When IT Management Suite is used there are a high degree of Ad-hoc or dynamic queries that are made through the day to day use of the Symantec Management Console and background actions. These types of queries are not cached using the default settings that are found in Microsoft SQL Server and can result in perceived console performance and Notification Server efficiency. When the “Optimize for Ad hoc Workloads setting” is enabled the plan cache (also known as the “procedure cache”) may benefit from enabling this feature. When enabled, the SQL Query Optimizer takes in a batch for execution and tries to locate an appropriate query plan in the plan cache. If it’s unable to find one, it compiles a plan and stores it in cache so that the next time it’s called, the cost of compiling such a plan is not incurred The increase in performance takes place when the particular query is run for a second time, as it is now cached. It is important to understand that the plan takes up space in memory and should not be implemented on Microsoft SQL Servers that are already maximizing available memory. This setting is found under the Advanced page of the SQL Server Instance Settings within Microsoft SQL Server.

See “About planning your SQL Server configuration” on page 30.

About maintaining SQL database

A SQL maintenance plan for rebuilding indexes and setting the index free space percentage to 10% within the Symantec/Altiris databases should be scheduled to run at least monthly (preferably weekly). This maintenance plan should also be configured to update column statistics (index statistics are updated during the index rebuild process). It is recommended that this plan be scheduled to run at a time when database utilization by the Symantec applications is at its lowest. This could be on a Sunday during the day or a during a scheduled maintenance cycle, etc.

Follow these recommendations for optimal maintenance of SQL:

- Update Statistics (nightly)
  - Ensures query processor makes “the best” choices it can given ITMS implementation.
  - Or, enable Auto Update Statistics Asynchronously
    Memory Leak in SQL - get latest update
    Database Properties > Options page.
    Enabling affects your ability to put a database into single-user mode (For Maintenance)
- Regular Database Page Maintenance

Rebuild Indexes (Monthly)
Reorganize pages (Weekly)

- Regular backup
  Simple Recovery Mode - yields lower IO but you should have an aggressive backup strategy Vs. FULL logging with backups

For more information see the following knowledge base article:

http://www.symantec.com/docs/HOWTO8589

About using Microsoft SQL failover clustering

Failover clustering is a process in which the operating system and SQL Server work together to provide availability in the event of an application failure, hardware failure, or operating-system error. Failover clustering provides hardware redundancy through a configuration in which mission critical resources are transferred from a failing computer to an equally configured database server automatically.

However, failover clustering is not a load balancing solution. Failover is not intended to improve database performance, reduce the maintenance required, protect your system against external threats, prevent unrecoverable software failures, single points of failure (such as non-redundant storage and hardware), or natural disasters.

Symantec recommends that you have sufficient knowledge and experience with Microsoft SQL failover methodologies before you attempt them in an ITMS or other suite or solution implementation.

You should also consider that Microsoft SQL Servers be properly sized with enough hardware capacity to run adequately for the expected failover workload.

IT Management Suite supports the following SQL Server failover methods:

- Two-node SQL cluster configuration (single instance failover cluster)
- Single clustered SQL configuration hosting two instances of CMDB (multi-instance failover cluster)

See “About planning your SQL Server configuration” on page 30.

About planning your site servers

A site is a management construct that allows mappings of subnets to site services. Site services are an extension of the Symantec Management Agent. When a site service is installed on a managed node, it promotes the Symantec Management Agent to a site server.

Task, package, monitor, and network boot services are all site server roles. These site services can be deployed in multiple combinations to meet endpoint demands. A remote site may only need a package server or a network boot server. A task server may be needed only at the datacenter. Your topology and your use of solutions determines if you should combine site services onto a single computer or use dedicated computers.

The standard Notification Server install only includes the minimum site server requirements. Additional site servers may use either a Windows desktop operating system or a Windows Server operating system. A site with fewer than 100 endpoints may only require 10 sessions; however; a Windows server may be required for larger remote sites.

Your primary consideration for a site server's hardware and operating system is the number of concurrent sessions that you need. A desktop operating system is limited to 10 or 20 concurrent TCP connections, but the server operating system does not have this limitation.

Note: If you install package server component of Deployment Solution or package service on a Windows 7 or Windows 2008 computer, you must install the IIS 6 compatibility mode services on it.

See "About the package service" on page 40.

See "About the task service" on page 37.

See "About the network boot service" on page 41.

About planning a site design

Consider the following recommendations when planning your site design:

- Plan, design, configure, and monitor sites for site health.
  In all infrastructures, you should consider planning, design, configuration, and monitoring activities for maintenance.
- Favor Sites, and Organizational Groups over Hierarchy.
  Do not rely on hierarchy to manage over geographically disperse implementations. Instead, use site servers. Your site design should account for the bandwidth needs and the total node counts.
- Use constrained package servers and cascade your package staging.
  You can use constrained package servers as the primary method to ensure that communications occur as you expect. However, some key agent communications do go directly to the ITMS server. These include requests such as GetPackageInfo, CreateResource, PostEvent, etc.
- Limit Task Server Communications on the ITMS Server.
  Provide Connection Management and Request Consolidation and not bandwidth consolidation.
  Do not have agents connect to the parent. Generally, you should have at least one task server.

See “About planning your site servers” on page 35.

About site maintenance

Site maintenance is the management of sites, subnets, and site services in your organization. You can manage your computers according to site and subnet, which lets you control groups of computers while you minimize bandwidth consumption. A site is typically a physical location in your organization (such as a particular building, or a level of a building). A subnet is a range of logical addresses on your network.

Under normal operating conditions, each package server or task server services only the Symantec Management Agents that exist within the assigned sites. If no sites have been defined, all site servers are available to service all Symantec Management Agents (although this method is not recommended).

If no sites are defined for a package server or a task server, Notification Server uses the following rules:

- Notification Server first tries to find any site servers on the same subnet as the requesting computer. If any are found, these site servers are returned to the Symantec Management Agent.
- If no site servers are in the same subnet as the requesting computer, all site servers are returned to the Symantec Management Agent.

You can assign site servers to sites by using the following methods:

- Assign the subnet that contains the site server to a site.
- Assign the site server to a site.
- Use Active Directory import to perform the task.
  Active Directory import overrides any subnets and sites that conflict with it. For example, if you manually assign subnets to a site that conflicts with the data from Active Directory import, the Active Directory information is used.

After the list of available site servers is returned to the Symantec Management Agent, the agent chooses the most suitable site server.

Site servers and managed computers may have multiple NICs and IP addresses; therefore, they may belong to more than one site through subnet assignment.

About the task service

Task communications are unique from policy communications. Managed computers start policy communications, and the server starts task communications.

You can do the following with the task service:

- Execute multiple tasks in a defined sequence that is called a Job.

- Provide logic to handle task errors or other return codes.
- Deliver command-line and VBscript capabilities to managed computers.
- Provide out-of-the-box power management.
- Execute client-side and server-side tasks.
- Reuse tasks in multiple Jobs. Tasks can be cloned and modified as required.

Symantec recommends at least one task server per Notification Server. Tasks place a performance demand on the Notification Server computer's processor and memory because it must regularly send tickle packets and receive execution status. This demand can negatively influence SQL data loading and user interface responsiveness.

See "About planning your site servers" on page 35.

Task servers use a high number of operating system sessions. If a task server supports more than 100 managed computers, a Windows Server operating system is recommended as it supports more concurrent operating system sessions. If a task server supports less than 100 managed computers, a desktop operating system might be adequate.

The task server computer must have IIS 7.0 or IIS 8.5 and .NET Framework 4.5.1 features enabled. Starting from IT Management version 7.6, task server cannot be installed to Windows XP and Windows 2003 operating system.

Task servers do not require high-performance hardware. A moderate speed processor is adequate. Disk IO is not a significant factor in task server performance.

Task servers are good at offloading performance demands from Notification Server. They are not designed to address network bandwidth limitations. You can put a task server in the same subnet as Notification Server because it has little influence on minimizing network traffic.

Use the following guidelines to configure task services within your infrastructure:

- Symantec recommends at least one task server per Notification Server.
  After the initial dedicated task server, add additional task servers for every 10,000 to 15,000 endpoints.
- You can load-balance multiple task servers within large sites to make sure that agents have the latest task execution.
- You can reduce the load on task servers if you increase the Task Update Interval and the Maximum Time Between Tickle Events settings. By default these are set to every 5 minutes. Consider changing these settings to a value greater than 10 minutes.
- You must use site management to force computers to use the task server if Notification Server and the task server are in the same site.
- To ensure that the task server is properly installed and configured, install the task service through the Symantec Management Console.

How task server uses the tickle mechanism

The tickle server is a component of Task Management. The tickle server component runs only on the Notification Server computer and is responsible for notifying task servers of pending tasks for their client computers. Tickle connection between Notification Server and task servers is also used for delivering new task server settings to task servers.

Task servers have the native ability to tickle their registered client computers. This tickle ability is separate from the tickle server component on the Notification Server computer.

The tickle server sends IP tickle packets to task servers when any of their registered client computers have a job or task to run. After the tickle packet is received, the task server immediately requests the task or the job information from Notification Server for its registered client computers. It also tickles its client computers. When the Client Task Agent receives the tickle packet, it requests the job or the task information from its registered task server. Only after the Client Task Agent receives the task information is the task executed. Status events for completed tasks are sent back to the registered task server upon completion.

If the tickle packets are blocked or otherwise cannot reach the destination, the Client Task Agent automatically checks back to its registered task server for any new job information. It performs this check every 30 minutes. This Task Request Interval is configurable in the Symantec Management Console. Task Server task and job information is not received through the Symantec Management Agent configuration policy. It is received directly by the Client Task Agent from its registered task server. If you force the Symantec Management Agent to update its configuration policy, it does not force the Client Task Agent to receive pending task information.

By default, the Tickle Server uses port 50123 for task servers and task servers use port 50124 to tickle Client Task Agents.

Note: Tickle mechanism does not function in Cloud-enabled Management (CEM) mode.

The following example assumes the Client Task Agent for ComputerA is registered with RemoteTaskServer1.

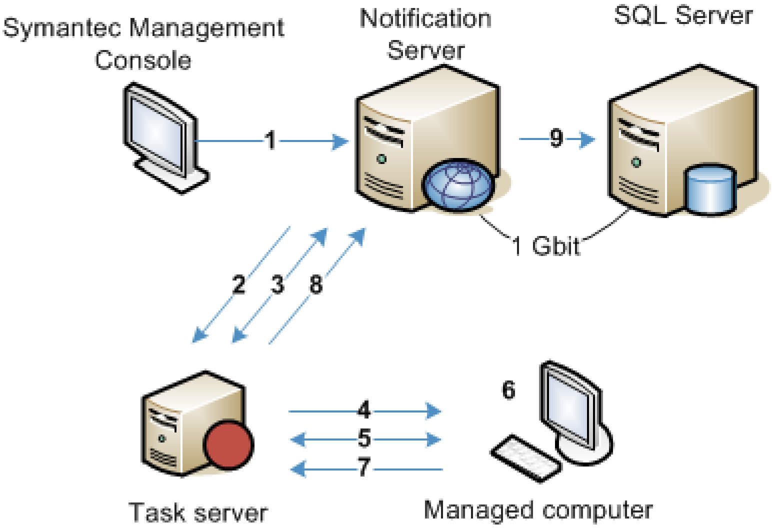
Table 3-3 Sequence for how the task server tickle works

Sequence	Description
One	A Notification Server administrator assigns a task to run immediately on ComputerA.
Two	The Tickle Server on the Notification Server computer sends a tickle packet to notify RemoteTaskServer1 of the pending task.
Three	RemoteTaskServer1 receives the tickle packet and immediately requests the job information from Notification Server.

Table 3-3 Sequence for how the task server tickle works *(continued)*

Sequence	Description
Four	RemoteTaskServer1 tickles ComputerA to notify it of the pending task.
Five	ComputerA receives the tickle packet and immediately requests the job information from its registered task server – RemoteTaskServer1.
Six	ComputerA receives the job information and executes the task.
Seven	Upon completion of the task, ComputerA sends a status event back to RemoteTaskServer1.
Eight	RemoteTaskServer1 caches the status event and immediately attempts to forward it back to Notification Server.
Nine	Notification Server receives the status event from RemoteTaskServer1 and records the information in the database.

Figure 3-1 Sequence for how task server tickle works



About the package service

Package servers are deployment mechanisms to efficiently move data into a site. They work with Notification Server as local file servers for managed computers at a site. Package servers do not require server-class hardware and software.

Package servers help you reduce network traffic by allowing a package to copy across the network only once per site. You can place a package server locally at a site to store and deliver packages. This architecture can help you manage sites with low-bandwidth connections to Notification Server.

See “About planning your site servers” on page 35.

When you enable a package on Notification Server, it is copied to all of the package servers that Notification Server knows about. Once the copy is successful, managed computers download the packages from the local package server instead of the remote Notification Server.

The number of package servers that you require is dependent on your network topology and bandwidth. It also depends on the size of your packages and frequency of the packages to be delivered.

You can stagger the deployment of packages to the package servers to reduce load. You can deploy a limited number of packages at a time to all package servers. You can also only deploy to select group of package servers at a time.

