Symantec Management Platform Architecture and Design

Version 1.1

21-June-10

Table of Contents

GENERAL DESIGN CONCEPTS **1**

ABOUT CENTRALIZED MANAGEMENT 1
ABOUT DECENTRALIZED MANAGEMENT 2
SQL server considerations *2*
SQL memory management *2*
SQL Database size considerations *2*
ABOUT SITE SERVERS 4
Site server requirements *5*
Package services design *5*
Task services design *6*
BRANCH SITES WITH MOBILE USERS 6

UNDERSTANDING SYMANTEC MANAGEMENT PLATFORM COMMUNICATIONS **8**

COMMUNICATIONS CONCEPTS OF THE SYMANTEC MANAGEMENT PLATFORM 8
Deployment Solution data communications *8*
Deployment Solution servers 8
Deployment site server setup 9
About capturing master disk images 10
About distributing disk images to deployment site servers 11
How disk-image deployment works *12*
Inventory Solution data communications *13*
Patch Management Solution data communications *14*
Asset Management Suite data communications *16*
COMMUNICATION CONCEPTS OF MULTIPLE NOTIFICATION SERVER COMPUTERS ON THE SYMANTEC MANAGEMENT PLATFORM 17
About hierarchy *17*
About hierarchy topology *17*
What you can do with hierarchy *18*
Concepts of replication *18*
About hierarchy replication *19*
About replication rules *19*
How hierarchy replication works *19*
Requirements of hierarchy *20*
Design considerations of hierarchy *21*
About site server architecture in a hierarchy *21*

INFRASTRUCTURE SIZING RECOMMENDATIONS **22**

Recommendations for small environments *22*
Recommendations for medium environments *22*
Recommendations for large environments 23

General design concepts

To design your Symantec Management Platform infrastructure, you must assess your specific organizational features and requirements. Your requirements can include several variables such as the following:

- The geographic implications of your environment.
  Is there a large central site with many small sites, or are there combinations of large and small sites?
- The distribution and policies of IT management

  What operations does IT manage centrally and what operations does IT manage locally? Will IT tasks be implemented from a central location or from local sites? Who should be responsible for managing Notification Server computers, site servers, databases and other operational items? Who should receive status information and at what levels? Often a regional or local group can repair issues locally. What are the security policies of your organization?
- The network infrastructure requirements.

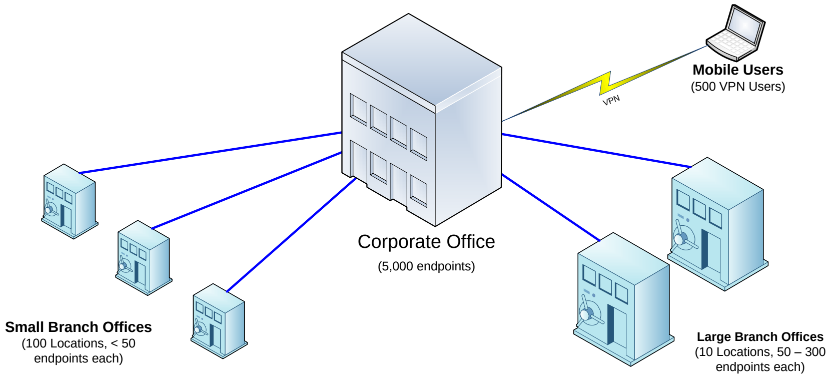
  Requirements can include specific SQL server resources, network resources, operational processes, management reporting needs, administration requirements of the IT department,
- The connectivity ranges in your environment. Are there tier 1 sites that are well connected but tier 2 sites that are poorly connected? Are there traveling users that may dial-in or use a VPN from different locations?

These variables will impact your design decisions, one of the primary choices you must make, is if to use a centralized or decentralized management model.

About centralized management

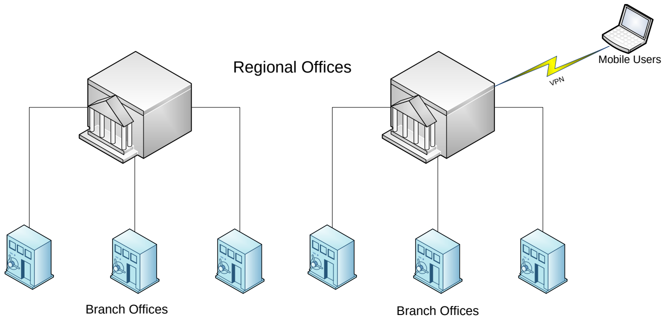
A centralized management design uses hierarchy to support a wide variety of IT distribution models. For example, you could have central corporate office with thousands of managed computers as well as both large and small branches. The centralized design can be effective for managing global policies and tasks.

If your IT organization is currently mostly centralized, then the Symantec Management Platform can be designed to fit the organization. It uses a parent Notification Server computer that is connected to additional children Notification Server computers.



About decentralized management

The decentralized 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 uses multiple Notification Server computers that operate independently.



SQL server considerations

A Notification Server computer can be configured to use a local database or a remote database. The largest use of resources on the Notification Server computer is consumed by database processing. A Notification Server computer with a local database requires more resources than a Notification Server computer with a remote database configuration. The database requirements themselves are driven by the number of solutions that are installed on the Notification Server computer and how they are used. The database requirements are also influenced by the number of managed computers reporting to the Notification Server computer.

SQL memory management

Memory Management is especially important when SQL is run locally on the Notification Server computer.

- **3GB**—This 32-bit Windows boot option limits the operating system to 1GB of RAM reserving 3GB for applications.
- **Maximum Server Memory**—A SQL setting which limits the memory SQL can consume.
- **PAE**—This 32-bit Windows boot option allows some applications (SQL) to the address memory beyond the first 4GB.
- **AWE**—This SQL option allows SQL to utilize more than 2GB of RAM
- **64-bit SQL**—By using a 64-bit OS (Windows 2003 or 2008) and 64-bit SQL you can avoid the memory issues which PAE and AWE address thereby safely ignoring those options.

SQL Database size considerations

A basic Symantec Management Platform with no solutions or clients creates a database size of about 300 MB. This size is a little over 7 percent of the maximum database size of SQL Express. An additional 500 managed computers can increase to size to approximately 500 MB. As solutions are introduced, and are used over periods of time between purging, databases can have additional growth.

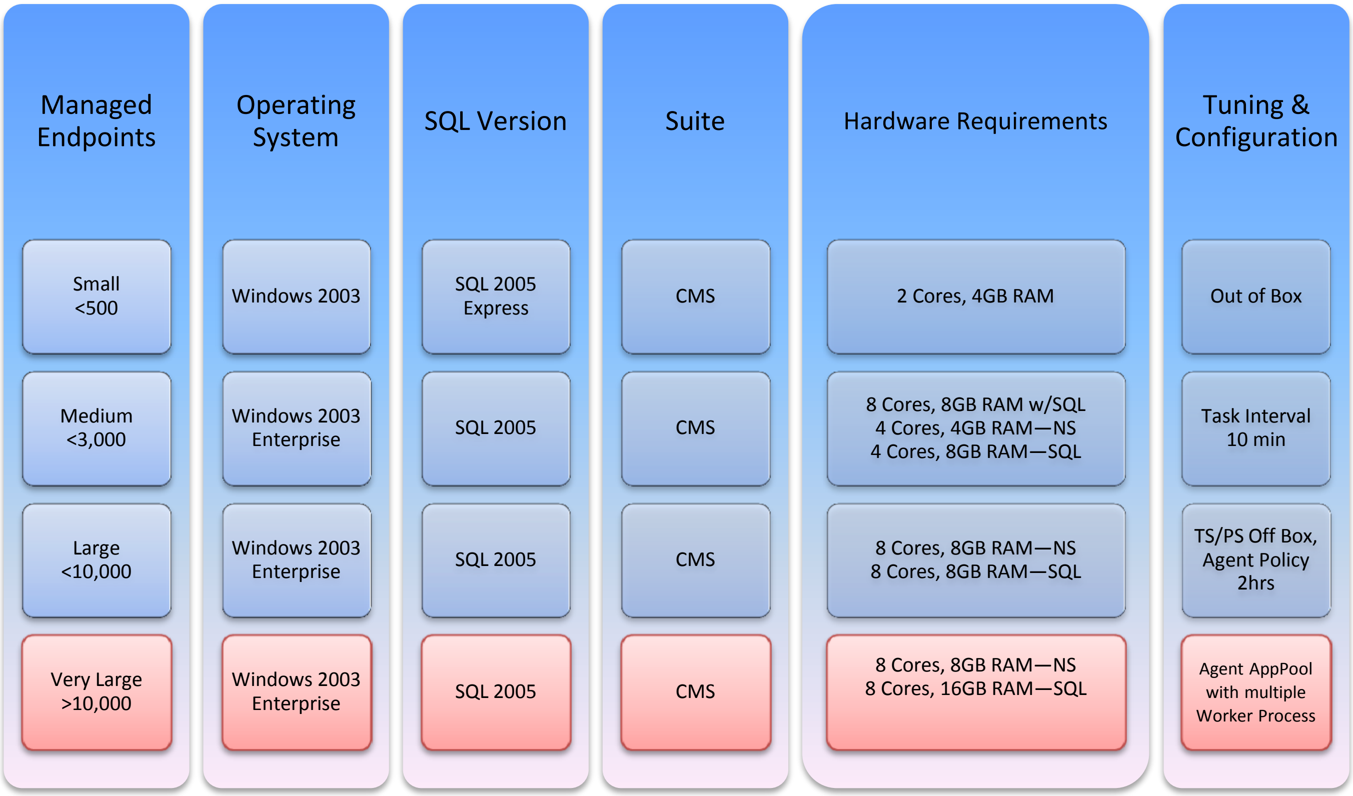
Consider allowing three-quarters to 1 MB per client in the Notification Server computer database. This sizing does not account for database fragmentation beyond initial creation. Actual sizes vary based on the solutions that are installed and the regularity of configured policy, tasks, and schedules. The database maintenance strategy that you employ will affect your actual database size.