A constrained package server can operate only within the sites to which it is assigned. An unconstrained package server can get packages and other resources from anywhere in the system. The unconstrained package server collects any required resources from outside the site and makes them available to all of the constrained package servers. A site server can function as a package server only when there is at least one unconstrained package server that is assigned to it. There must be at least one unconstrained package server in a site with one or more constrained package servers.

About the network boot service

A network boot server's purpose is to provide PXE Boot services and boot packages for network segments. The most common purpose is for restoring a standard image for support or for rolling out new computers during initial provisioning. Typically, PXE protocol is controlled on a network. It may be limited to work within a subnet or other defined range based on IP helpers. If many systems must be reimaged simultaneously, you can place network boot servers within each network subnet and add more in a large subnet. In addition to providing PXE services, a network boot server is similar to a package server in that it hosts packages called boot images.

See “About planning your site servers” on page 35.

Each subnet must have access to a network boot server. However, routers normally block PXE broadcast packets.

You can use the following three methods to provide each subnet with access:

- Use “DHCP forced mode,” which is a DHCP setting that forwards client PXE requests to the closest network boot server. This method works even when the client computer is on a different subnet than the network boot server. DHCP determines the correct server by using subnet mask and ping tests.

- Use “IP Helpers,” which is a setting you can configure at each router that lets you forward PXE requests across subnets.
- Install a network boot server on each subnet. This method is not recommended because it creates unnecessary overhead.

A network boot server contains the following objects:

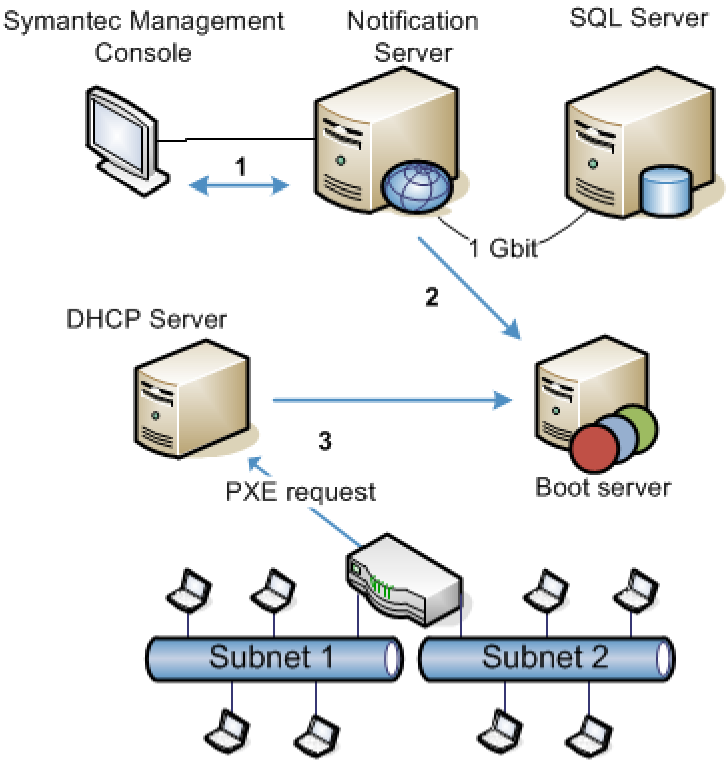
- PXE service
- Boot images
- The NSCap or Package Server share with the imaging executables if the executables are not a part of the Preboot image.
- The driver database

When new settings are applied to an existing boot image, an updated boot image is compiled locally at each network boot server. These changes are delivered with a policy and are dependent on the Symantec Management Agent update schedule.

Table 3-4 Sequence for network boot server configuration

Sequence	Description
One	Deployment Solution is installed on the Notification Server computer. The administrator configures and manages deployment jobs and tasks from the Symantec Management Console. Required device drivers should be imported from Symantec Management Platform and deployment administrator must make sure that **DriversDB** is up-to-date on all PXE servers. PreBoot environment should be rebuilt.
Two	The administrator enables and configures the network boot service.
Three	The DHCP server can route PXE requests from the client computers to the network boot servers that are on multiple subnets.

Figure 3-2 Sequence for network boot server configuration



Symantec Management Agent deployment planning

In some environments, computers are set up with a corporate software image or a standard base list of software. If you add the agent image to the computer image, you can save time and effort. The Symantec Management Agent can be preinstalled and placed in a directory with a “Run Once” operating system directive.

See “About tuning the Symantec Management Agent for performance” on page 86.

You can also use scripting mechanisms to install the agent. You can push the Symantec Management Agent from the Symantec Management Console if you do not want to add the agent to an image build.

Push requires less outside intervention than other methods of deploying the agent to computers already in service. With this method Notification Server contacts the client computer, and then the client computer requests the agent from Notification Server. The push method requires you to disable the file-sharing setting.

You can still deploy the agent with file-sharing enabled. The client computer still has the ability to initiate this request itself. For example, with email, either a script can be emailed or a Web link can be sent to pull the agent.

Ports and protocols for IT Management Suite

The following article lists the ports and protocols that are used by the components of IT Management Suite:

http://www.symantec.com/docs/DOC6770

Chapter 4

Hardware recommendations

This chapter includes the following topics:

Recommended IT Management Suite 8.5 hardware

To determine your hardware requirements, use the recommendations in this topic. The following are general hardware recommendations for most environments with IT Management Suite 8.5. Depending on your specific circumstances, the appropriate hardware may vary.

Virtual machine (VM) considerations

ITMS has “burst” activities surrounding schedules and corresponding data processing. A common failing in environments is for VM & Storage admins to pull away resources because the baselines may not indicate continuous need for resources. However, the resources should continue to be available to handle activity peaks as well.

Be cautious of “VM Environment” induced latency. Latency can be caused from things like insufficient memory, slow disk subsystem configurations, use or excessive use of snapshots, insufficient CPUs, and many factors that can affect the ability of the VMs to get the resources when they are needed

VM latency commonly occurs from oversubscription of resources. But, can also come from other factors such as vMotion and associated resource storms, miss-configuration, and even usage of snapshots on some storage systems which cause excessive writes due to MBR alignment problems between VMware and the storage provider when snapshots are in use

Hardware recommendations

Note: These recommendations are NOT minimum specifications. Implementing them should ensure reasonable Notification Server performance for inventory collection and UI response times.

Table 4-1 Hardware recommendations for Microsoft SQL Server

Component	1 - 1,000 endpoints	1,000 - 5,000	5,000 - 10,000	10,000 - 20,000	20,000 - 35,000 endpoints
CPU Cores (Speed)	4 (2.4 Ghz)	8+ (2.4 Ghz)	8+ (2.4 Ghz)	16+ (2.4 Ghz)	32+ (2.4 Ghz)
Disk Speed (in IOPS)	180 - C: OS 200 - D: SQL	180 - C: OS, SQL App 300 - D: SQL DB 300 - E: Logs 200 - F: TempDB	180 - C: OS, SQL App 400 - D: SQL DB 400 - E: Logs 300 - F: TempDB	180 - C: OS, SQL App 600 - D: SQL DB 600 - E: Logs 400 - F: TempDB	180 - C: OS, SQL App 1200 - D: SQL DB 600 - E: Logs 1200 - F: TempDB
OS + SQL (Capacity)	300 GB	300 GB	300 GB	300 GB	300 GB
DB (Capacity)	300 GB	300 GB	300 GB	300 GB	800 GB
Logs (Capacity)		100 GB	100 GB	100 GB	300 GB
Temp (Capacity)		100 GB	100 GB	100 GB	300 GB
RAM	12 GB	16+ GB	24+ GB	32+ GB	64+ GB
Cache	6 MB Level 2 or more				
Network	Dual Gigabit Load Balanced				

Table 4-2 Physical and virtual hardware recommendations for Notification Server

Component	1 - 1,000 endpoints	1,000 - 5,000	5,000 - 10,000	10,000 - 20,000	20,000 - 35,000 endpoints
CPU Cores (Speed)	8 (2.4 Ghz)	8 (2.4 Ghz)	8+ (2.4 Ghz)	16+ (2.4 Ghz)	32+ (2.4 Ghz)
Disk Speed (in IOPS)	300 - OS, SMP	400 - OS 200 - SMP	600 - OS 200 - SMP	600 - OS 200 - SMP 200 - package handling	600 - OS 500 - SMP 200 - package handling
OS + SMP (Capacity)	300 GB	300 GB	300 GB	300 GB	600 GB
Packages (Capacity)	600 GB	600 GB	600 GB	600 GB	1 TB
RAM	8 GB	16 GB	16 GB	16 GB (Parent: 24 GB)	32 GB
Cache	6 MB Level 2 or more				
Network	Dual Gigabit Load Balanced				

Note: Your Notification Server disk capacity requirements may increase depending on your specific strategy for storing Deployment disk images, Patch Management Bulletins, and your Software Library.

The services in Table 4-3,Table 4-4,Table 4-5 can be combined on one site server or deployed separately, depending on your environment. Often package and PXE services are installed on a single computer

Note: Site server is a computer running one or more of the task, package, or network boot server (PXE) services. The task, package, and PXE services can be combined on one site server or deployed separately, depending on your environment.

Site servers may use either a Windows desktop operating system or a Windows server operating system. Distributed and large environments may require multiple site servers to meet configuration management demands. Choosing a server or a desktop operating system depends on the concurrent sessions that site server needs. Windows desktop operating systems are limited to 10 or 20 concurrent TCP connections sessions but Windows server operating system does not have the same limitation. A site with fewer than 100 endpoints may only require 10 sessions; however, a Windows server may be required for larger remote sites.

Table 4-3 Physical and virtual hardware recommendations for Task Server

Component	10 - 100 endpoints	100 - 1,000 endpoints	1,000 - 5,000	5,000 - 15,000
Operating system*	Desktop operating system	Server operating system	Server operating system	Server operating system
CPU Cores	2	4	4	8
Disk Capacity	5 GB	5 GB	5 GB	5 GB
RAM	2GB	4 GB	4 GB	8 GB
Cache	6MB L2 or more			

* For more information about the supported operating systems, see the following knowledge base article:

http://www.symantec.com/docs/HOWTO9965

Table 4-4 Physical and virtual hardware recommendations for Package Server

Component	10 - 100 endpoints	100 - 1,000 endpoints	1,000 - 5,000	5,000 - 7,500
Operating system	Desktop operating system	Server operating system	Server operating system	Server operating system
CPU Cores	2	2	4	4
Disk Capacity*	100 GB - 250 GB	100 GB - 250 GB	100 GB - 250 GB	100 GB - 250 GB
RAM	2 GB	4 GB	4 - 6 GB	4 - 8 GB
Cache	6MB L2 or more			

* Note that the disk capacity requirements depend on the number and size of the software packages, deployment images, etc.

Table 4-5 Physical and virtual hardware recommendations for Network Boot Server (PXE)

Component	10 - 100 endpoints	100 - 1,000 endpoints	1,000 - 5,000	5,000 - 7,500
Operating system	Desktop operating system	Server operating system	Server operating system	Server operating system
CPU Cores	1	2	4	4

Table 4-5 Physical and virtual hardware recommendations for Network Boot Server (PXE) *(continued)*

Component	10 - 100 endpoints	100 - 1,000 endpoints	1,000 - 5,000	5,000 - 7,500
Disk Capacity	100 - 250 GB	100 - 250 GB	100 - 250 GB	100 - 250 GB
RAM	4 GB	4 GB	4 GB	8 GB

Recommended Internet gateway hardware

Symantec recommends having at least two Internet gateways to provide failover options, load balancing, and to maintain communication continuity. Each Internet gateway can serve multiple Notification Servers. This configuration is supported even if Notification Servers are organized in a hierarchy structure. Each Internet gateway supports 1- 60,000 endpoints and 15,000 concurrent connections.

See “About Cloud-enabled Management” on page 22.

Running Internet gateway on a virtual computer is not recommended. Running Internet gateway on virtual hardware can lower its scalability by up to 40%.

Table 4-6 Hardware recommendations for Internet gateway

Component	Requirement
Processors	Dual-core CPU
Disk Capacity	At least 40 GB
RAM	8 GB
Network adapters	Two 1Gbit network adapters

Recommended configuration for Notification Server with locally installed SQL database

For environments with up to 5,000 managed computers, a Notification Server with a locally installed SQL database might perform adequately. A Notification Server with SQL installed on the same server is referred to as an "on-box" SQL installation. Symantec recommends supporting no more than 5,000 managed computers with on-box SQL. Even with fewer than 5,000 managed computers, performance is unlikely to be as robust as with an off-box SQL configuration. Performance is most noticeable with console responsiveness and inventory collection.

See “About planning your SQL Server configuration” on page 30.

See “About hard drive configuration for SQL Server” on page 31.

Table 4-7 IT Management Suite 8.5 physical hardware recommendations for Notification Server with on-box SQL

Component	Evaluation (1 - 20 endpoints)	100 - 1,000 endpoints	1,000 - 5,000 endpoints	> 5000 endpoints
Processors	2 cores	8 cores	12 - 16 cores	Not recommended
Disk Capacity	80 GB	80 GB	200 GB	
RAM	8 GB	16 GB	20 GB+	

Recommended maximum computer count for IT Management Suite 8.5

The following information is based on IT Management Suite scalability testing in a 1x6x35,000 hierarchy configuration.