When Client Management Suite, Server Management Suite, or other solutions are installed in a large environment, you can expect the Symantec Management database to grow to 6 GB to 12 GB. When choosing a database growth strategy, account for this kind of data growth to allow for the optimal performance by avoiding SQL file growth.

Once you have estimated the approximate size of the database it is recommended that you create a database file of this size prior to NS installation. This will ensure that you will have the space available and it will reduce the performance hits from SQL having to grow the database continually. It is also advised that you de-fragment and re-index the database after initial installation.

If a SQL cluster is proposed for a shared database infrastructure, it is important to properly evaluate the size of the cluster, number of nodes and the availability options. It is also critical that the individual databases for each Notification Server computer exist on a separate instance. This is recommended to avoid TempDB contention.

The following table depicts the recommended hardware and software specifications various scenarios:



Managed Endpoints	Operating System	SQL Version	Suite	Hardware Requirements	Tuning & Configuration
Small <500	Windows 2003	SQL 2005 Express	CMS	2 Cores, 4GB RAM	Out of Box
Medium <3,000	Windows 2003 Enterprise	SQL 2005	CMS	8 Cores, 8GB RAM w/SQL 4 Cores, 4GB RAM—NS 4 Cores, 8GB RAM—SQL	Task Interval 10 min
Large <10,000	Windows 2003 Enterprise	SQL 2005	CMS	8 Cores, 8GB RAM—NS 8 Cores, 8GB RAM—SQL	TS/PS Off Box, Agent Policy 2hrs
Very Large >10,000	Windows 2003 Enterprise	SQL 2005	CMS	8 Cores, 8GB RAM—NS 8 Cores, 16GB RAM—SQL	Agent AppPool with multiple Worker Process

About site servers

A Notification Server computer can distribute its workload processes and minimize network traffic by delegating package downloads and tasks to site servers. For example, a site server can be placed locally at a site to store software distribution packages. The package must only be copied to the site once for all managed computers at the site to access it. This can help if you have sites with low-bandwidth connections.

Any managed computer can serve as a site server and does not require special server hardware and software. The Symantec Management Platform provides a utility called site management to help you organize your site servers. With the site management utility you can assign your network subnets and sites to site servers. A site server supports managed computers within its site and subnet. If no sites are defined, then all site servers are available to support all managed computers (although this is not recommended).

There are three main types of site server services. These services include, package services, task services, and deployment site services. Any combination of these services may be enabled on a single managed computer.

The number of site servers required in any environment is based on your network topology and bandwidth. It also depends on the following:

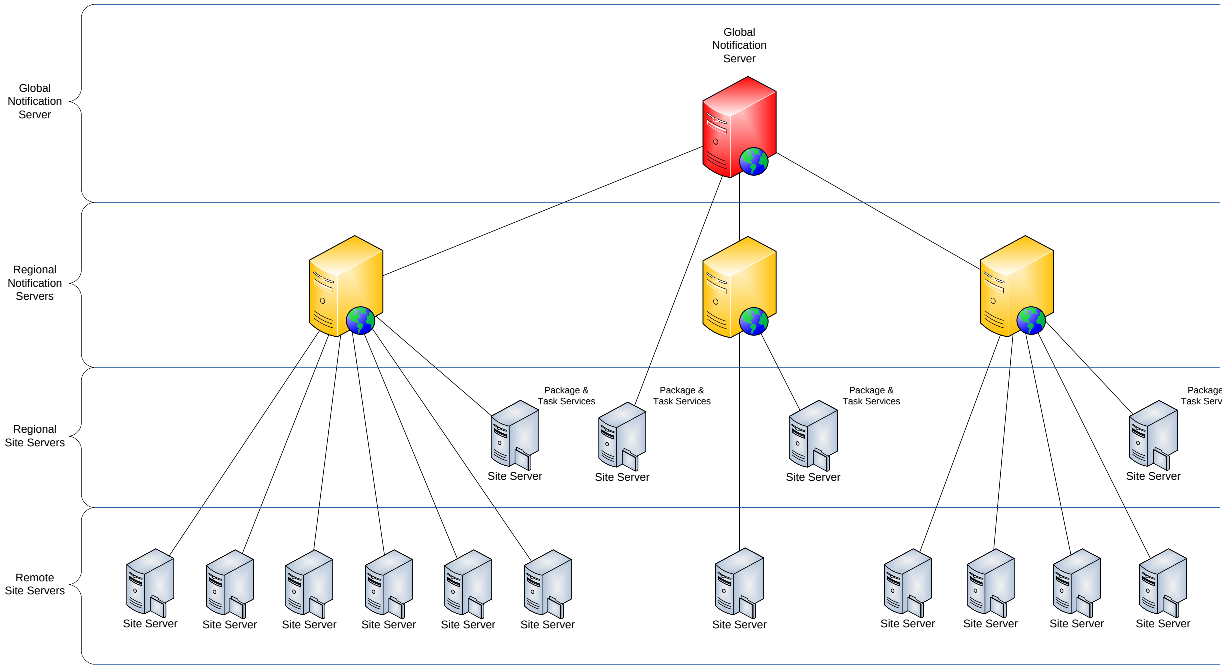
- The size and frequency of the packages to be delivered
- The number of managed computers.

The following table lists the minimum number of site servers you will need for the number of managed computers for a single Notification Server computer with task, package and deployment site services enabled.

Notification Server computers	1	1	1	1	1
site servers	1	1	1	2	4
Managed computers	500	1000	2500	5000	10000

A single Notification Server computer can manage up to 500 site servers, and up to 5,000 packages.

The following diagram illustrates the use of multiple site servers:



Site server requirements

The number of managed endpoints a site server can support depends on its hardware and software. The following recommendations are based on the minimum hardware recommendations. They assume a site server with the package, task and deployment services enabled.

Item	Minimum Specifications	Recommended Minimum
CPU	Pentium 4 or Better	Pentium 4 2.0Ghz or Better
RAM	512 MB	1 GB
Operating System	**x86 versions of the following:** Windows 2000 SP4 or Later Windows XP SP2 or Later Windows Vista (all) Windows 2003 Server SE SP1 or Later Windows 2008 Server SE	Windows 2003 Server Standard (x86) SP1+
Web Server	IIS 5.0	IIS 6.0
Min. Storage	1.5 GB + 120% of total package size	2 GB + 120% of total package size
File System	NTFS	NTFS
RAID	Not Required	Not Required – R1 if Available
Prerequisites	Symantec Management Agent 7 installed Microsoft .NET Framework 1.1 TCP Ports 50120-50124 opened	Symantec Management Agent 7 installed Microsoft .NET Framework 1.1 TCP Ports 50120-50124 opened

Package services design

When considering package services design, placement and configuration the following factors can affect the efficiency of the infrastructure:

Stagger the deployment of packages to the site server. Deploy a few packages at a time on all package servers, or deploy a reasonable amount of packages to only a few package servers at a time

- If hierarchy replication is used, you must have at least one site server with package services installed on the same site as each Notification Server computer.
- To minimize network traffic and load follow these guidelines to aid in planning package distribution:
    - If you have multiple sites, add a site server with package services for each site.
    - Assign a package to all site servers.
    - Assign a package to selected site servers.
    - Manually assign sites to packages from a list of sites configured in the site management page. When a site is assigned to a package, all package servers within the selected site will host the package.
    - Configure servers automatically with manual presaging or Active Directory Import so sites will be automatically assigned to packages according to Symantec Management Agent and site server requirements for that package.
- For a site to function as a package server there must be at least one unconstrained site server with package services assigned to it. An unconstrained site server with package services can get packages and other resources from anywhere in the system, while a constrained site server with package services can operate only within the sites to which they are assigned. To use constrained and unconstrained package servers, you have to put them both on the same site. In other words, there has to be at least one unconstrained PS in a site with one or more constrained PS's.
- You need an unconstrained site server with package services in the site to collect any required resources from outside the site and make it available to all the constrained site server with package services within the site.
- When sites are unassigned from a package, they are not reassigned at the next package refresh interval, even if there is an enabled task associated with the package. A package is reassigned to the unassigned sites if an Symantec Management Agent in these sites requests the package.