See “Recommended IT Management Suite 8.5 hardware” on page 45.

See “About planning your site servers” on page 35.

Table 4-8 Ranges of recommended component totals for IT Management Suite 8.5

Components	Range
Managed computers per Notification Server	1 - 35,000
Package servers per Notification Server	1 - 600
Task servers per Notification Server	1 - 600
Network Boot Servers per Notification Server	1 - 300
Managed computers per package server[1]	1 - 7,500
Managed computers per task server[2]	1 - 15,000
Managed computers per network boot server[3]	1 - 7,500
Concurrent PXE sessions per network boot server[3]	200
Concurrent console sessions per Notification Server	100 (75 managers + 25 asset managers)

Table 4-8 Ranges of recommended component totals for IT Management Suite 8.5 *(continued)*

Components	Range
CEM Agents per Internet Gateway	30,000 (15,000 concurrent)

[1] This number depends on package use and frequency. The appropriate number for a specific architecture should be determined using Microsoft Windows file transfer speeds, because package servers are basically file servers.

[2] If you plan to use tasks excessively, this number needs to be lower due to the number of tasks to process. In this case, the client computer node count is secondary.

[3] Deployment Solution has a dependency on task services. As a result, this client computer number should match the task server number. However, care should be taken to not initiate deployment jobs on more than 200 clients per task server at a time. This scenario can have multiple constraints:

- The disk speed of the task server hosting WinPE and the images.
- The number of available IP addresses in a given DHCP scope for newly discovered computers.
- The size of the image/s.

Supported operating systems for Notification Server and site servers

The latest version of the Symantec Management Platform requires Windows Server 2016, or Windows Server 2012 R2. However, the Symantec Management Platform can host middleware components on computers other than the Notification Server. These middleware components support several operating systems.

The official name for a middleware component is a "site service." Any computer that hosts a site service is known as a site server. Examples of site services are package service and task service. A site server can have one or more site services installed on it. For example, if you install the package server site service (the "package service") onto a computer, that computer becomes a package server.

Site servers can use either a Windows desktop operating system or a Windows server operating system. A site server with a package service installed can also use a Linux server operating system.

Distributed and large environments may require numerous site servers to meet configuration management demands. Notification Server makes sure that the site service is installed only on the computers that satisfy the minimum requirements. Your primary consideration is the number of concurrent sessions that you need when you choose between a server operating system and a desktop operating system. A Windows desktop is limited to 10 or 20 concurrent TCP connections and a server operating system does not have the same limitations. A site with less than 100 endpoints may only require 10 sessions. However, a Windows server may be required for larger remote sites.

For more information on Symantec IT Management Suite platform support, see http://www.symantec.com/docs/HOWTO9965.

See "SQL Server recommendations and third-party software requirements" on page 53.

Microsoft SQL Server Collations

The Symantec Management Platform supports the following Microsoft SQL Server Collations:

- Latin1_General_BIN
- Latin1_General_BIN2
- Latin1_General_CI_AI
- Latin1_General_CI_AS
- Latin1_General_CS_AI
- Latin1_General_CS_AS
- Latin1_General_CP1_CI_AS

IIS role services installed by the Symantec Installation Manager

Before you begin the installation of the IT Management Suite, you must install the Web server (IIS) role on the computer. If the required IIS role services are not installed, you are prompted to install them on the **Install Readiness Check** page from the Symantec Installation Manager (SIM). When you confirm the installation, the SIM can automatically install and configure these IIS role services on the server.

Note: Apart from the IIS role services that are installed with the Web server, you may also require to install a few additional IIS role services. These roles services are required to install the IT Management Suite. The SIM identifies such IIS roles services and prompts you to install them automatically through the **Install Readiness Check** page of the SIM installation wizard.

SQL Server recommendations and third-party software requirements

The IT Management Suite 8.5 requires an x64 version of SQL Server either installed on-box or off-box. The version of SQL Server that you need depends on the number of endpoints that you manage.

Table 4-9 IT Management Suite 8.5 SQL Server recommendations

1-1,000 endpoints	1,000 to 5,000 endpoints	5,000-10,000 endpoints	10,000-20,000 endpoints	20,000-35,000 endpoints
Microsoft SQL Server 2012 or higher. Although you can host SQL Server on box, Symantec recommends that you host SQL Server off box.	Microsoft SQL Server 2012 or higher. Although you can host SQL Server on box, Symantec recommends that you host SQL Server off box.	Microsoft SQL Server 20012 or higher. Symantec recommends that you host SQL server off box.	Microsoft SQL Server 2012 or higher. Symantec recommends that you host SQL server off box.	Microsoft SQL Server 2012 or higher. Symantec recommends that you host SQL server off box.

For more information, see the following knowledge base articles:

http://www.symantec.com/docs/HOWTO9965

http://www.symantec.com/docs/HOWTO10723

The IT Management Suite 8.5 solutions also require the following additional third-party software:

Table 4-10 IT Management Suite 8.5 required third-party software

Software	Purpose
Perl version 5.6 or later	Starting from 8.1, Patch Management Solution for Linux requires Perl to be installed on your Red Hat Linux, SUSE Linux, and CentOS Linux computers. All versions of Inventory Solution require Perl to be installed on your UNIX, Linux, and Mac computers. $PATH environment variable must have the correct reference to Perl location.
AJAX 1.0	Ajax is used to enable asynchronous calls to allow for a dynamic user interface. For example, loading menus on demand and rendering on the fly. Ajax is fundamental to many of the user interface control behaviors — menus, grids, trees, lists, component art controls, etc.
Microsoft Access 2010 OLEDB driver	Data Connector requires this driver to be able to communicate with Access (.mdb) and Excel (.xls) files. Install the 64-bit version of the driver.

Table 4-10 IT Management Suite 8.5 required third-party software *(continued)*

Software	Purpose
Microsoft Report Viewer 2008 Redistributable Package or later	The Microsoft Report Viewer 2008 Redistributable Package or later includes controls for viewing reports designed using Microsoft reporting technology.
Microsoft .NET Framework 4.5.1 or later	All components of ITMS depend on the Microsoft .NET Framework.
Server Manager roles and role services	Application Server role and IIS 6 Management Compatibility, ASP, and web server role services. **Note:** If the required IIS Role Services are not installed, you are prompted to install them on the **Install Readiness Check** page. See "IIS role services installed by the Symantec Installation Manager" on page 52.

Note: The IT Management Suite 8.5 solutions do not require Microsoft Network Monitor 3.4. However, this protocol analyzer can be useful for troubleshooting purposes because it allows you to capture, view, and analyze network traffic.

For more information about the platforms that are supported for the installation of Symantec Management Platform, the Client Management Suite, and the Server Management Suite components, refer to the following article:

http://www.symantec.com/docs/HOWTO9965

Chapter 5

Solution communications

This chapter includes the following topics:

How Deployment Solution tasks work

Deployment Solution lets you integrate standard deployment features with Symantec Management Platform. It helps reduce the cost of deploying and managing servers, desktops, and notebooks from a centralized location in your environment. The solution offers OS deployment, configuration, PC personality migration, and software deployment across hardware platforms and OS types.

How agent check-in intervals and basic inventory settings interact

A number of client-side and server-side settings interact to influence when for example, an application is deployed to a number of endpoints.This might explain why, after you added a set of computers to a policy, nothing seems to be happening.

Table 5-1 Sequence for agent-server communications

Sequence	Location	Description
One	Client	The basic inventory provides basic client information. For example, it provides agent version, sub-agent information, unique ID, etc.
Two	Server	The resource membership update adds the computer to one or more targets. This is based on the basic inventory and other inventory variables that may apply, such as conditional parameters, policies, and such.
Three	Server	The policy refresh schedule uses the membership tables to update policy tables. When a user saves a policy, it is immediately updated.
Four	Client	The agent configuration request runs and finds which policies apply.

How agent-based inventory communications work

Inventory Solution lets you see detailed reports about the hardware and software in your environment. You can target computers for policies and tasks based on this information. It includes predefined inventory policies. Some predefined inventory policies are enabled by default. However, you can modify them to meet your specific needs.

These policies include the following settings:

- What to inventory.
- When to run.
- Which computers to run on (targets); by default, this setting targets all computers with the Inventory Solution plug-in installed.
- Optional advanced settings.

Notification Server delivers the initial inventory task-based policy to the managed computer. The Inventory Solution plug-in runs its first inventory immediately. After the Inventory Solution plug-in has its policy settings, it continues to run the inventory task. It runs the task according to the settings and the schedule that are defined in the policy. If a policy setting is ever changed, then the task server pushes the new settings to the plug-in immediately. The Inventory Solution plug-in then immediately runs an inventory collection.

Inventory Solution runs independent of the Symantec Management Agent's configuration request. It uses tasks and task servers to perform its operations.

You can create your own custom schedules in the policy or you can use one of the following predefined schedules:

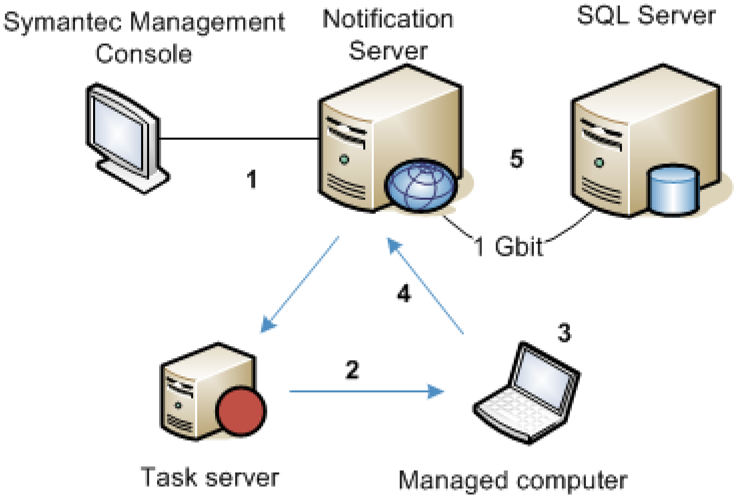
- Daily. This time is at 6:00 P.M. every day.
- Weekly. This time is at 6:00 P.M. every Monday.
- Monthly. This time is at 6:00 P.M. on the first Monday of each month.

When the Inventory Solution plug-in runs, it gathers hardware inventory, file scans, Microsoft add or remove programs and UNIX, Linux, and Mac software listings. The Inventory Solution plug-in immediately sends the data to Notification Server. The data is compiled as Notification Server Events (NSEs). Notification Server stores the NSEs in the Configuration Management Database. The data is then available for reporting from the Symantec Management Console.

Table 5-2 Sequence for Inventory communications

Sequence	Description
One	Predefined inventory policies are available for managed computers on Notification Server.
Two	After the initial Inventory plug-in deployment, inventory policies are delivered to managed computers by Notification Server Policy file.
Three	By default the Inventory plug-in runs ASAP. The Inventory plug-in then gathers the inventory according to its defined schedule.
Four	After inventory is gathered, by default it is immediately sent to the Notification Server computer.
Five	The Notification Server computer stores the inventory in the CMDB.

Figure 5-1 Sequence for Inventory communications



About configuring inventory policy and task settings for optimal resource usage

Inventory Solution lets you gather inventory data about computers, users, operating systems, and installed software applications in your environment.

Default inventory policy and task settings may overload your network. You can configure inventory policy and task settings to minimize impact on your environment.

Adhering to the following recommendations lets you tune the inventory performance to minimize the impact on your environment and network workload:

- Avoid over scheduling of inventory gathering activities.
  On the inventory policy page, you can choose to gather hardware and operating system, software, file properties, or server applications inventory, according to your needs. All of these types of inventory do not have to run at the same time.
  Symantec recommends that you use unique policies and schedules for different kinds of inventory.
  Note that if there are too many inventory tasks and policies running, it may increase the workload on Notification Server.
  Increasing the frequency of an inventory policy or task in an attempt to hit an "online window" causes redundant data to be sent to Notification Server. The workload on Notification Server increases as the duplicate data must still be processed and then discarded. Schedule inventory policies or tasks to occur only at the desired data refresh rate, so that the Symantec Management Agent can locally manage the inventory collection process.

- Use the type and method of gathering inventory that best suits your current needs.

  On the inventory policy page, you can choose and configure the type of inventory that you want to gather. You can also create a custom inventory policy to gather specific data. This lets you reduce network traffic and decrease the workload on Notification Server.

  See "Methods for gathering inventory" on page 61.

- Use policies instead of tasks for recurring activities.

  Symantec recommends to use policies, not tasks, for recurring inventory activities.

  Inventory policies have more options and allow more flexibility for running regular inventory. For example, you can schedule an inventory policy to apply to a specific group of users or computers, and the policy automatically runs on all new computers that you add to the target group.

- Review all inventory tasks before you turn them on.

  Inventory tasks have some options enabled by default. This can result in significant database growth. Symantec recommends that you review the task settings and disable the options that are not necessary for your specific purpose.

- Avoid over usage of the **Collect Full Inventory** policy and its associated inventory task.

  Symantec recommends that you run full inventory regularly to minimize the potential for inventory to get out of synchronization with the server. The default recommendation is to collect full inventory once a week, but you can configure the policy settings according to your needs.

  Running full inventory scan too frequently may increase the workload on Notification Server. To reduce the load on your environment, Symantec recommends to establish longer intervals between gathering full inventory, and run delta inventory during those intervals.

  Delta inventory reports only the data that has changed since the last full inventory scan. Running delta inventory helps reduce the network load.

  The process of collecting delta inventory runs as follows:

Step 1	When you run a full inventory policy, it collects the information about data classes, records hash for each data class in delta.cache, and sends this information to the Notification Server. You can view the inventory data in the Resource Manager or in reports.
Step 2	The following delta inventory calculates a new hash for every data class, compares it to the current information in delta.cache, updates delta.cache, and then sends the changed information to the Notification Server.
Step 3	Each new delta inventory updates the information in delta.cache according to the changes it discovers.
Step 4	When you collect full inventory, it completely rewrites the existing delta.cache.

The data in the Configuration Management Database (CMDB) can get outdated if you make significant changes to the environment, so that the delta.cache on the client computer is not consistent with the information in the database anymore. This may happen when the computers are merged, deleted and then added to the Notification Server again, redirected from one Notification Server to another, or when a new database is used.

In this case, Symantec recommends that you run full inventory after you make the changes.

Also, the inventory data files can occasionally get corrupted or not processed by the Notification Server. In this case, to synchronize the information again, you need to run a full inventory scan.

- Configure **File Properties Scan Settings**.

  When you configure an inventory policy or task settings, in the **Advanced Options** dialog box, review the **Files Properties Scan Settings** on the following tabs:

Drives	By default, all local drives are scanned. You can exclude the drives that you don't need to scan.
Folders	You can exclude the directories that you don't need to scan.
Files	In the **Include file rules** dialog box, Symantec recommends to check **Report size/file count only** if you do not need to collect full information about files. This lets you decrease the network load.

- Only enable the **Access network file systems (UNIX/Linux/Mac)** option if necessary.

  Enabling this option in the **Advanced Options** dialog box may result in getting redundant inventory data reports.

  Scanning remote volumes is disabled by default to prevent numerous computers from reporting redundant inventory data.

- Configure the inventory scan throttling option.

  Throttling lets you randomize the beginning of the inventory scan, to decrease the network load.

  Symantec recommends that you use throttling in larger environments. For example, when you have multiple virtual machines on a single physical host computer, running an inventory scan can result in significant performance issues. Throttling lets you randomize the time when the inventory scan starts, which also effectively randomizes the time when the Notification Server receives the inventory scan results. The network and Notification Server can process inventory over time.

  For example, you can set the scan throttle period to 24 hours. At the scheduled time, the scan process starts, but then it immediately goes to sleep, and wakes up at some random time within the specified time period (in this example, 24 hours) to complete the scan.

  To enable throttling, on an inventory policy or task page, click **Advanced**, and then, in the **Advanced Options** dialog box on the **Run Options** tab, check **Throttle inventory scan evenly over a period of: *X* hours**.

Note that when a policy is executed with this setting, the task will be shown as running in the Task History, even when sleeping for the random amount of time.

Note: This feature is currently available for Windows only.

- Configure the **System resource usage** option.

  This option only affects the file scan process, and does not affect the collection of hardware, operating system, and **Add/Remove Programs** data.

  The **System resource usage** option lets you define the inventory process priority and thus modify the usage of the processor and disk on the client computer during an inventory scan. To determine its value, consider how fast you want the inventory to be gathered and how the inventory process affects performance of the client computer.

  To configure this option, on an inventory policy or task page, click **Advanced**, and then, in the **Advanced Options** dialog box, on the **Run Options** tab, specify the **System resource usage** value according to your needs.

  On the Windows platform, if you decrease the priority, the process of gathering inventory requires less resources on the client computer but the inventory scan takes longer. If you increase the priority, the inventory scan finishes faster but also consumes more resources.

  For UNIX, Linux, and Mac computers, the **System resource usage** value defines the priority of the inventory process, but does not define the percentage of resource usage. UNIX, Linux, and Mac computers dedicate more CPU cycles for high priority processes and less CPU cycles for low priority processes. If the computer is in an idle state and runs only the inventory scan, then low priority process may take the available resources.

  CPU usage reduces as soon as another process with a higher priority begins to run.

Note: On the Windows platform, this option is only applicable to file scans. On UNIX, Linux, and Mac platforms, this option is applicable to the entire inventory scan process.

Methods for gathering inventory

You can use different methods for gathering different types of inventory data. Each method has special features and requirements.

Table 5-3 Methods for gathering inventory

Method	Description	Features and requirements
Basic inventory	The basic inventory is gathered automatically when the Symantec Management Agent is installed on managed computers. This feature is a core function of the Symantec Management Platform and does not require any additional inventory components. Basic inventory data includes computer name, domain, installed operating system, MAC and IP address, primary user account, etc. This information is updated on a regular basis as long as the Symantec Management Agent is running on the computer. For more information, see the topics about the Symantec Management Agent and recommended Symantec Management Agent data update intervals in the *IT Management Suite Administration Guide*.	The features are as follows: ■ Inventory data is automatically collected when the Symantec Management Agent is installed on the client computer. No other components or steps are needed. ■ Inventory data is updated at regular intervals. ■ You can use this method on different platforms. ■ You can use this method for gathering inventory data on managed Windows computers in the Cloud-enabled Management environment. The requirements are as follows: ■ Target computers must be managed using the Symantec Management Agent. **Note:** Basic inventory data is limited in scope.

Table 5-3 Methods for gathering inventory *(continued)*

Method	Description	Features and requirements
Standard inventory on managed computers	Inventory Plug-in works with the Symantec Management Agent and uses scheduled policies to gather standard inventory data that is more detailed than basic inventory. By default, standard inventory data is gathered through more than 100 predefined data classes. Standard inventory data includes the following details about managed computers: ▪ Hardware components, operating system, and user accounts and groups. ▪ Software and virtual software layers. ▪ File properties. More detailed information about the software, such as manufacturer, version, size, etc. When Inventory Plug-in is installed on managed computers, you can manage all the inventory policies from the Symantec Management Console. You can schedule inventory policies to run at regular intervals according to your needs, so that gathering inventory does not affect your network performance. You can use Inventory Plug-in on Windows, Linux, UNIX, and Mac platforms.	

Table 5-3 Methods for gathering inventory *(continued)*

Method	Description	Features and requirements
		The features are as follows: ■ You can gather a broad range of inventory data. ■ Inventory data is automatically collected and updated using scheduled policies and tasks. ■ You can gather the most important inventory data frequently during a day. You can also gather software inventory on Windows computers in real time. See "About predefined inventory policies" on page 80. ■ You can configure policies to report only the data that has changed since the last full inventory scan (delta inventory). ■ Inventory Solution automatically detects the computers with data discrepancies and maintains the inventory data consistency without overloading your environment. ■ This method can be used on multiple platforms. ■ You can gather standard inventory on managed Windows and Mac computers in the Cloud-enabled Management environment. The requirements are as follows: ■ Target computers must be managed using the Symantec Management Agent. **Note:** Maintaining current inventory data can be difficult on the computers that are not regularly connected to the network. ■ Target computers must have Inventory Plug-in installed. **Note:** The scope of inventory information that is collected depends on your account

Table 5-3 Methods for gathering inventory *(continued)*

Method	Description	Features and requirements
		permissions.
Standalone inventory	To gather standalone inventory, you must create stand-alone packages on the Symantec Management Console. Then you distribute the packages using email, network shares, login scripts, etc., and run the packages on your target computers. The standalone inventory method lets you gather standard inventory data on the computers that are not managed through the Symantec Management Agent, do not have Inventory Plug-in installed, and are not connected to Notification Server You can gather detailed information about hardware components, operating system, local users and groups, software, and virtual software layers. You cannot use this method in the Cloud-enabled Management environment.	The features are as follows: ▪ You can gather a broad range of inventory data. ▪ Only Windows-based computers are supported. The requirements are as follows: ▪ External delivery of inventory package is required. ▪ If target computers are not connected to Notification Server, the data must be posted manually. **Note:** The inventory data is not centrally managed, and may not be current.

Table 5-3 Methods for gathering inventory *(continued)*

Method	Description	Features and requirements
Custom inventory	To gather custom inventory, you must install Inventory Plug-in on your managed computers. This method lets you gather additional data beyond the predefined data classes in Inventory Solution. You can create the custom inventory data classes that may be unique to your environment. You can then run the custom inventory scripts that collect the custom inventory data classes.	The features are as follows: ■ You can add the data classes that are unique to your environment, and are not included by default. ■ You can use a sample script task to create or configure a custom inventory script task. ■ This method can be used on different platforms. ■ You can use this method for gathering inventory data on managed Windows computers in the Cloud-enabled Management environment. The requirements are as follows: ■ Target computers must be managed using the Symantec Management Agent. ■ Target Unix, Linux and Mac computers must have Inventory Plug-in installed. ■ You must create custom inventory data classes, and include the data classes in your custom scripts. ■ You must create and run the custom inventory scripts that collect your custom inventory data classes.

Table 5-3 Methods for gathering inventory *(continued)*

Method	Description	Features and requirements
Software-based usage tracking and application metering	To perform the software-based usage tracking and application metering, you must install Inventory Plug-in and Application Metering Plug-in on your managed computers. You can gather the data about application usage and the summary data of monitored applications. You can perform the following tasks on your managed computers: ■ Track usage of the managed Mac software at the software product and component level. Track usage of the managed Windows software at the software product, component, and file level. This task is the primary method to use for the majority of software products. ■ (Windows only) Meter the use and control the availability of applications by running predefined or custom application metering policies. Symantec recommends that you use this task only if you need to meter start, stop, and denial events for applications at the file level. ■ (Windows only) Deny multiple applications from running by configuring the predefined **Blacklisted Applications** policy or running custom application metering policies.	The features are as follows: ■ On Windows computers, you can control the availability of applications. You can deny applications from running. You can also configure deny events to be sent to Notification Server when a user tries to run a denied application. ■ On Windows and Mac computers, the usage tracking option lets you track software usage at the product level and lets you know how often a software is used, not only if it is installed. This feature can help you manage your software licenses. ■ You can use this method for gathering inventory data on managed Windows and Mac computers in the Cloud-enabled Management environment. The requirements are as follows: ■ Target computers must be managed using the Symantec Management Agent. ■ Target computers must have Inventory Plug-in and Application Metering Plug-in installed. ■ Only Windows and Mac client computers are supported. **Note:** This method is not supported on Windows and Mac servers.

Table 5-3 Methods for gathering inventory *(continued)*

Method	Description	Features and requirements
Baseline inventory	To gather baseline inventory, you must install Inventory Plug-in on your managed computers. This method lets you gather the data about files and registry settings on computers. You can generate a baseline that identifies the files or registry settings of a computer. You can later run the compliance scans on the managed computers to compare their current files or registry keys with those in the baseline. The differences between the baseline scan and compliance scan are reported to the CMDB.	The features are as follows: ■ You can track the files and registries that deviate from the corporate standards. ■ You can verify the accuracy of rollouts and upgrades. ■ System administrators or the help desk can get automatic notifications when a computer is non-compliant. ■ You can view a compliance level summary of the computer and reports of the changes in files. The requirements are as follows: ■ Target computers must be managed using the Symantec Management Agent. ■ Only Windows-based computers are supported. **Note:** You cannot use this method in the Cloud-enabled Management environment.

Table 5-3 Methods for gathering inventory *(continued)*

Method	Description	Features and requirements
Inventory for Network Devices	Inventory for Network Devices gathers inventory data from the discovered devices in your network. This inventory is gathered from the devices that are not managed through Symantec Management Agent. Because a management agent is not required, this inventory is considered an agentless inventory. You can gather inventory on the following types of devices: ▪ Cluster ▪ Computer ▪ Computer: virtual machine ▪ Infrastructure device ▪ IP phone ▪ KVM device ▪ Network-attached storage ▪ Network backup device ▪ Network printer ▪ Physical rack ▪ Physical enclosure ▪ Physical bay	The features are as follows: ▪ Agentless inventory gathers inventory on the devices that are already discovered and exist as resources in the Configuration Management Database (CMDB). The requirements are as follows: ▪ Before you gather inventory from network devices, you must collect the data about the SNMP-enabled devices on your network. ▪ Before you gather inventory from network devices, make sure that the connection profile of the **Network Discovery** task has the SNMP turned on.

About package delivery in hierarchy

The process of package delivery in a hierarchy consists of several stages. The principal factors that can influence the process are the package size and the bandwidth.

The time that each stage needs for completion also depends on the settings that you specify. The table below describes the process of package delivery for the default settings.

Table 5-4 Process for package delivery in hierarchy

Stage	Process description	Estimated time
1	You create a package on parent Notification Server.	The time needed to create a package depends on the size of the package.