Task services design

The following guidelines should be observed to ensure proper configuration and efficiency of task services within your infrastructure:

- If a Notification Server computer is managing a substantial amount of solutions and client computers already, adding task server management could significantly affect performance. The following statement summarize the proper use of task services:
  - If Notification Server computer is managing 500 registered end points or less, Notification Server computer can have dual role as a managing site server with task services enabled.
  - If Notification Server computer is managing more than 500 registered end points, remote site servers with task services should be deployed.
- A site server with task services can be configured to register up to 5,000 endpoints with a supported desktop operating system and up to 10,000 Registered Endpoints with a supported server class operating system.
- Consider adding an additional site server with task services enabled for every 2,500-5,000 endpoints
- Task services can be load balanced within a Site; assign more than one site server running task services to a Site to ensure agents always have the latest task execution
- Increasing the "Task Update Interval" and "Maximum Time Between Tickle Events" settings found in the task services to a value greater than 10 minutes can reduce the load on the site server.
- The amount of client computers that a task server can service depends on the hardware configuration of the task server computer. As you increase the hardware capabilities, you can increase the managed client numbers.
- If you install a task server in a site with a Notification Server, then you have to use site management to restrict all managed computers to use the task server instead of the Notification Server for tasks.

Branch sites with mobile users

Small organizations can install Symantec Management Platform on a single server, or distribute servers across multiple servers to manage clients. With one or more servers, you can set up local peer servers on a single computer or distributed across multiple computers to manage a site.

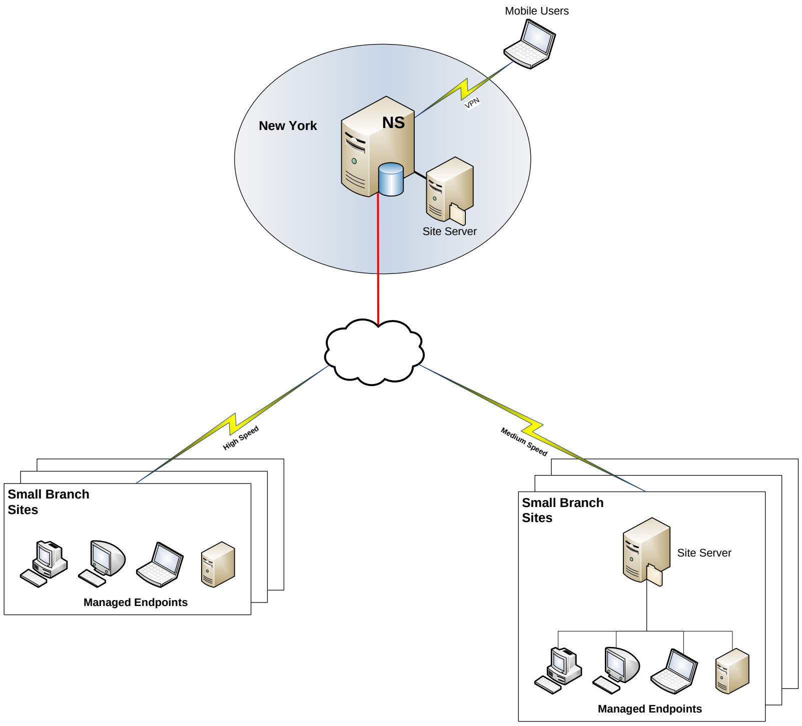
For organizations with remote sites and personnel, servers can be configured to manage satellite locations from a regional Notification Server computer. If the branch site is small and has no resident IT person, package servers can be installed to download software and image packages deployed from a local site.

Placing site servers at a branch site depends on the number of client computers managed and if IT personnel are on site. The Notification Server computers and the managed endpoints can utilize local package server at each branch location. Remote users can update patches and other software packages across the WAN from the closest package server for remote users or satellite offices.

Notification Server computers at the corporate level can inventory itinerant users and download software using the closest package server. When the user returns to the home office, the portable computer can be updated with larger packages from the Local site server across the LAN.

Example:

The illustration below shows an example of an organization that consists of a main site, remote users and small branch sites with high speed and lower speed connections.



This scenario demonstrates the following:

- A single Notification Server computer Can be used to manage various connection strategies
- High Speed connected branch sites with small numbers of managed endpoints do not require site servers if the available bandwidth is good and connection speeds are consistent.
- Lower speed connected branch sites with smaller or larger numbers of managed endpoints should use site servers to reduce the impact on the network segment.
- Remote users can be managed through the Central Notification Server computer, as well as the branch sites with package servers.

Understanding Symantec Management Platform communications

Communications concepts of the Symantec Management Platform

To use the Symantec Management Platform, you need to understand the communications concepts of the solutions on it. This section provides information regarding how communications are done for fundamental use cases of solutions on the Symantec Management Platform.

Deployment Solution data communications

The two main uses for provision with Deployment Solution are:

- Bare-metal deployment of an image to a new computer.
- Reimaging of a production computer to restore to a company standard settings.

Depending on the state of the computer and the deployment site server settings that you configure, you can deploy images to computers in the following ways:

- Deploy to a managed computer. – Requires that the computer have the Symantec management agent previously installed. Because the computer is managed, you can target it directly from the console and start the deployment job. You can configure this to either deliver the pre-OS environment over the network in real-time, or to use an automation folder that is pre-installed on the managed computer. If you previously installed the automation folder it can simplify and speed up the reimaging process. Once the pre-OS environment is loaded, the job is completed.
- Deploy to a predefined computer – Requires one job per computer. You enter the MAC, serial number, and the UUID of the hardware into the Symantec Management Console in advance. When the computer connects to the network, PXE loads the pre-OS environment and the job is started.
- Deploy to an unknown computer when any unknown computer connects to the network, PXE loads the pre-OS environment, and the job is started.

  Warning: This feature is intended to be used in isolated provisioning environments. Do not enable this option in your production network as it can result in unintentionally re-imaging computers.
- Boot from a local media device like boot disc, CD/DVD, or USB drive. With local access to the computer you can use boot media to load the pre-OS environment. Once the computer is connected to the network and the pre-OS environment is loaded, the job is started.

Although the pre-boot environment gets to the computer in different ways, once the boot environment is loaded, all deployment jobs run the following tasks:

- Boot to automation task
- Deploy image task
- Reboot production

Deployment Solution servers

Deployment solution has components installed on the Notification Server computer, and a deployment site server.

The Notification Server computer includes:

- Deployment site server settings- used for managing your deployment site servers.
- Pre-Boot environment setting- used for setting up WinPE and Linux boot images.

The deployment site server includes:

- Deployment share- where the imaging executables and boot images are stored.
- The disk-image package- the package used to provision computers.
- Driver database- drivers to support multiple computer hardware types.
- PXE serves- responds to the client computer’s PXE requests.

Deployment site server setup

You must use the Symantec Management Console to enable deployment, package, and task site services on every site server.

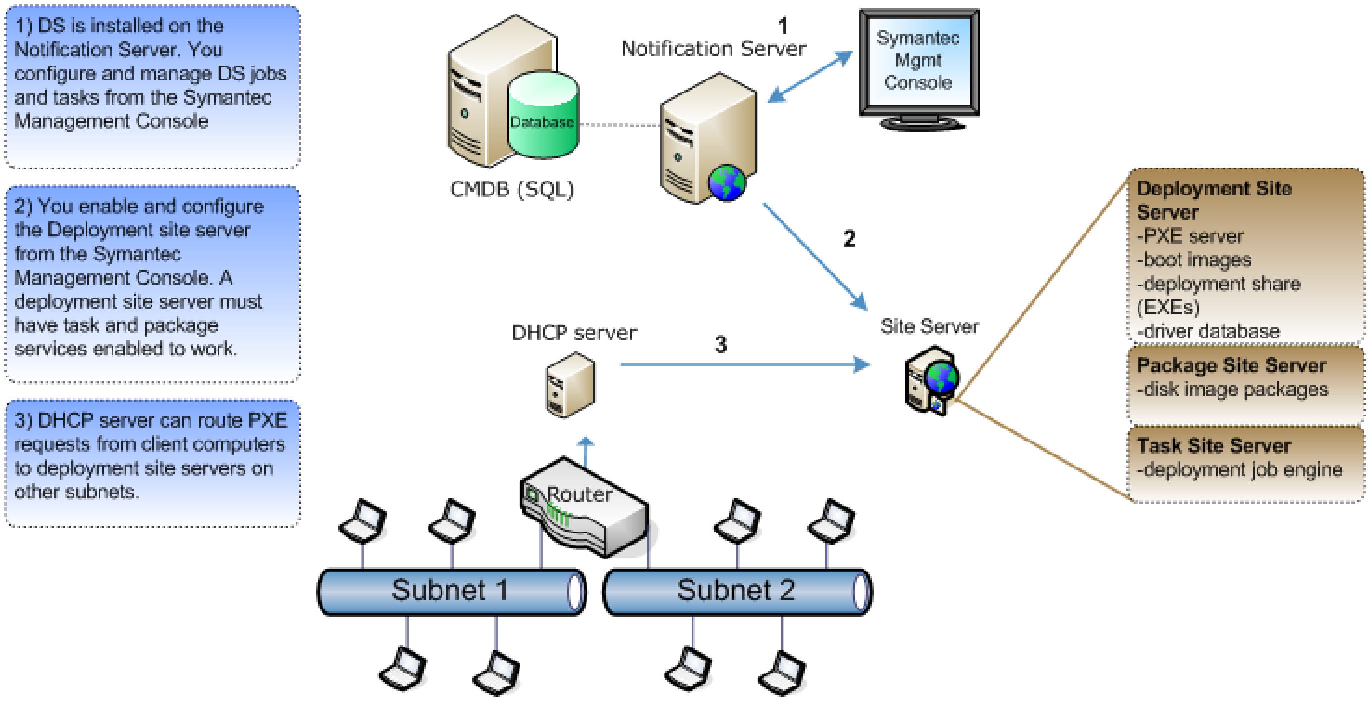
Task services require IIS which normally is installed on a server OS. Therefore, each deployment site server is a significant investment to factor into the design. Where possible, you will want to limit the number of deployment site servers.