Table 5-4 Process for package delivery in hierarchy *(continued)*

Stage	Process description	Estimated time
2	Parent package server that is assigned to parent Notification Server requests policies.	The process may take up to 75 minutes in case of the default replication settings (1 hour policy request timeout plus 15 minutes for delta membership update schedule).
3	Parent package server downloads the package from a local parent Notification Server directory, or from an alternative network resource.	The time needed to download the package depends on the package size and bandwidth.
4	Next replication (complete or differential) from parent Notification Server to child Notification Server occurs. Package delivery policy and all the information about the package is replicated.	The replication may take up to 24 hours in case of the default replication settings, plus the amount of time needed to replicate data. If you create the package after the start of replication, this package will be replicated only at the next day replication.
5	Child package server assigned to child Notification Server requests policies.	The process may take up to 75 minutes in case of the default replication settings (one hour policy request timeout plus 15 minutes for delta membership update schedule).
6	Child package server requests the package location from child Notification Server. The child Notification Server redirects the child package server to the parent Notification Server, which then redirects it to the parent package server.	The package location request and server redirection happen almost instantly.

Table 5-4 Process for package delivery in hierarchy *(continued)*

Stage	Process description	Estimated time
7	Child package server downloads the package from the parent package server.	The time needed for download depends on the package size and bandwidth.
8	Child package server sends its codebases (the data about the location of the package) to child Notification Server. This information is used for reference by other package servers that request the package location. Unless all the previous steps are completed, the child package server gets an empty list of the package locations and retries downloading the package.	If the child package server fails to download a package, it repeats the attempt every 3*2N minutes until it reaches the 24-hour limit. After that, it repeats the attempt every 24 hours. The server stops retrying to download the package if the package is deleted or no longer applicable. **Note:** To save time, you can create a standalone replication rule that runs more frequently on the parent package server, and replicates only package objects and their associations (program and command-line objects).

How Patch Management Solution data communications work

Patch Management Solution takes inventory of managed computers to determine the operating system and software updates (patches) they require. The solution then downloads the required patches and provides wizards to help you deploy patches. The solution enables you to set up a patch update schedule to ensure that managed computers are kept up-to-date with the latest vendor security updates. Managed computers are then protected on an on-going basis.

You can schedule Patch Management Solution to automatically download critical security bulletins into the CMDB. Symantec recommends setting this schedule to daily for Windows computers and weekly for Linux computers. This schedule does not download the patch installation files, only the information about them in the security bulletins. This download is called the software updates catalog. The first software updates catalog import on a new platform can take several hours. However, subsequent imports typically take less than an hour because each import only performs delta downloads of often only a few MBs. If you choose to enable multiple languages, then the number of security bulletins to download, the size of downloads, and the time to download increases. You can customize software updates catalog updates by creating exclusions for the software that you do not want to patch. You can create custom schedules for the download.

By default, every four hours the Software Update Plug-in contacts Notification Server to check for patches. If new security bulletins are added to the CMDB by the software updates catalog, the Software Update Plug-in checks to see if they are applicable. It also checks if the updates have already been installed. It sends the results of the check to the Notification Server computer. The data is available for compliance reporting.

After the software updates catalog import has completed, you can select which security bulletins you want to stage on Notification Server. This staging processes triggers a download of the patch installation files to a folder on the Notification Server computer.

After the download of the patches has finished, you can create and enable your patch distribution policy. If you use multiple package servers, your site management settings for package distribution determine how the patch installation files get distributed to the package servers.

The policy is not applied until the Symantec Management Agent has checked in. By default, every hour the Symantec Management Agent contacts the Notification Server computer and requests its configuration updates. However, your schedule may be different.

The Notification Server computer sends the patch distribution policy to the Symantec Management Agent. The Notification Server computer advertises the location of the package server to the Symantec Management Agent. The Symantec Management Agent connects to the package server and downloads the patches.

After the patches are downloaded, the installation waits for the next scheduled maintenance window to run. It waits unless you set it to ignore the maintenance windows for zero-day exploits.

It then does the following:

- Verifies that patches have been downloaded.
- Installs the patches and restarts the computer.
  You can configure restart settings so that servers do not restart immediately after patching updates. A no restart window may be given to client computers so that users can defer the restarts.
- Runs a vulnerability analysis.
  If a restart has not occurred, the computer may still appear in reports as vulnerable.

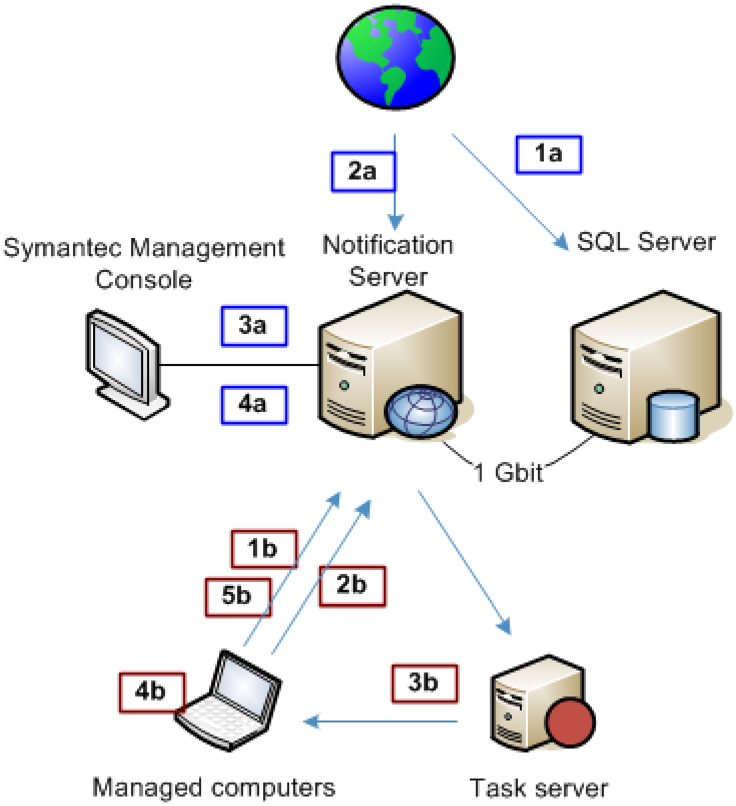
After the patching process completes, the Software Update Plug-in sends the updated vulnerability analysis to Notification Server and stores it in the CMDB. You can use the compliance reports to view vulnerability information from the Symantec Management Console.

The patching process has multiple dependencies, so order of operations is important. The Software Update Plug-in is used to determine vulnerability. The Symantec Management Agent performs the software update. They each may have a different update schedule. The larger schedule defines the window for patches to be delivered to managed computers. The maintenance window defines when the patches are installed. Compliance reports do not show success until after these steps are completed.

Table 5-5 Sequence for patch communications

Sequence	Description
One (a)	Import runs automatically on Notification Server and pulls security bulletins into the CMDB.
Two (a)	You select the patches from the security bulletin and they are staged to a local folder on the Notification Server computer.
Three (a)	You create a patch delivery policy and include the patches that were downloaded.
Four (a)	After the agents have completed, you run a compliance report to check the patch status.
One (b)	Patch plug-in checks in every four hours by default. It uses the latest patch management import data and runs a vulnerability scan. The scan is dependent on patch management import being complete.
Two (b)	The Symantec Management Agent checks in and receives the latest Patch policies and the location of the patches.
Three (b)	The Symantec Management Agent downloads the patch packages from the Notification Server computer or its assigned packaged server.
Four (b)	During the next maintenance window, the Symantec Management Agent installs the patches. After installation, the computer restart settings are run.
Five (b)	After the package is installed, a vulnerability analysis is run again and the information is sent to the Notification Server computer.

Figure 5-2 Sequence for patch communications



How asset management data communications work

Asset Management Suite provides a management console, a database environment, and a suite of solutions that let you track assets and asset-related information.

The suite includes Asset Management Solution and CMDB Solution. It specializes in tracking IT-related assets, such as computers and software. You can also use it to track other types of assets, such as office equipment or vehicles.

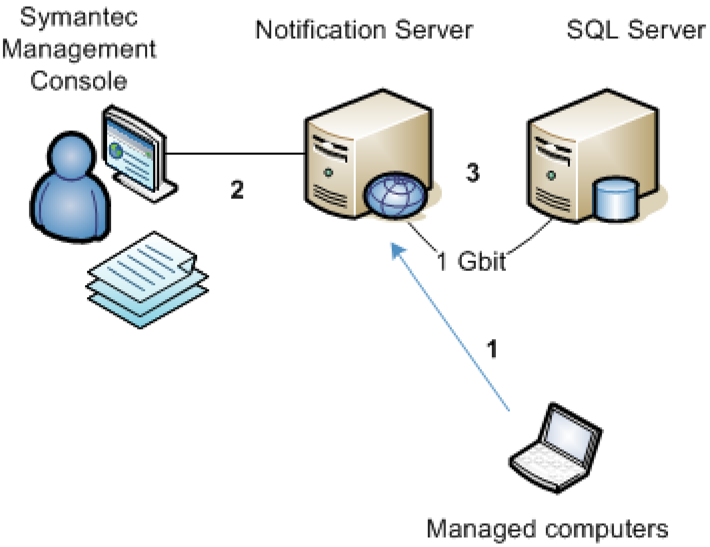
Table 5-6 Sequence for asset management communications

Sequence	Description
One	Asset Management Solution relies on Inventory Solution to gather and deliver data about managed computers.

Table 5-6 Sequence for asset management communications *(continued)*

Sequence	Description
Two	Administrator adds non-managed assets using the Symantec Management Console.
Three	Data that is stored in the CMDB is available for reporting and administrator can use reports to create management policies.

Figure 5-3 Sequence for asset management communications



Choosing a software delivery method

You can deliver software to one or more managed computers by creating and running a Software Management task or policy. The method that you use to create the task or policy depends on your delivery requirements.

If you need to quickly deliver a single software resource, you can use the task-based Quick Delivery method to specify the software to deliver, the action to perform, and the computers to deliver to. Because of its simplicity, Quick Delivery is an ideal way for non-administrators, such as help desk personnel, to deliver software safely and accurately.

You also use the task-based Package Delivery, if you need to deliver a package that is not associated with a software resource.

If you need to perform an advanced software delivery, you use an intelligent policy-based Managed Software Delivery method. This delivery method supports recurring schedules, software dependencies, software replacement, sequencing, and other complicated delivery scenarios.

Table 5-7 Methods for delivering software

Your requirement	Delivery method	Description
Perform a quick delivery of a single software resource.	Quick Delivery	You can use the task-based Quick Delivery method to specify the software to deliver, the action to perform, and the computers to deliver to. Quick Delivery uses the default task settings, which you can change when necessary. Because of its simplicity, Quick Delivery is an ideal way for non-administrators, such as help desk personnel, to deliver software safely and accurately. The software that you deliver in this way must be defined as a deliverable software resource in the Software Catalog.
Perform one or more of the following advanced delivery actions: ■ Deliver on a recurring schedule. ■ Install to a known state and ensure that the state is maintained. ■ Install software with the other software that it depends on. ■ Install a software resource that replaces other software. ■ Sequentially install multiple software and tasks. ■ Run any client task at any stage of the delivery. A client task is one that is defined in Notification Server and is intended to run on a client computer.	Managed Software Delivery	Managed Software Delivery is a policy-based delivery method that lets you fulfill advanced delivery requirements. A single Managed Software Delivery policy can perform multiple delivery actions. The software that you deliver in this way must be defined as a deliverable software resource in the Software Catalog. Managed Software Delivery leverages the software resource information and the logic that is in the Software Catalog. For example, Managed Software Delivery uses the software resource's dependencies, package, and detection rule.

Table 5-7 Methods for delivering software *(continued)*

Your requirement	Delivery method	Description
Deliver software in response to a direct request from a user.	Software Portal	(Windows and Mac only) With the Software Portal, users can request software and responds to those requests. If the user is pre-approved to install the software, the installation occurs without the administrator's involvement. Otherwise, the Software portal administrator or the Software portal manager needs to approve the requests. If the software is not in the Software catalog, the Software portal administrator can add and publish it on the portal, or deliver it directly to the user who requested the software.
Deliver a package that is not associated with a software resource.	Package Delivery	Package Delivery is a task-based delivery method. It lets you deliver any package regardless of whether it is associated with a software resource.

Chapter 6

Performance tuning and optimization recommendations

This chapter includes the following topics:

About determining if you require performance tuning

If you have an existing system, you may experience some symptoms that indicate you need performance tuning. You can also use performance tuning to proactively prevent these symptoms from occurring.

Some common indicators for performance tuning include the following:

- Random server errors
- Server timeouts

- Query timeouts
- Slow operations
- Queues filling up
- Caching warnings in the log
- Excessive deadlock retries in the log
- Key performance counters (Disk, Wait Stats)

Other symptoms may not be as obvious. For example the following: IIS Server Busy requests performance indicators, and disk latency issues may require more detailed reviews. In some cases, it may appear that the server is only asleep. For example, you can have heavy IIS communications that result in rejections. For example, no CPU, no disk, no SQL, and low Network.

See “Symantec Management Platform performance factors” on page 79.

Symantec Management Platform performance factors

Many factors influence the performance of your infrastructure.

The throughput of the SQL Server is a primary consideration for Symantec Management Platform performance. The configuration of SQL server and its hardware will influence overall performance. Most of the decisions you make that influence performance are related to architectural choices. For example, SQL Server will perform better if it is installed on a separate server from the Notification Server. This is referred to as installing SQL "off box." It offloads the work of data processing and frees resources for Notification Server processing. Another decision that influences SQL performance is disk IO.

The following are some of the common items that influence performance:

See “About tuning Notification Server Event processing for performance” on page 79.

See “About tuning the Symantec Management Agent for performance” on page 86.

See “About improving Symantec Management Console performance” on page 88.

About tuning Notification Server Event processing for performance

A notification sever event (NSE) is the standard mechanism by which Notification Server receives data. NSE processing directly influences performance on the Notification Server computer. The most direct method to influence the processing of NSEs is to adjust the volume and the frequency of your inventory gathering settings.

The following schedules influence the processing of NSEs:

- **Collect full inventory**

  Full inventory lets you gather data about managed computers. It includes data about hardware, operating system, installed software, and file properties. This data is sent to Notification Server in the NSE format. Full inventory can be resource-intensive . The default schedule runs full inventory once per month. Best practice is to collect full inventory once a month during non-production hours. We do not recommend that you run full inventory more often than once a week, even in small environments.

  Custom inventory can be run more frequently and more efficiently than full inventory. Custom inventory lets you collect very specific data points.

  See "About predefined inventory policies" on page 80.

- **Collect delta inventory**

  Delta inventory and Full inventory have similar resource consumption on managed computers. A delta inventory contains all the information that was added, removed, or changed since the previous inventory. The delta inventory file is smaller than the complete inventory file. Collect delta inventory can be run daily or weekly. You can improve the Symantec Management Console's UI performance if collect delta inventory is run during non-production hours. We recommend that you run delta inventory weekly rather than every day for environments with more than 10,000 clients per Notification Server. Environments with less than 10,000 clients can consider a daily delta inventory schedule.

  Delta inventory cannot track removed software. Only full inventory tracks removed software.

  See "About predefined inventory policies" on page 80.

- **Resource membership updates**.

  The resource membership update schedules determine how accurate and current your resource filters, organizational groups, and resource targets are. Notification Server has three resource membership update schedules:the complete update schedule, the delta updates schedule, and the policy update schedule. The more frequently resource membership updates run, the less latency there is on updates or remediation. However, when resource membership updates run, Notification Server must read and analyze the data in the CMDB. When Notification Server runs resource membership updates, computing resources are consumed. An example of how the resource membership update schedule can influence your day-to-day use is with assigning software from the Software Portal . Users that request software from the Software Portal must wait until after the delta resource memberships update completes.

  See "Scheduling resource membership updates" on page 84.

See "Symantec Management Platform performance factors" on page 79.

About predefined inventory policies

You can use predefined inventory policies to quickly start gathering inventory data. You can configure predefined policies to meet your needs. If you want to configure a predefined policy, Symantec recommends that you clone it, and then configure the copy.

To use inventory policies, you must install Inventory Plug-in on target computers.

In addition to gathering inventory data, all inventory policies and tasks send data recency information to Notification Server to ensure that the inventory data is current. Data recency information helps Inventory Solution automatically detect the computers with data discrepancies and maintain the inventory data consistency without overloading your environment.

Table 6-1 Predefined inventory policies

Policy	Turned on by default?	Default schedule	Default target	Notes
Collect Full Inventory	Yes	Weekly, every Monday at 18:00 (6:00 P.M.)	All computers with Inventory Plug-in installed	This policy collects a full inventory. By default, it collects hardware and operating system, software, and file properties inventory data. Symantec recommends that you collect full inventory weekly, but you can configure the policy settings according to your needs. You must install Inventory Plug-in on target computers before you can use this policy.
Collect Delta Hardware Inventory	No	Monthly, every first Monday at 18:00 (6:00 P.M.)	All computers with Inventory Plug-in installed	This policy reports only the data that has changed since the last full inventory scan.
Collect Delta Software Inventory	No	Weekly, every Monday at 18:00 (6:00 P.M.)	All computers with Inventory Plug-in installed	This policy reports only the data that has changed since the last full inventory scan.

Table 6-1 Predefined inventory policies *(continued)*

Policy	Turned on by default?	Default schedule	Default target	Notes
Collect Time-Critical Inventory	No	Frequently during a day	All computers with Inventory Plug-in installed	

Table 6-1 Predefined inventory policies *(continued)*

Policy	Turned on by default?	Default schedule	Default target	Notes
				This policy collects the most important hardware and software data classes on client computers frequently during a day with repeat interval in hours. The policy excludes the data classes that constantly change, such as TCP and UDP ports. The **Real-Time Inventory** feature of the policy lets you gather software inventory on Windows client computers in real time to validate the current software state. The **Real-Time Inventory** feature does the following: ■ Monitors the software state on target Windows client computers. ■ Invokes the software inventory scan within 10 minutes as soon as software is installed or removed. ■ If the software state changes, sends delta inventory and data recency information to Notification Server. ■ If no changes are found, sends data recency information to Notification Server. As all inventory policies, the **Collect Time-Critical Inventory** policy is configured to run as soon as possible (ASAP) for the first time, apart from the configured schedule. Additionally, the turned on **Collect Time-Critical Inventory** policy runs ASAP if the current policy differs from the previously processed policy, and the interval between the policies is more than 30 minutes. If client computer receives different **Collect Time-Critical Inventory** policies, the Inventory Plug-in uses the settings of the first processed policy, and ignores other policies. If you need to gather the inventory on computers in real time and perform immediate hardware and software state analysis, you can also use Time Critical Management feature. For more information, see the topic about Time Critical

Table 6-1 Predefined inventory policies *(continued)*

Policy	Turned on by default?	Default schedule	Default target	Notes
				Management.
Collect Full Server Inventory (Inventory Pack for Servers required)	Yes	Weekly, every Monday at 18:00 (6:00 P.M.)	All computers with Inventory Pack for Servers Plug-in installed	This policy only exists if the Inventory Pack for Servers product is installed. Even though this policy is turned on by default, you must install Inventory Pack for Servers Plug-in on target computers before inventory data is gathered.
Collect Delta Server Inventory (Inventory Pack for Servers required)	No	Weekly, every Monday at 18:00 (6:00 P.M.)	All computers with Inventory Pack for Servers Plug-in installed	By default, this policy collects only the server applications inventory data that has changed since the last full server inventory.

Scheduling resource membership updates

You can keep all of your resource filters, organizational groups, and resource targets up to date by configuring the appropriate filter update schedules. These schedules let you update the filters, organizational groups, and targets that you need at suitable intervals. These schedules help you manage the processing load that is imposed on Notification Server.

Predefined resource membership update schedules are supplied with the Symantec Management Platform. These schedules are suitable for most purposes and you should not need to change them. However, as the requirements of your organization change, you can make the necessary changes.

Table 6-2 Resource membership update schedules

Schedule	Description
Delta Update schedule	Updates the membership of the following: ■ Filters that have had membership changes since the last update. ■ All dynamic organizational groups. ■ All invalid targets. A target may be invalidated by the following events: ■ Its definition is saved. ■ A filter that it uses has membership changes. ■ An organizational group that it uses has membership changes. ■ The security that is applied to an organizational group that it uses changes. By default, this schedule runs every five minutes.
Complete Update schedule	Completely re-creates the membership of all filters, organizational groups, and targets, regardless of inventory status or any changes to policies. The complete update may impose a significant load on Notification Server and should be scheduled accordingly. By default, this schedule once a day.
Policy Update schedule	Updates the membership of filters that a policy uses, if the policy has changed since the last update. This schedule ensures that when you update or create a policy, all the filters that are included in the new policy targets or modified policy targets are updated automatically. By default, this schedule runs every five minutes.

To configure the resource membership update schedules

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Resource Membership Update**.
2. On the Resource Membership Update page, configure the update schedules that you want to use.
3. If you want to run an update schedule immediately, in the appropriate panel, click **Run**.

   For example, you can ensure that all the changes to your filters take effect immediately, rather than waiting until the scheduled update.
4. Click **OK**.

About tuning the Symantec Management Agent for performance

The Symantec Management Agent has three general settings that can affect your Notification Server computer’s performance and network bandwidth usage. You can access these settings in the **Symantec Management Console**, in the **Settings > Agents/Plug-in Settings > Targeted Agents Settings** page.

See “Symantec Management Platform performance factors” on page 79.

The agent has the following general settings:

- **Download new configuration**.

  This setting is the interval at which the Symantec Management Agent requests new policy information from Notification Server. Modifications to the setting influence your Notification Server computer's performance.

  The Symantec Management Agent communicates regularly with Notification Server to determine if it has work to do. This interval is the primary setting for agent communication time frames and determines how quickly work is delivered to managed computers. The more frequently your managed computers request a new configuration, the more total load is placed on the Notification Server computer’s resources and the network. The configuration request itself does not increase the load on Notification Server computer. Rather, the work that the Notification Server computer must do to respond to each request increases the load. You can change the request interval to adjust the total number of requests and the total volume of network traffic that is generated.

  The default request interval to download new configuration settings is one hour. A typical request generates approximately 3 kbits of network traffic

  For example, 5,000 managed computers make 120,000 total requests to Notification Server each day, totaling approximately 360,000 kbits of network traffic. However, by adjusting the setting to every two hours, you reduce the number of requests to 60,000. You also reduce the volume of network traffic to 180,000 kbits. This schedule halves the network traffic on the Notification Server computer; however, it also doubles the time between updates to the managed computers.

  Use the following guidelines to determine the appropriate value for the Symantec Management Agent configuration update interval:

Number of managed computers	Agent configuration update interval
< 1,000 endpoints	Every hour
1,000 to 5,000 endpoints	Every hour
5,000 to 10,000 endpoints	Every two hours
10,000 to 15,000 endpoints	Every three hours

Number of managed computers	Agent configuration update interval
15,000 to 20,000 endpoints	Every four hours

- **Upload basic inventory**.
  This setting is the interval at which the Symantec Management Agent sends basic inventory to Notification Server. Notification Server uses the information to uniquely identify each managed computer. Basic inventory contains information such as a list of installed agent/plug-ins and the TCP/IP address. The default interval uploads basic inventory once a day. A typical basic inventory update is between 20 kbit and 25 kbit in size.

Recommended configuration settings based on managed endpoints

This section displays recommendations for common configuration settings for the agent, inventory, resource membership updates, and the task service update schedule that can influence the performance of IT Management Suite.

See "Symantec Management Platform performance factors" on page 79.

Table 6-3 Configuration settings based on number of managed endpoints

Setting	< 1,000 endpoints	1,000 - 5,000 endpoints	5,000 - 10,000 endpoints	10,000 - 15,000 endpoints	> 15,000 endpoints
Agent configuration schedule	Every one hour	Every one hour	Every two hours	Every three hours	Every four hours
Full Inventory collection schedule	Monthly	Monthly	Monthly	Monthly	Monthly
Delta Inventory collection schedule	Weekly	Weekly	Weekly	Weekly	Weekly
Full resource membership update schedule	Daily	Daily	Daily	Daily	Daily
Delta resource membership update schedule	Every 5 minutes	Every 5 minutes	Every 5 minutes	Every 5 minutes	Every 5 minutes
Task Service update schedule	Every 5 minutes	Every 5 minutes	Every 15 minutes	Every 15 minutes	Every 15 minutes

You can also perform the following customizations to improve the performance:

- For tasks & policies, reduce targeting and scheduling.

- For reports, optimize your reports that you run often and query lowest level resource views in the resource type hierarchy.
- Optimize all custom filters and query lowest level resource views in the resource type hierarchy.

About improving Symantec Management Console performance

In large environments, Symantec recommends using the **SuppressReportAutorun** functionality. In NS Configurator, when **SuppressReportAutorun** is enabled and you open any report, the report does not run immediately. To see the results of the report, you must click **Refresh**. Note that by default the **SuppressReportAutorun** functionality is disabled. You can enable it in **NS Configurator**, under **Core Settings > User Interface > Report > SuppressReportAutorun**.

In large environments, Symantec also recommends configuring the enhanced view settings. You can configure specific search fields so that you can see your results as you type the parameter. You can also configure these same search fields so that you can see your results only after you press **Enter**.

You can configure the enhanced views to use IME (Input Method Editor) so that you can input double-byte characters in these views. You can also configure the number of computers and software that appear in the results list.

To configure the enhanced view settings, in the **Symantec Management Console**, on the **Settings** menu, click **Console > Enhanced Views**.

Chapter 7

Multi-Notification Server environments

This chapter includes the following topics:

About Notification Server hierarchy

Hierarchy is a technology designed to reduce the total cost of ownership (TCO) of managing Symantec software and solutions across multiple Notification Servers. Hierarchy reduces the TCO by supplementing the Notification Server system with centralized management capabilities.

If you have multiple Notification Servers, you can use hierarchy to define collections of Notification Servers that share common configuration settings and data.

A hierarchy topology defines the relationships between Notification Servers, which in turn controls how synchronization occurs between adjacent nodes. Also, it defines schedules for synchronization.

A hierarchy topology complies with the following rules:

- Each Notification Server can have zero or one parent.

- Each Notification Server can have zero or more children. Symantec recommends that you have maximum six child Notification Servers per one parent.

Each child Notification Server computer is only aware of its parent and is unaware of other child Notification Servers.

You can manage from both the parent and the child Notification Server computers. If management is done from a parent server, it can apply to all of the child servers and their managed computers. If management is done from a child server, the task only applies to the child server’s managed computers.

See “Hierarchy and replication requirements” on page 92.

See “About hierarchy replication rules” on page 93.