Each subnet must have access to a deployment site server, however routers normally block PXE broadcast packets. You can use following three methods provide each subnet with access:

- Use ”DHCP forced mode” which is a DHCP setting to forward client PXE requests to the closest deployment site server. This method works even when the client computer is on a different subnet than the deployment site server. DHCP determines the correct server by using subnet mask and ping tests.
- Use “IP Helpers” is a setting you can configure at each router that lets you forward PXE requests across subnets.
- Install a deployment site server on each subnet which is not recommended because it creates unnecessary overhead.

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

The following diagram represents setting up your deployment site server:


1) DS is installed on the Notification Server. You configure and manage DS jobs and tasks from the Symantec Management Console
2) You enable and configure the Deployment site server from the Symantec Management Console. A deployment site server must have task and package services enabled to work.
3) DHCP server can route PXE requests from client computers to deployment site servers on other subnets.
1
Notification Server
Symantec Mgmt Console
Database
CMDB (SQL)
2
DHCP server
3
Site Server
Router
Subnet 1
Subnet 2
Deployment Site Server
-PXE server
-boot images
-deployment share (EXEs)
-driver database
Package Site Server
-disk image packages
Task Site Server
-deployment job engine

About capturing master disk images

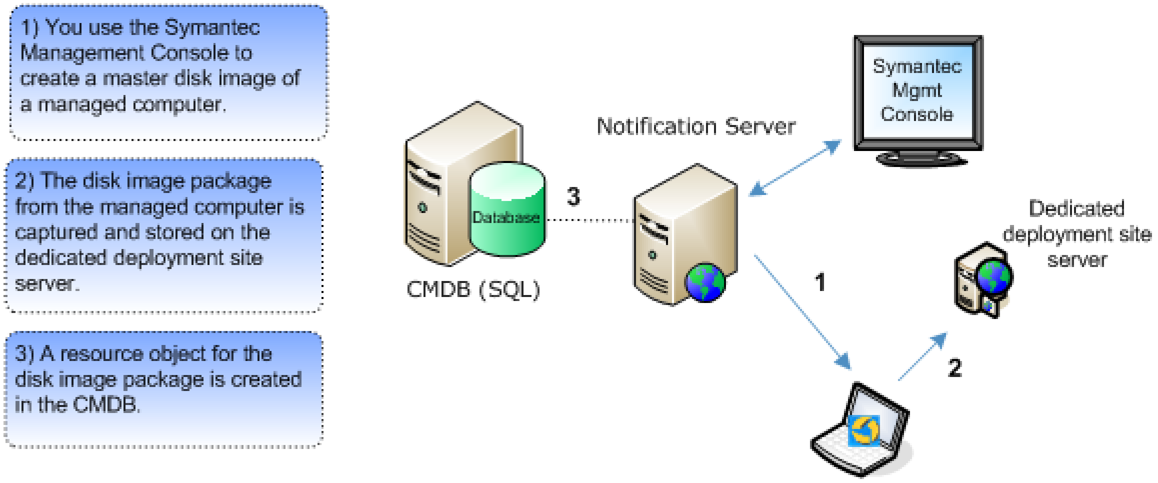
You capture a master disk image of a managed computer with Deployment Solution in the Symantec Management Console. This is done by creating a disk imaging task. When you create the disk imaging task, you should use a meaningful name to identify the disk image. This is because when you later select the disk image to deploy, you will rely entirely on the image name to locate it.

The master image of the computer already contains the Symantec management agent. This eliminates the need to roll-out new agents every time a computer is deployed or reimaged. By default, when the image is restored to a new computer, the Symantec Management Agent that is contained in the image will attempt to connect to the same Notification Server computer that the source computer was communicating with. To force the agent to connect to a new Notification Server computer, you must include a run-script task in the deployment job, that runs in the pre-OS environment to reconfigure agent with the location of the correct Notification Server computer. If you have multiple Notification Server computers in your environment, it may be easier to create a separate deployment job that contains the run-script task for each Notification Server computer.

The disk image is captured and stored on its assigned package server. The disk imaging task does two main things. First it creates a disk image package. Second, it creates a resource object for the package in the CMDB. This relationship between the image file and its resource in the database lets you create, manage, and deploy all of your disk images from the web-based Symantec Management Console.

We recommend that you use a dedicated package server to store and host your master disk images. Because each image is uniquely identified, images do not overwrite each other. Every time you capture an image, a new package is created and not related to any earlier versions. You should not manually delete any master disk images from the package server because it creates orphaned resources in the CMDB.

The following diagram represents capturing disk images:



1) You use the Symantec Management Console to create a master disk image of a managed computer.

2) The disk image package from the managed computer is captured and stored on the dedicated deployment site server.

3) A resource object for the disk image package is created in the CMDB.

About distributing disk images to deployment site servers

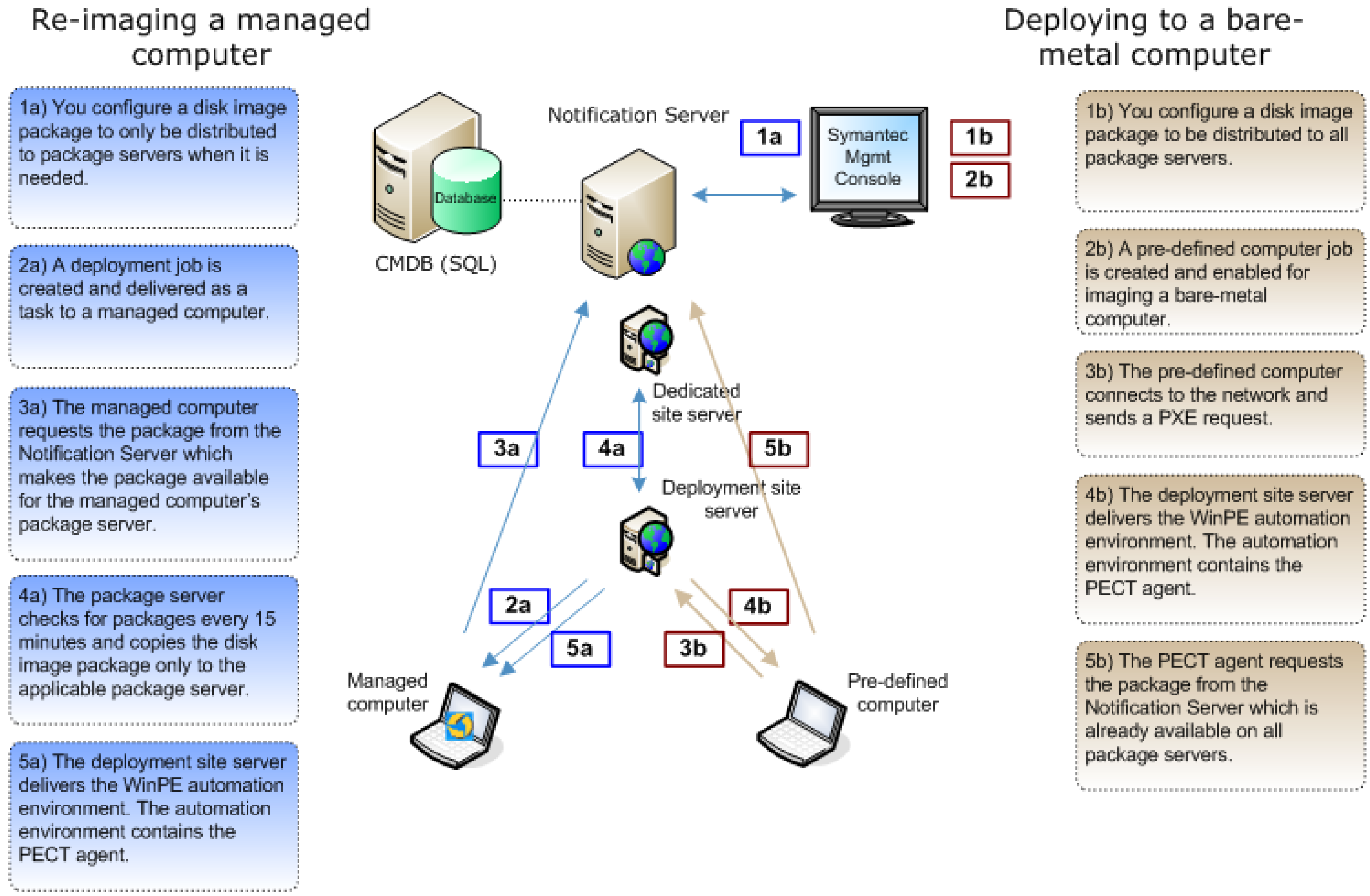
A deployment site server is a package server and must include the package services. Site management, package settings, and package servers all determine how your disk images are distributed to the package servers. By default, package servers check in for updates every fifteen minutes.