For more information about implementing hierarchy, see the *IT Management Suite Administration Guide*.

Key features of hierarchy

Hierarchy is a method to centrally manage client computers when multiple Notification Server computers are required.

See “About Notification Server hierarchy” on page 89.

See “About hierarchy replication rules” on page 93.

Hierarchy lets you do the following:

- **Centralized management**
  One of the key features of hierarchy is to provide the ability to manage several Notification Servers (children) from a single (parent) Notification Server.
  Hierarchy gives you the global management capabilities but also preserves the autonomy of the child Notification Server computers. For example, a global policy can be distributed from the parent Notification Server computer to all managed computers. Child Notification Server administrators can create policies for their specific requirements.
  Note that hierarchy does not increase the number of managed computers that each Notification Server computer can independently support.
- **Hierarchy editable properties (HEP)**
  HEPs let the parent server administrator control which properties of the replicated data the child server administrator is permitted to edit.
  By default, most of the data that is replicated from the parent Notification Server overwrites the data on child Notification Server. However, the parent server administrator can manually set HEPs to prevent overwriting of the data on child Notification Server. For example, the parent server administrator can define whether a child server administrator has rights to enable or disable a global policy and change the schedule or the target of a global policy.

- **Hierarchy events**

  Hierarchy events transfer data or raise events at the destination server when certain events occur at the source server. For example, hierarchy events are raised after resource merge, agent movement, agent purging, change of agent trust state, and synchronization issues. In such situations, hierarchy events are raised and the data is delivered immediately to keep all critical data up to date throughout the hierarchy.

- **Custom replication**

  On parent Notification Server, you can enable the custom replication. In the Symantec Management Console, you can then select the items that you want to replicate to child Notification Server. You can use the reports to view the items that are available for replication.

- **Urgent replication**

  To replicate an item to a destination server immediately, use the **Replicate Now** option in the right-click menu, in the Symantec Management Console. You can use this option for replicating in both up and down direction.

- **Agent trust**

  On the parent Notification Server, you can see the agent trust information from child Notification Servers. For example, you can see the status of the registration requests and the number of trusted agents. Note that you can approve or reject the agents only on the Notification Server to which they are assigned. You cannot approve or reject the agents of the child Notification Server on the parent server.

- **Managing duplicates**

  Duplicate resources that may appear in multi-server environments have different GUIDs but the same resource keys. If duplicate resources are found during the replication or during the resource creation, they are merged. After the resources merge, the hierarchy event is raised to synchronize the new resource GUID with all servers.

- **Managing ownership**

  Child Notification Server only replicates the managed (owned) resources. The resources that are imported using the Active Directory Import or Data Connector are not replicated to parent Notification Server.

  Parent Notification Server can detect within 15-30 minutes if the ownership of an agent has changed. When the agent is moved from one Notification Server to another, the hierarchy events are raised to update the data on parent Notification Server and communicate the new ownership to child Notification Servers.

  Parent Notification Server also tracks if each resource is assigned to only one server. If more than one server owns the resource, the parent Notification Server detects the owner, resolves the conflict, and communicates the new resource owner to the child Notification Servers.

- **Security tracking**

All security changes on the parent Notification Server are tracked and delivered to the child Notification Servers during the next synchronization. For example, if you change permissions of a folder that is replicated to the child server, the next synchronization applies the same permissions to this folder on the child Notification Server.

- **Emergency Software delivery**
  This feature lets you quickly distribute a software package to all computers in the organization. Emergency Software delivery first checks if the current Notification Server supports hierarchy and if it has child Notification Servers. If a child Notification Server is found, the replication starts immediately. The urgent replication rule distributes the emergency policy item, its replicated policy, software resources, and the software package down to child Notification Server.
- **Package delivery**
  To enable package delivery within the hierarchy, the parent Notification Server and its children synchronize their encryption keys. In the hierarchy, the encryption keys are always up to date on each Notification Server. If the encryption keys change, the hierarchy event is raised immediately.

  You can replicate packages from parent Notification Server to its children. After the package item is replicated to the child Notification Server, the policy with the replicated package item is distributed to the child Package Server. The child Package Server is then redirected to parent Package Server for package download.

Hierarchy and replication requirements

To share or receive common configuration settings and data with multiple Notification Server computers, you must first add the Notification Server computer to a hierarchy. Because Notification Server computers can be managed locally, each Notification Server computer must be added or removed from a hierarchy individually with the appropriate access credentials. Typically, the Symantec Administrator managing the topology design accesses the Notification Server computers in other sites remotely to add them to a hierarchy.

See “About Notification Server hierarchy” on page 89.

The requirements for configuring the hierarchy or replication are as follows:

- Network traffic must be routable between adjoining Notification Server computers within the hierarchy.
- HTTP/HTTPS traffic must be permitted between adjoining Notification Server computers within the hierarchy.
- If you use self-signed certificates for Notification Server computers, ensure that the trust between those computers is established. To do so, in the **Microsoft Management Console**, in the **Certificates (Local Computer)** store, manually install certificates to **Trusted Root Certification Authority**.

- Trust relationships must exist between adjoining Notification Server computers within the hierarchy, or credentials for the privileged accounts that facilitate trust must be known.
- Each Notification Server computer must be able to resolve the name and the network address of any adjoining Notification Server computers within the hierarchy.
- There must be sufficient bandwidth between Notification Server sites to support package and data replication.

  Bandwidth and the hardware that is required depend on the size of your hierarchy topology and the data replicated.
- A site must exist for each Notification Server computer, and must include the subnet that contains Notification Server. The site must also contain a package server (a site server that is running the package service) that serves the Notification Server computer.

  If you do not use Deployment Solution, use the task services on Notification Server. If you use Deployment Solution, dedicate a computer to host both the task services and the package services. This computer is called a network boot server. You must have a dedicated network boot server on each Notification Server site. When you use a dedicated task server, you must manually configure site management to restrict all client computers to use the dedicated task server.

Replication rules in multi-Notification Server environment

Depending on your requirements, you can use the following types of replication rules:

Hierarchy replication rules	Let you copy the information between parent Notification Server and its children. The hierarchy replication rules define which items are replicated, the direction that each item type flows, and when the replication occurs on each server in the platform. See “About hierarchy replication rules” on page 93.
Standalone replication rules	Require you to specifically define the items to replicate and the direction that they replicate. You must configure the rules very selectively because there is no automatic conflict prevention in standalone replication. See “About standalone replication rules” on page 95.

See “Hierarchy and replication requirements” on page 92.

About hierarchy replication rules

Hierarchy replication relies on hierarchy replication rules. These rules define the data that replicates to other Notification Server computers. Many items are configured to replicate by default. However, there are practical constraints, particularly on the number of items that can replicate up the hierarchy. For example, many inventory data classes are not enabled to replicate up the hierarchy by default. Without those data classes, some reports do not function at the parent Notification Server computer. You should be selective in choosing which data classes to replicate up. You can disable a replication rule at any time and enable it again later; it is not deleted.

Warning: For data consistency, Symantec recommends not to use the standalone replication rules to replicate data between servers in hierarchy.

Hierarchy has two modes of replication:

Differential

Replicates the objects and the data that have changed since the last replication. This mode is enabled by default and reduces the load and the bandwidth that hierarchy uses.

Complete

Replicates all objects and data. This mode is disabled by default.

In the hierarchy, the objects and data types can only be replicated in one direction. To provide centralized management capabilities, the objects and data types that are associated with configuration and management operations can only be replicated down the hierarchy.

Configuration and Management Items

Policies, tasks, filters, and reports are replicated down the hierarchy.

Items use differential replication, which is handled by hashing each item to check for changes and replicating those that have changed.

Note: Server Jobs are not replicated from parent Notification Server to child Notification Servers.

Security Settings

Security roles, privileges, and permissions are replicated down the hierarchy.

Security objects, such as roles and privileges, always use complete replication.

Resources	Resource information, such as computers, users, sites, and their associated data classes are replicated up or down the hierarchy. **Note:** If, on parent Notification Server, you manually assign a primary user to a computer, the association is only replicated down the hierarchy. Note that this association can only be changed on parent Notification Server. Resources use differential replication. Differential replication is based on the "last changed" timestamp on the source data. Any data that has changed since the last replication is replicated to the destination server. The data on the destination is then verified, if data verification has been enabled in the appropriate replication rule. Data verification imposes significant processing load on Notification Server. To reduce this load, you can verify a specified percentage of data on the destination server with each replication. For example, if you verify 10% of the data for each replication, that ensures that all data has been verified after 10 replications.
Packages	Packages that are associated with software resources and the data classes that are associated with the packages are replicated down the hierarchy.
Events	Event classes, such as software delivery execution, are replicated up or down the hierarchy. Note that events can overwhelm a parent Notification Server computer when replicated. By default, no events are enabled to replicate. These should be replicated only with great caution and for limited time periods. Note that because replication does not occur real-time, raw event data cannot be used for alerting at the parent Notification Server computer.

Note that critical system data, such as resource GUIDs, certificates, agent ownership data, and alerts, is synchronized as quickly as possible using the hierarchy events. All other data is synchronized according to the hierarchy schedules using the hierarchy replication rules.

Note: Some Symantec solutions create custom replication rules to ensure that specific items are always synchronized.

See “Key features of hierarchy” on page 90.

About standalone replication rules

Replication using the standalone replication rules is a one-way transfer of data between two Notification Servers.

The following replication types are supported:

Differential

Replicates the objects and the data that have changed since the last replication. This method is the recommended method because it reduces the network load and bandwidth consumption when data is replicated.

Complete

Replicates all objects and data.

This method is commonly used for hierarchy replication. A complete replication is typically performed monthly to ensure full replication.

To configure replication, you need to set up the appropriate replication rules on each Notification Server computer. Each rule specifies the data to replicate from that server (the source server) to one or more specified destination servers and the schedule to use.

You can create the standalone replication rules for the following items:

Events

Replicates Notification Server events.

Items

Replicates Notification Server configuration items and management items such as tasks, policies, filters, and reports.

Resources

Replicates Notification Server resource types, resource targets, and specific data classes.

If you include resource targets in a resource replication rule, remember that resource scoping applies to the contents (resources) of the replicated target. Therefore, the resources that are replicated depend on the owner of the resource target. The Notification Server administrator can choose to replicate resource targets in their current state (owned by somebody else, with the corresponding scope). Alternatively, they can take ownership of the targets, save them with the administrator’s scope (which usually contains more resources) and replicate them in that state. All the current members of a resource target are replicated. The actual resource target item is replicated in the background as a dependent item. The target that is applied to a stand-alone rule is replicated when the stand-alone rule itself is replicated. When the rule is run, the target is not sent.

Security

Replicates Notification Server security roles and privileges. Two types of security replication rules are available: Privilege and Role. The configuration procedure is identical for each.

When you include a security role in a replication rule, you must also configure a replication rule to replicate all of the privileges in the role. The replicated security role does not recognize any privileges that already exist on the destination Notification Server computer.

Note: Standalone replication of packages is not supported between two Notification Servers with the same version.

Hierarchy replication implementation considerations for Patch Management Solution

This section includes specific considerations about Patch Management Solution to be aware of before you implement a hierarchy replication plan.

The following are implementation considerations with Patch Management Solution:

- Use patch management in a hierarchy to replicate software updates down the hierarchy for distribution and receive vulnerability reports at the top of the hierarchy.
- In a hierarchy, patches must be imported at the parent Notification Server.
- To minimize distribution times, replication schedules must account for the following order of operations: Patch import schedule; Patch import replication rule; site server download; agent update interval.
- Without aligning schedules, patch distribution typically takes more than 48 hours.
- A compliance summary is all that's available at the parent Notification Server computer. Full vulnerability analysis reports drill down to each child Notification Server .

Hierarchy replication implementation considerations for Software Management Solution

Before you implement a hierarchy replication plan, be aware of certain considerations about Software Management Solution.

The following are implementation considerations with Software Management Solution:

- Hierarchy replication replicates software delivery policies and packages to child Notification Server computers for distribution.
- Policies, filters, and packages are replicated automatically down the hierarchy.
- Duration of the software delivery depends on the replication schedules, the frequency of the replication, and the complexity of the environment.
- Replication rules must be customized to include the software inventory details. The details are needed for reporting.

About MultiCMDB reporting with IT Analytics

The MultiCMDB feature lets you run global IT Analytics reporting across multiple CMDBs. You do not need to replicate large amounts of data. You can populate existing cubes from many Notification Server computers. It does not matter if Notification Servers are configured in a hierarchy or are standalone. MultiCMDB supports connections to both external 7.0, 7.1, 7.5, 7.5 SP1, 7.6, and 8.0. CMDBs. You can enable the cubes that you have data for and not enable others. This ability lets you use CMDBs with different solutions installed. They do not have to be consistent.

You currently cannot create filters (for policy targets, for example) from the ITA reports. MultiCMDB provides reporting but it does not provide top-down management. You should also note that the MultiCMDB feature does not support reporting on the ServiceDesk data. The MultiCMDB feature only covers data that is in a Symantec CMDB. ServiceDesk uses a separate database

IT Analytics MultiCMDB can provide the following:

- Efficient global ITA reporting across multiple CMDBs in environments without hierarchy.