You must use site management to select one of the following global package distribution settings:

- **(default) Wait for a managed computer to request a specific package**- The method is called manual pre-staging. When a managed computer gets a policy or task that requires a package, it then requests its package information. Site management distributes the package to only the applicable package server(s). Tasks are able to track the package availability and knows when the package is available on the package server execution.
- **Copy to all package servers-** copies your packages to all of the package servers in your production environment.
- **Copy to specific package servers-** copies your packages only to the servers that you define.

You can create a custom distribution setting for specific packages that can override the global settings.

The following diagram represents distributing disk images to site servers:



Re-imaging a managed computer

1a) You configure a disk image package to only be distributed to package servers when it is needed.

2a) A deployment job is created and delivered as a task to a managed computer.

3a) The managed computer requests the package from the Notification Server which makes the package available for the managed computer's package server.

4a) The package server checks for packages every 15 minutes and copies the disk image package only to the applicable package server.

5a) The deployment site server delivers the WinPE automation environment. The automation environment contains the PECT agent.

Deploying to a bare-metal computer

1b) You configure a disk image package to be distributed to all package servers.

2b) A pre-defined computer job is created and enabled for imaging a bare-metal computer.

3b) The pre-defined computer connects to the network and sends a PXE request.

4b) The deployment site server delivers the WinPE automation environment. The automation environment contains the PECT agent.

5b) The PECT agent requests the package from the Notification Server which is already available on all package servers.

How disk-image deployment works

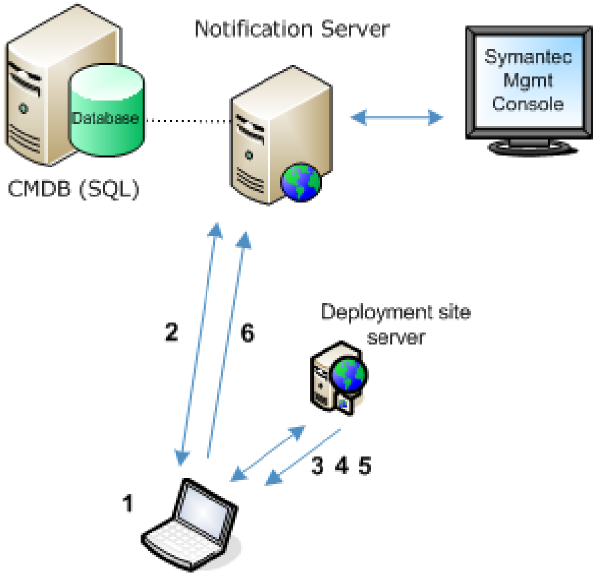
The following diagram shows how disk imaging works:

1) The pre-OS environment is loaded onto the targeted computer. The PECT agent is run. The PECT is a Symantec Management Agent that runs in a pre-OS environment.

2) The PECT agent requests information about which task server it should communicate with from the Notification Server.

3) The PECT agent requests jobs from the task server.

4) The task server distributes the deployment job to the PECT agent. The deployment job contains the path to the imaging .EXE and to the disk image package. They must both be stored on the same server because it uses the same name for the task server and the package server.



5) The image is pulled from the package server and is restored on the computer and the computer reboots to the production OS.

6) The Symantec Management Agent collects and sends basic inventory and is able to load any additional policies and tasks that apply to it. Any custom tasks that are included in the job, such as a personality transplant, are run at this time.

Inventory Solution data communications

Inventory Solution lets you see detailed reports about the hardware and software in your environment and target computers for policies and task based on this information.

There are pre-defined inventory policies that are enabled. The policies include the following settings:

- what to inventory
- when to run
- which computers to run on (targets), which is, by default, all computers with Inventory plug-in installed
- optional advanced settings

Inventory runs independent of the Symantec Management Agent check-in schedule. It uses tasks and task server to perform its operations.

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

- Daily = 6pm every day.
- Weekly = 6pm every Monday.
- Monthly = 1st Monday of each month 6pm.

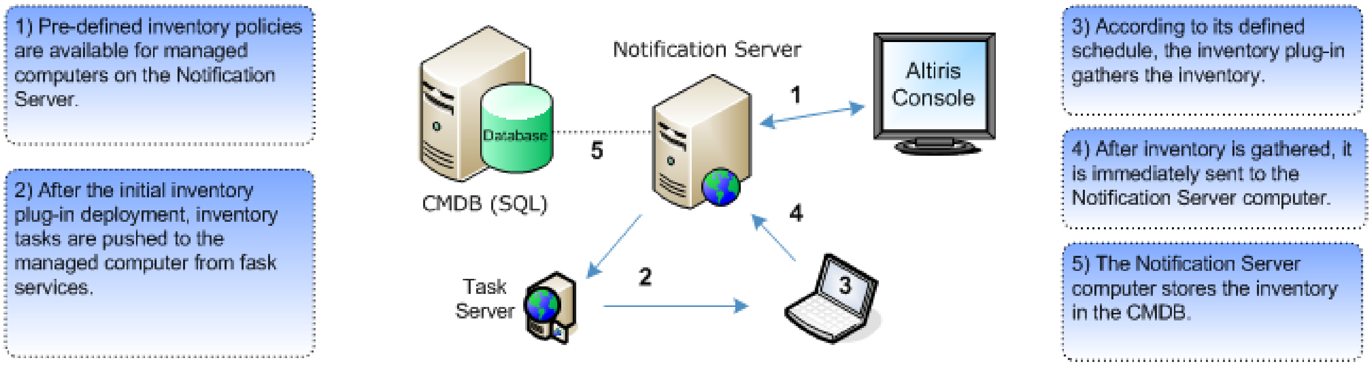
The time that the inventory runs applies to the time-zone of the managed computers and not the time-zone of the Notification Server.

Whenever the inventory plug-in runs, it gathers hardware inventory, file scans, Microsoft add/remove programs and Unix, Linux, Mac software listings. The inventory plug-in immediately sent the data to the Notification Server as Notification Server Events (NSEs). When the Notification Server receives the inventory NSEs, it stores the data in the CMDB. The data is then available for reporting from the Symantec Management Console.

Notification Server delivers the initial inventory task-based policy to the managed computer. The inventory plug-in runs the first inventory immediately.

After the inventory plug-in has its policy settings, it continues to run the inventory task according to the settings and schedule that is defined in the policy. If a policy setting is ever changed then the task server pushes the new settings to the plug-in immediately and it runs an inventory collection.

The following diagrams represent data communications of Inventory Solution:



1) Pre-defined inventory policies are available for managed computers on the Notification Server.

2) After the initial inventory plug-in deployment, inventory tasks are pushed to the managed computer from task services.

3) According to its defined schedule, the inventory plug-in gathers the inventory.

4) After inventory is gathered, it is immediately sent to the Notification Server computer.

5) The Notification Server computer stores the inventory in the CMDB.

Patch Management Solution data communications

Patch Management Solution for Windows 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.

Patch Management Solution is scheduled to automatically download critical security bulletins into the CMDB twice per month. This does not download the patch installation files, only the information about them in the security bulletins. This download is called the PMImport. The first PMImport on a new platform can take several hours, however subsequent imports typically take less than an hour because it only performs delta downloads and often only a few MBs. If you choose to enable multiple languages then the numbers of security bulletins, size, and time increases. You can customize PMImport by creating exclusions for the software that you don't want to patch, and creating custom schedules for the download.

By default every four hours the patch management plug-in contacts the Notification Server to check for patches. If new security bulletins have been added to the CMDB by the PMImport, the patch plug-in checks to see if they are applicable to the computer and if the updates have already been installed or not. It sends the results of the check to the Notification Serer computer. The data is available for compliance reporting.

After the PMImport has completed, and you know which patches you need, then you can select which security bulletins you want to stage on the Notification Server computer. This triggers a download the patch installation files to a folder on the Notification Server computer.

Once 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 are going to 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.

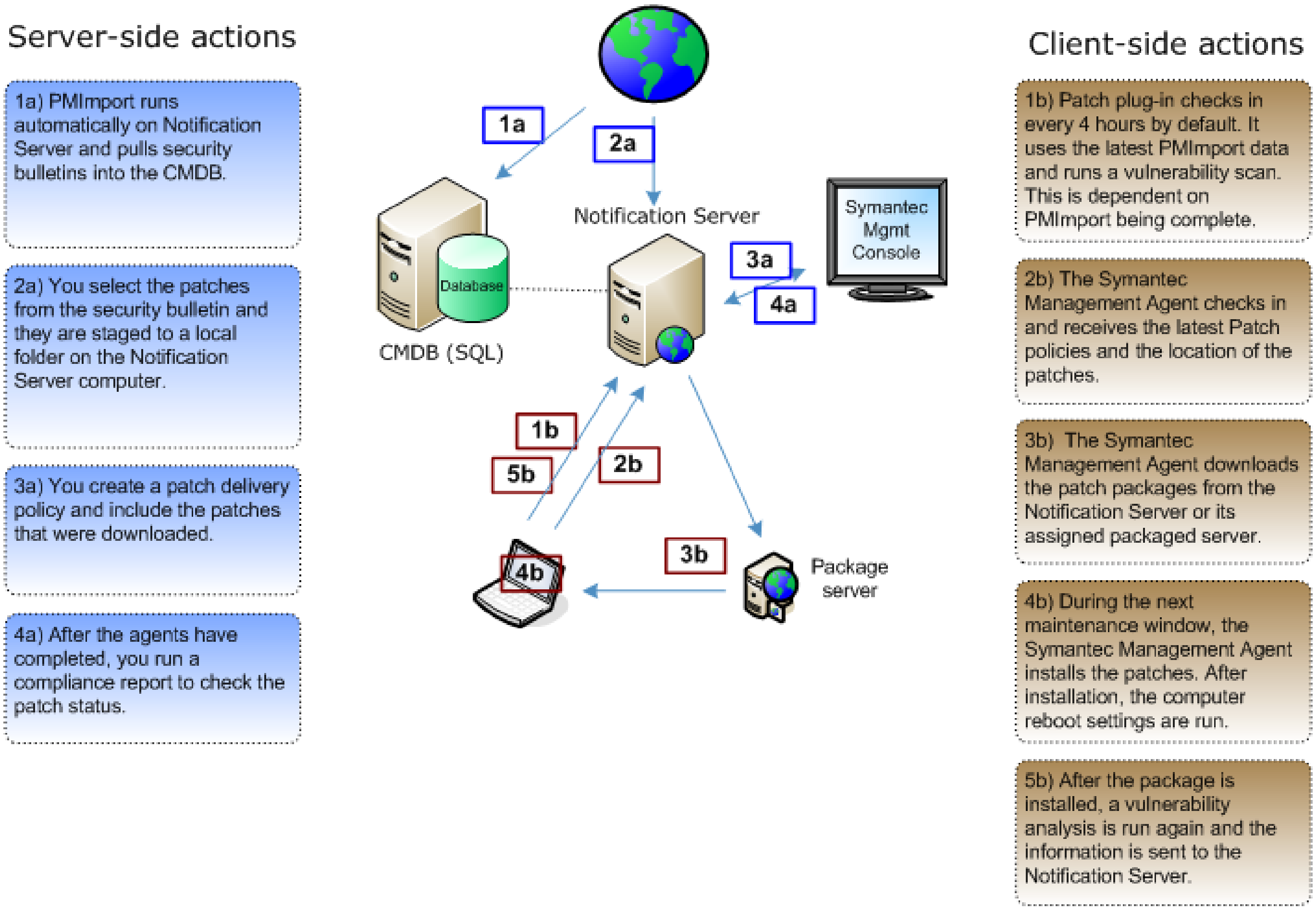
Once the patches are downloaded, the installation waits for the next scheduled maintenance window before it runs unless you set it to ignore the maintenance windows for zero-day exploits. Then it does the following:

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

After the patching completes the patch plug-in sends the updated vulnerability analysis to the Notification Server and stored in the CMDB. You can view vulnerability information from the Symantec Management Console with the compliance reports.

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

The following diagram represent some of the common data communications for Patch Management Solution:



Server-side actions

1a) PMImport runs automatically on Notification Server and pulls security bulletins into the CMDB.

2a) You select the patches from the security bulletin and they are staged to a local folder on the Notification Server computer.

3a) You create a patch delivery policy and include the patches that were downloaded.

4a) After the agents have completed, you run a compliance report to check the patch status.

Client-side actions

1b) Patch plug-in checks in every 4 hours by default. It uses the latest PMImport data and runs a vulnerability scan. This is dependent on PMImport being complete.

2b) The Symantec Management Agent checks in and receives the latest Patch policies and the location of the patches.

3b) The Symantec Management Agent downloads the patch packages from the Notification Server or its assigned packaged server.

4b) During the next maintenance window, the Symantec Management Agent installs the patches. After installation, the computer reboot settings are run.

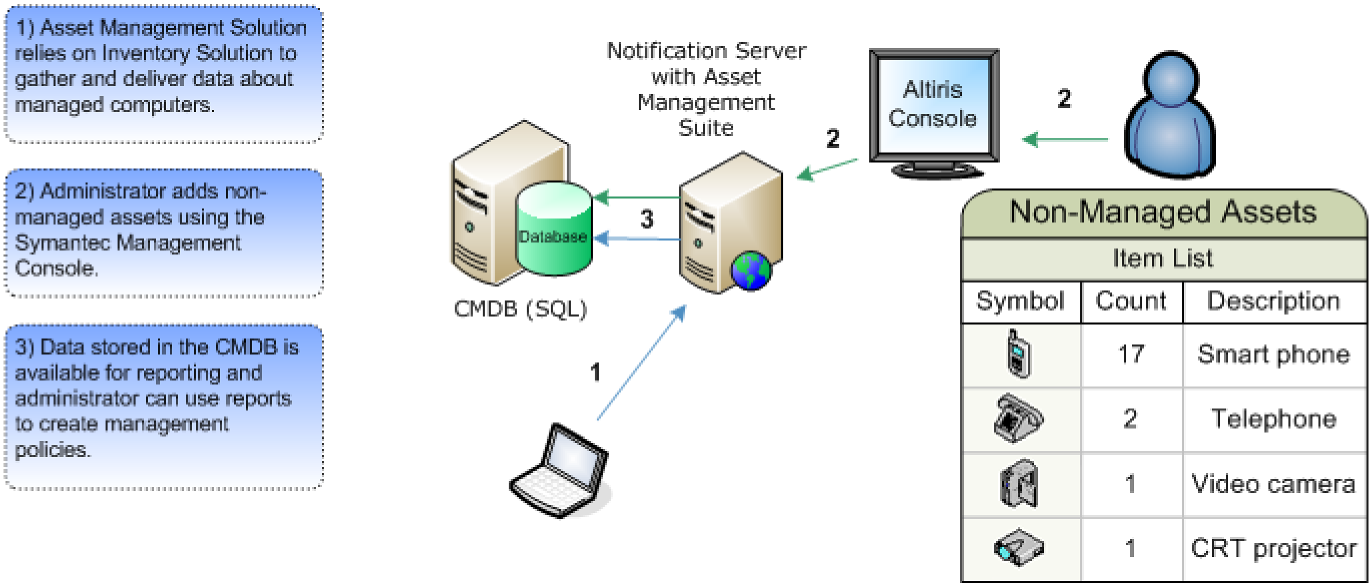
5b) After the package is installed, a vulnerability analysis is run again and the information is sent to the Notification Server.

Asset Management Suite data communications

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, Barcode 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 furniture and company cars.

The following diagrams represent some of the common data communications for Asset Management Suite system:



1) Asset Management Solution relies on Inventory Solution to gather and deliver data about managed computers.

2) Administrator adds non-managed assets using the Symantec Management Console.