  MultiCMDB does not replace hierarchy. It allows for global IT Analytics reporting without the need to replicate large amounts of data. Hierarchy is still needed for management for the top use cases. MultiCMDB capability is not hierarchy-aware. You must manually point IT Analytics to all the CMDBs that you want ITA reporting on. This operation can be done in the IT Analytics configuration page.
- Efficient global ITA reporting across multiple CMDBs in environments with hierarchy.

  You must pay specific attention to whether to include the top-level node in the hierarchy into the global reporting. You should exclude the top-level node from the MultiCMDB if your top-level server is used to receive data from a child level. Excluding the top node helps address an asset duplication issue. Currently this feature is not a good fit for the hierarchical environments that use Asset Management Solution.
- Efficient global ITA reporting during the 7.X to 8.0 migration (where at least one server is already on 8.0 and the rest are on 7.X), with or without hierarchy.

  You can use the MultiCMDB feature during IT Management Suite 7.X to 8.0 migration. The MultiCMDB feature lets you report on a mix of 7.X data and 8.0 data. This reporting can be helpful if the environment leverages hierarchy because hierarchy must be recreated during a 7.X to 8.0 migration.
- Multi-CMDB cube inclusion

  The cube inclusion functionality allows a customer to pick and choose which CMDBs should be processed for each cube. Choosing the CMDBs addresses the duplicate data problem by allowing a customer to effectively exclude the parent CMDB from all inventory-specific cubes and only process the parent CMDB for the Asset-specific cubes. In addition the child CMDBs can be configured to only be in scope for the inventory-based cubes (Computers, Patch).

Glossary

Active Directory Import A feature of the Symantec Management Platform that lets the user import Active Directory objects such as users, computers, sites, and subnets, into the CMDB (Configuration Management Database).

AeXGenClientCert.exe A command-line tool that generates the client certificates that Cloud-enabled Management requires.

AeXGenSiteServerCert.exe A command-line tool that generates the site server certificates.

AeXRevokeCertificate.exe A tool that revokes certificates.

agent registration policy A policy that lets the user automate the agent registration process. Agent registration policy is a set of rules that determine how the incoming registration requests are processed.

alert A notification about issues, failures, and particular states of the system. The user can customize which alerts are sent, logged, and where the alerts are sent.

Alert Manager A feature that generates a ticket when an event occurs, and sends notification messages to the designated users.

applicability rule A rule that determines whether a computer has the correct environment for an installation of a specific software package.

application identity of Notification Server An account under which Notification Server runs.

automated action An action that runs in response to an event. Automated actions can generate alerts, execute tasks, create reports, and send emails.

automation policy A rule in XML format that defines the attributes of a resource such as its groups, relationships, and wanted states. Automation policy initiates automated actions to update the resource and bring its attributes into compliance.

Basic filter A type of filter that filters the computers according to the static parameters.

blockout period The time when all communication between the agent and the Notification Server computer is disabled.

CEM (Cloud-enabled Management) A feature that lets the user manage the client computers outside the corporate network without a VPN (virtual private network).

client certificate A certificate that allows a client computer or a site server to identify itself to Notification Server.

client computer A computer that has Symantec Management Agent installed on it and can be managed from the Notification Server computer through Symantec Management Console.

client task A task that is executed on a client computer.

Client Task Agent A sub-agent that runs on client computers. Client Task Agent accepts tickles from a task server and receives job and task information. It then passes this information to a handler and sends status information back to the task server. This sub-agent is installed automatically with the Symantec Management Agent.

Cloud-enabled agent An agent that is allowed to communicate with Notification Server through an Internet gateway.

CMDB (Configuration Management Database) The central database that stores all the data that Symantec Management Platform uses and generates.

Command-Line Builder A tool that is used to create a syntactically correct command.

complete hierarchy replication A process that replicates all objects and data in the hierarchy.

Complete Update schedule A schedule that completely recreates the membership of all filters, organizational groups, and targets, regardless of inventory status or any changes to policies.

connection profile A group of settings that defines which network protocols are used to communicate with the network devices.

Credential Manager A secure store for the credentials that Notification Server and installed solutions use.

Data Connector A component of the Symantec Management Platform that lets the user transfer data between external data sources and the CMDB (Configuration Management Database).

delta update schedule A schedule that updates the membership of the filters that have had membership changes, all dynamic organizational groups, and invalid targets.

detection rule A rule that determines if specific software is installed on a computer.

differential hierarchy replication A process that replicates the objects and the data that have changed since the last replication.

discovery The process of searching for computers or other resources on the network that meet specific requirements.

Documentation Library A collection of help content that is installed with each IT Management Suite component.

event Any action that Notification Server can monitor.

filter A query that identifies a dynamic group of resources that share common criteria.

Full Windows Installer Repair

A policy or task that runs on client computers and verifies that all of the component resources of the Windows Installer applications are installed correctly. If any element of a component is not installed correctly, Full Windows Installer Repair initiates the repair of that component.

global exclude entry

A way to exclude application data from being saved in any application layer. Global exclude entry is used to prevent the loss of data when an application layer is reset.

hierarchy

An organizational structure of multiple Notification Servers that identifies a parent Notification Server. It then replicates the relevant data to any number of child servers, which can be located on different structural levels.

Internet gateway

A computer that tunnels communication between client computers outside the corporate network and the Symantec Management Platform infrastructure. Setting up an Internet gateway is required to use Cloud-enabled Management.

Inventory Rule Management

The software feature that lets the user create, edit, and delete rules and the expressions that make up rules.

item

Any object that belongs to CMDB (Configuration Management Database), such as a policy, a folder, or a computer that can be managed. Each item has a name, description, GUID, and attributes, and can be cloned, imported, exported, presented, and secured. Items can be linked with references or named relations between them.

job

A sequence of tasks that are executed on a target. Jobs can include the conditions that specify when the task runs.

Jobs and Tasks Portal

A page in the Symantec Management Platform that lets the user create and schedule tasks to run on the managed resources.

layer exclude entry

A way to exclude application data from being saved in a specific application layer. Layer exclude entry is used to prevent the loss of application data when an application layer is reset.

legacy agent

Symantec Management Agent that has the version that is previous to the Notification Server version. For example, in IT Management Suite 7.5 a legacy agent is Symantec Management Agent 7.1.

LAC (Legacy agent Communication)

Log Viewer

A tool that lets the user monitor several locations of logs for different components.

maintenance window

A scheduled period of time when maintenance operations may be performed on a client computer.

managed computer

A computer on which the Symantec Management Agent is installed. Another term for a client computer.

Managed Delivery

A policy that can perform complex software delivery tasks. Managed Delivery can perform recurring software deliveries, check for compliance, perform remediation, and install dependency software. It can also deliver multiple software resources and uninstall superseded software.

migration A process of moving Symantec Management Platform data from an older platform version to a newer one. Migration is performed when the Configuration Management Database (CMDB) is not compatible with the newer version of the platform.

migration wizard A tool that is used to perform a migration. Migration wizard is shipped with Symantec Installation Manager.

My Portal page The default page that opens when a new user runs the Symantec Management Console.

Network Discovery A process of discovering all IP devices that are connected to a network.

Network Discovery task A scheduled task that discovers either a single device or multiple devices on a network.

Network Discovery wizard A tool that is used to create a Network Discovery task.

Notification Server The main component of Symantec Management Platform communicates with Symantec Management Agent and the CMDB (Configuration Management Database), and provides the user interface and the background that the solutions that are part of the IT Management Suite require. Notification Server processes events, facilitates communications with managed computers, and coordinates the work of the other Symantec Management Platform services.

NS Configurator A tool that lets you change most core Notification Server configuration settings. These settings include many that are not accessible from the Symantec Management Console.

NSE (Notification Server Event) An XML file that is transferred between Notification Server and Symantec Management Agent. NSE can contain the following information: event processing, basic or full inventory, success or failure of a package download.

offline installation package A file that is used to install Symantec Management Agent on computers outside the corporate network. It contains an executable installation file that is generated on the Notification Server computer, and a Cloud-enabled Management policy.

organizational group A set of resources that are grouped by common properties or similar features for management and security purposes.

organizational view A hierarchical grouping of resources that reflects a real-world structure of an organization.

package A file that is intended for installation on client computers.

Package Delivery task A task that delivers and installs the software on client computers.

package server A type of site server that is used to distribute packages from Notification Server to client computers.

permission An ability of a particular user or group to perform specific actions on a resource and access particular items.

policy A set of rules that are applied to a resource or a set or resources that control the execution of automated actions. Policies can be scheduled or based on the incoming data that triggers an immediate action. Policies determine when an action should start and how the results of the action are processed.

Policy Update schedule A schedule that updates the membership of filters that a policy uses if the policy has changed since the last update.

portal page A customizable Symantec Management Console page.

privilege A setting that determines the actions in the Symantec Management Console that a user or a group of users can perform.

Purge Maintenance A script that deletes old and obsolete data from CMDB (Configuration Management Database).

Query Builder A tool that lets the user configure the query SQL to build the filter query.

Query filter A type of filter to which the user can add the criteria from a default filter criteria list. When the user creates a new filter, it is automatically created as a Query filter.

Quick Delivery A task that lets the user deliver the software without the need to know which package to select or how to create the command line.

replication A one-way transfer of data between Notification Server and a client computer or another Notification Server.

replication rules The regulations that define the data that needs to be replicated to other Notification Servers.

report drilldown An action that is performed when the user clicks on an item in the report results.

resource Any item that Notification Server can track or manage, such as a user, site, installed application, computer, switch, router, or handheld device.

resource import rule A regulation that lets the user specify the resources that should be imported from Active Directory.

Resource Manager A feature that displays information about a resource, such as its properties and current state. Resource Manager also lets the user troubleshoot and perform actions on managed resources.

resource report A report that lets the user drill down on a particular resource to view full details in the Resource Manager.

resource scoping A security and resource management feature that limits the data that a user can access based on the security role membership. Resource scoping is implemented by assigning permissions to organizational groups.

resource target A framework that lets the user apply tasks and policies to a dynamic collection of resources.

rule expression A combination of symbols (identifiers, values, and operators) that yields a result upon evaluation. These symbols form the instructions that define the items that a rule should check the client computer for.

schedule A set time and date when an action, for example, a task, is executed. Actions can be scheduled to execute only once or with a set interval.

security role An organizational group that contains Symantec Management Platform users. A security role is characterized by name, permissions, and the privileges that are assigned to the role.

Security Role Manager A console that lets administrators set permissions for security roles.

server task A task that is executed on the Notification Server computer.

shared schedule A schedule that a number of items, such as policies or tasks, use.

site A group of client computers that is usually based on one or more subnets.

site server A computer that hosts a site service. A site service is a middleware component that is used to provide packages, tasks, and PXE configuration to Symantec Management Agents. A site server can host one or more from the following site services: Package Service, Task Service, Monitor Service (RMS), and Network Boot Service (DS). Site servers are used to reduce the load on the Notification Server computer.

smart rule A rule that determines whether a package is installed on a client computer.

Software Catalog A catalog that contains a list of known applications and predefined software products. Software Catalog is regularly updated to include the new inventory data.

Software Library The physical location of the software packages that are defined in the Software Catalog. The Software Library is the source of the definitive, authorized versions of the software packages.

Software Management Framework An interface that lets the user create and manage the software resources that are in the Software Catalog, and the packages in the Software Library.

Software Portal A web-based portal that lets the user request and install software with little or no outside intervention.

solution A product that leverages the services of the Symantec Management Platform and adds specific functionality to the platform.

solution plug-in A piece of software that is installed on a client computer and adds functionality to the Symantec Management Agent. A plug-in provides specific functions for the solution with which it is associated.

Source Patch Update A policy or task that updates Windows Installer applications with resilient source paths.

SQL filter A type of filter for which the user can edit the query SQL.

standard rule A rule that determines whether a specific software application is installed on a client computer. Standard rule expressions are static.

Symantec Management Agent The software that is installed on the computers that you want to manage. It facilitates interactions between Notification Server and a managed computer. The agent receives requests for information from Notification Server, sends data to Notification Server, and downloads files. The Symantec Management Agent also lets you install and manage solution plug-ins that add functionality to the agent.

Symantec Management Console A web-based user interface that lets the user manage the Symantec Management Platform and any other installed solutions.

Symantec Management Platform The platform that provides a set of services for IT-related solutions. These services include security, scheduling, client communications and management, task execution, file deployment, reporting, centralized management, and CMDB (Configuration Management Database) services.

target A framework that lets the user perform actions on dynamic sets of resources. A target consists of at least one organizational view and a number of filters.

task An action that is performed on a client computer or a group of client computers. Server tasks are run on Notification Server. Client tasks are run on managed computers.

task server A site server that distributes task information from Notification Server to client computers.

upgrade A process of patching the IT Management Suite to the newest version. This process is performed with Symantec Installation Manager. In contrast to migration, the upgrade can use the same CMDB (Configuration Management Database).

user-based policy A policy that is executed based on the user that is logged in on a given computer.

virtual data class A data class that lets the user integrate third-party system data with the Symantec Management Platform CMDB (Configuration Management Database) without the need to import data to CMDB.

Windows Installer Repair A policy or task that runs on client computers and verifies that all of the component resources of the Windows Installer applications are installed correctly. If any element of a component is not installed correctly, the policy or task initiates the repair of that component.

Index