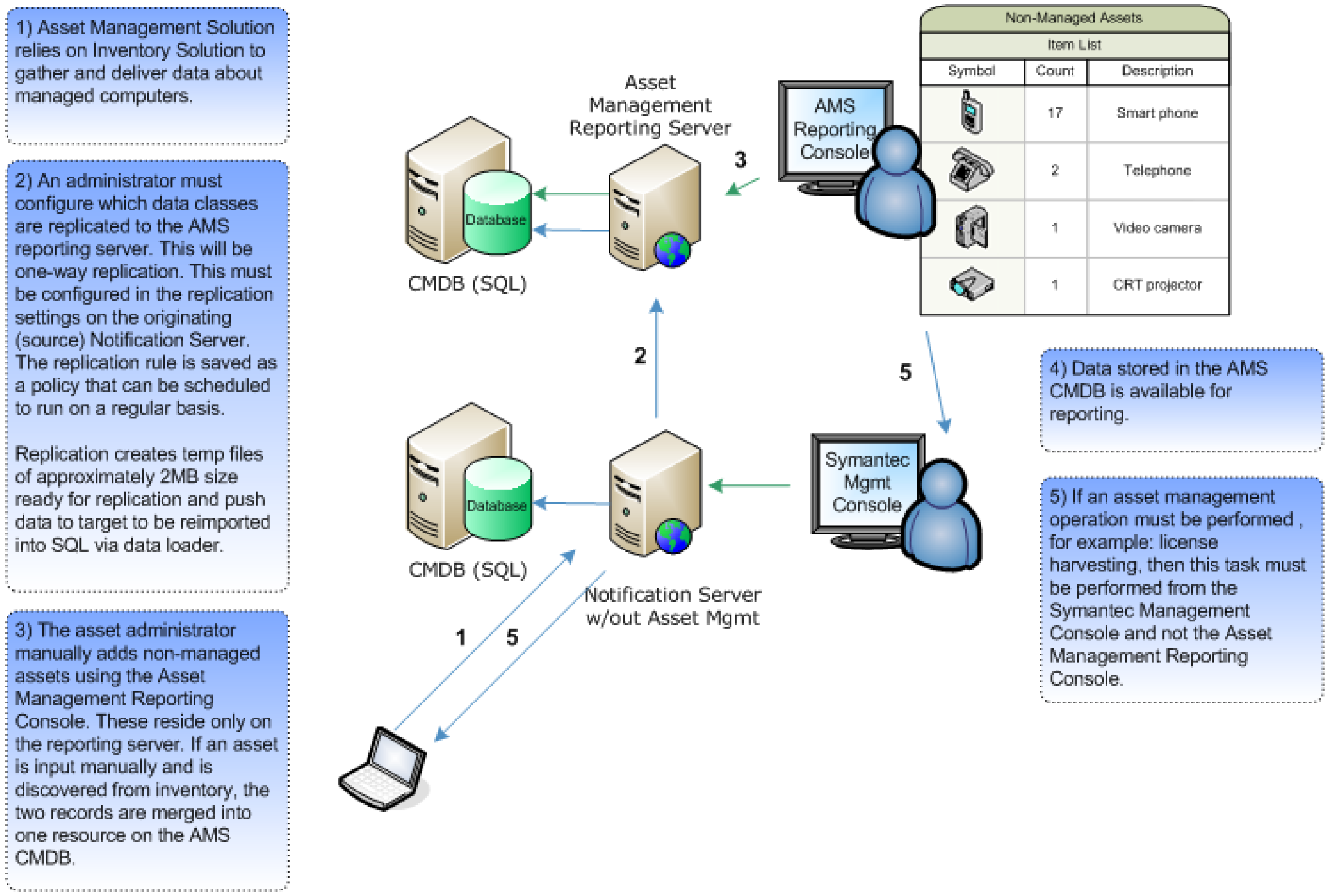
3) Data stored in the CMDB is available for reporting and administrator can use reports to create management policies.

Non-Managed Assets

Item List

Symbol	Count	Description
📱	17	Smart phone
☎	2	Telephone
📹	1	Video camera
📽	1	CRT projector

The following diagram represents some of the common data communications for an Asset Management Suite system that employs a dedicate Asset Management Reporting Server:



1) Asset Management Solution relies on Inventory Solution to gather and deliver data about managed computers.

2) An administrator must configure which data classes are replicated to the AMS reporting server. This will be one-way replication. This must be configured in the replication settings on the originating (source) Notification Server. The replication rule is saved as a policy that can be scheduled to run on a regular basis.

Replication creates temp files of approximately 2MB size ready for replication and push data to target to be reimported into SQL via data loader.

3) The asset administrator manually adds non-managed assets using the Asset Management Reporting Console. These reside only on the reporting server. If an asset is input manually and is discovered from inventory, the two records are merged into one resource on the AMS CMDB.

Non-Managed Assets

Item List

Symbol	Count	Description
📱	17	Smart phone
☎	2	Telephone
🎥	1	Video camera
📽	1	CRT projector

4) Data stored in the AMS CMDB is available for reporting.

5) If an asset management operation must be performed , for example: license harvesting, then this task must be performed from the Symantec Management Console and not the Asset Management Reporting Console.

Communication concepts of multiple Notification Server computers on the Symantec Management Platform

About hierarchy

Hierarchy is a method of organizing multiple Notification Server computers on your Symantec Management Platform. It lets you manage multiple child servers from a single parent server. You can maintain more consistent data, reduce human errors, and reduce duplication of resources and efforts by centralizing your management operations in a hierarchy.

A hierarchy uses parent-to-child relationships to define how information flows across multiple Notification Server computers. These relationships are called your hierarchy topology.

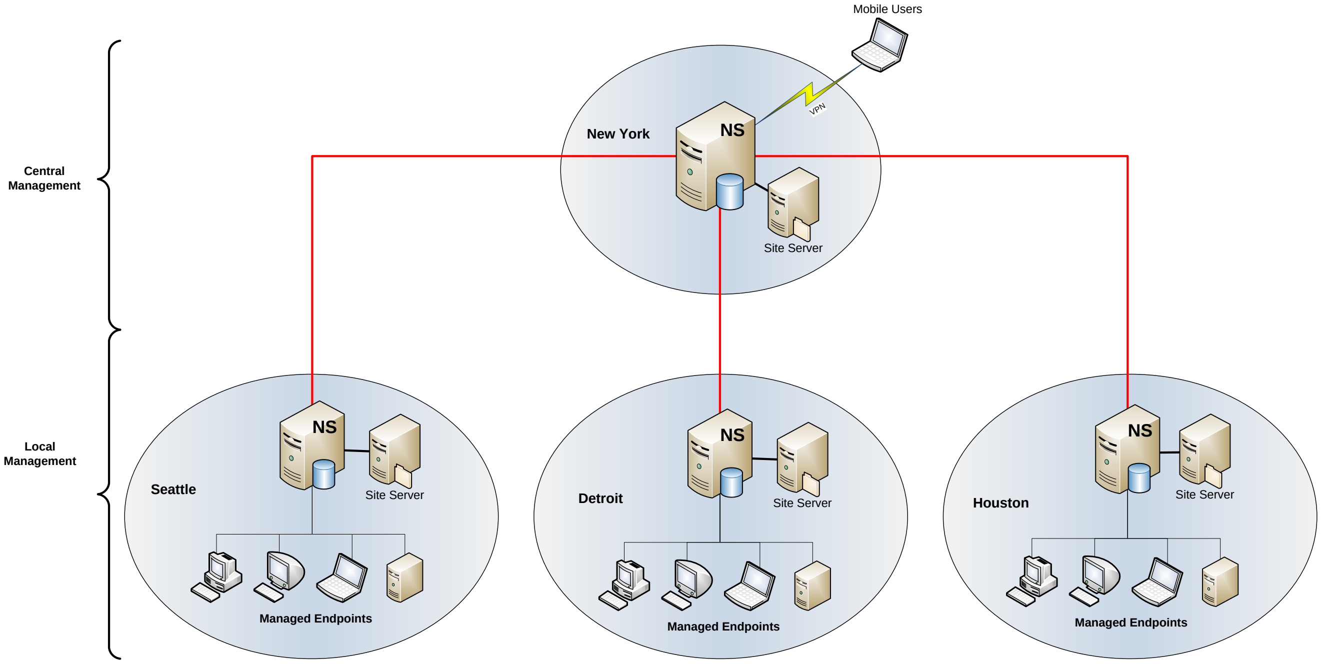
About hierarchy topology

The hierarchy topology is a set of one-to-on parent-to-child relationships between two or more Notification Server computers. Each Notification Server computer in the hierarchy can have multiple children servers but each child server may only connect to a single parent server. Each Notification Server computer is only aware of is immediate parent and its immediate children. The servers are unaware of peer members in the hierarchy.

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

When you set up the relationships of your hierarchy topology, you must add them two at a time. You must have administrative rights on both Notification Server computers. The relationships can be established from either the child server or the parent server.

There is a dedicated security role in the Symantec Management Platform for manipulating hierarchy topology settings like establishing relationships, editing schedules and configuring replication rules. Your administrators can force hierarchy to replicate individual items without being assigned this security role.



What you can do with hierarchy

Hierarchy lets you combine multiple Notification Server computers into a single Symantec Management Platform to increase the number of endpoints that you can manage from a single Symantec Management Console. However, hierarchy does not increase the number of endpoints that each Notification Server computer can support.

For example, you can replicate a software delivery policy. Replicating a policy also replicates the associated data such as a software package so that the software can be delivered to the applicable client computers of the child Notification Server computers.

In a hierarchy you can manage from both the parent Notification Server computer and the child Notification Server computers. Management from the parent server applies to all child servers. Management at a child server only applies to its endpoints and not all endpoints in the platform. This lets you combine both global management practices and regional management practices into a single platform. For example, a global policy can be distributed from the parent Notification Server computer to all managed endpoints, but regional administrators can also create policies that apply to their specific region.

Concepts of replication

There are two types of replication that are used in a Symantec Management Platform. These include the following types:

- Hierarchy replication - copies information between multiple Notification Server computers. It defines which items are replicated, the direction that each item type flows and when the replication occurs on each server in the platform. You can use replication to copy policies and tasks, and reporting information to other Notification Server computers. This form of replication is called "hierarchy replication."

- Peer-based replication - Another kind of Notification Server computer replication is “peer-based replication.” It functions differently than hierarchy replication. Peer-based replication requires 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 peer-based replication.

You can use both Hierarchy replication and peer-based replication concurrently within a single Symantec Management Platform environment.

About hierarchy replication

Hierarchy replication copies information between multiple Notification Server computers. It defines which items are replicated, the direction that each item type flows and when the replication occurs on each server in the platform.

Objects and data are constrained to only replicate in known directions to avoid conflicts. The data from the source server is always given priority and overwrites older versions of the data on the target server. The replicated data is read-only on the target server. This also applies for the items that are replicated up the hierarchy. Although the items are replicated as read-only by default, the policies can have the "hierarchy editable properties" (HEPs) that allow some settings to be edited at the child Notification Server computer. The HEPs must be configured on the parent Notification Server computer. The HEP that is currently implemented is 'enable/disable' of the policy. To change this setting, the administrator must edit the hierarchy properties on each policy, one at a time.

Each unique child server replicates with its immediate parent according to its own schedule. By default, the hierarchy replication schedule is every 24 hours. You should stagger the hierarchy replication schedule for each server to balance the load on the parent server. To estimate the how long each replication takes, you can check the event logs to see how long the regular replication events take and add a buffer. It is recommended to do this estimation after the initial replication, because the initial replication is a complete replication whereas the subsequent replication will be mostly differential.

Hierarchy replication does not affect any peer-based replication that you set up between two Notification Server computers independently of the hierarchy topology. The difference between peer-based replication, and hierarchy based replication, is that servers in a hierarchy topology have predefined definitions of the direction that each type of data flows.

About replication rules

Hierarchy replication relies on replication rules. These rules define the data that will replicate 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 will 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 - it is not deleted - and enable it again later.

Events are another item that 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. Table 1-1 shows the categories used to configure replication rules.

How hierarchy replication works

Hierarchy replication copies selected data from the parent server to its child server and from the child server to parent. It is neither realistic nor necessary to replicate all of the data in the entire platform. The default rules of hierarchy replication are unique for each solution. Only some items are enabled for hierarchy replication by default. Parent and child Notification Server computers are not mirror replicas of one another because replicated data is limited to only what is necessary for management and reporting.

The limitations of how much data you can replicate are evident with upstream replication. There are large amounts of data available that the platform can gather. For example, the level of detail that inventory solution can be configured to collect can over-load the parent Notification Server computer.

Hierarchy replication rules define if an item is replicated and the platform includes several rules by default. You can modify these existing hierarchy replication rules or create your own. To do this you must identify the data classes and resources in the CMDB that you want to replicate.

When you select which data to replicate, you do not need to specify the direction that the data replicates. Each Data type only flows in one direction. For example, policies, tasks, packages, and configuration settings flow downstream from the parent server to the children servers. The data classes that are needed for reporting flow upstream from the children servers to the parent server.

The following are commonly replicated objects and the direction that the data flows:

- **Configuration and Management Items** – Policies, tasks, filters, and reports are replicated as read-only items down a hierarchy.
- **Security** - Security roles, privileges, and permissions are replicated down a hierarchy.
- **Resources** - Resource information, such as computers, users, sites, and their associated data classes are replicated up or down a hierarchy.
- **Events** - Event classes, such as software delivery execution, are replicated up or down a hierarchy. There are no events that are replicated by default. To avoid overwhelming the parent server, event replication should only be done on a limited and temporary basis.

Replication can be initiated in two ways. Individual items, such as policies, can be replicated by right-clicking on the item and choosing "replicate now". If the option does not appear in the right-click menu, then the item does not support replication. You can also initiate replication through a schedule. Replication rules define items that replicate through the hierarchy according to the schedule. The default replication schedule is to replicate every 24 hours.

Requirements of hierarchy

Hierarchy can simplify the management of multiple Notification Server computers. However, having multiple Notification Server computers does not necessarily indicate that you should implement a hierarchy. Even if a hierarchy simplifies your administration, it will increase your Notification Server computer infrastructure overhead.

Consider the following before implementing a hierarchy:

- Three-tier hierarchies are supported, but two-tier hierarchies are recommended to minimize the overhead and to increase the replication speed.
- Typically you can have between one and twelve child Notification Server computers in a hierarchy. This number depends on the hardware capabilities of each server and your IT management requirements. For example, the frequency and amount of inventory that you gather impacts the number of clients each Notification Server computer can support. In a highly complex hierarchy scenario, you should contact Symantec Consulting services to analyze your requirements and fine tune the platform architecture to meet your needs.
- Hierarchy adds the cost of a Notification Server computer to act as the parent.
- Replication has some impact on the performance of all the Notification Server computers. This additional load on the child Notification Server computer may influence its maximum supported client count.
- There is a time-delay of replicating information.
- Network traffic must be routable between parent and child Notification Server computers.
- HTTP/HTTPS traffic must be permitted between parent and child Notification Server computers.
- Trust relationships must exist between the parent and child Notification Server computers or credentials for privileged accounts that facilitate trust must be known.
- Parent and child Notification Server computers must be able to resolve the name and network address of each other.
- There must be sufficient bandwidth between Notification Server computers to support package and data replication.

Design considerations of hierarchy

Consider the following aspects and requirements of hierarchy:

- Replicating more than once a day can have unintended consequences.
- Not all solutions in the Symantec Management Platform support hierarchy replication.
- All Notification Server computers must have the same versions of the Symantec Management Platform and Solutions installed. To determine the version of Symantec Management Platform software, you can open the Symantec Installation Manager locally on each Notification Server computer and note the versions. To perform Symantec Management Platform updates, hierarchy replication must be disabled prior to performing the update to avoid conflicts between dissimilar versions. You can easily enable or disable hierarchy replication on specific Notification Server computers with a single step. To perform Solution updates use Symantec Installation Manger locally on each Notification Server computer.
- You cannot get real-time data with hierarchy replication. There is a time delay when data is moved through the hierarchy. For example, if the default 24-hour replication schedule is used while distributing a software package, then up to 24 hours may be required for each tier in the hierarchy to deliver the software. Note, that individual items may be "replicated now" instead of waiting for the schedule.
- If clients are configured with SSL (HTTP or HTTPS) then their Notification Server computer must also be configured for it. Mixed SSL and non-SSL environments should not be supported. If one Notification Server computer has SSL then all of them must have it configured.

About site server architecture in a hierarchy

Hierarchy replication uses site services to operate. There must be a package server in each Notification Server computer site and this server must be off-box. You must offload package services on adjoining NS's to a managed device candidate capable of running package services. Ensure the site server running those services is "assigned" to a site or subnet NS belongs too before setting as a first step to setting up hierarchy.

There must be either a task server for each site or the task services must be enabled on each Notification Server computer. If you do not use Deployment Solution in your Symantec Management Platform, then it can be cost effective to use the task services on the Notification Server computer. However if Deployment Solution is used then you must use a dedicated computer for hosting both task and package services on each Notification Server computer site. If the task server is off-box you must manually configure site management to restrict all client computers to use the off-box task server.

Infrastructure sizing recommendations

Recommendations for small environments

A single server with the Symantec Management Platform (SMP) can support 500 managed endpoints. Small-scale environments can use SQL Express 2005 or SQL Server 2005 running on the same server. Several small-scale environments can be managed by a central server as part of a larger hierarchy. However, the top node system in a hierarchy should not use SQL Express.

In a small environment, you can install the Symantec Management Platform on a VMware ESX Server. If you use a VMware ESX Server for the platform, we recommend that you install SQL Server off-box on a physical computer. If you choose to host SQL Server in a virtual environment, then refer to Microsoft's Web site for supported virtualization configurations.

In a small environment, a typical installation without solutions can expect to have a database of approximately 500 MB. With solutions, the database can increase to 2 GB. Additional growth is dependent on the purging strategy and database maintenance plan for the SQL Express installation. Should database size become an issue with SQL Express, evaluate whether the event data class purging is aggressive enough. You should also evaluate the solutions that significantly contribute to disk consumption.

Hardware	Recommendation
CPU	2 Cores
CPU Speed	2.5 GHz
Memory	4 GB, DDR2
Cache	3 MB L2
Network	Gigabit
Disk	10 GB free. Mirrored 10,000 RPM SCSI or better.
OS	Windows 2003 Server Standard (32 Bit)
SQL	SQL Express 2005 or SQL Server 2005
	See Microsoft KB for optimal SQL configuration.

Memory recommendations for small environments

- **Small Environments:** Use the /3GB switch and SQL Maximum Server Memory is set to 1.2GB RAM.

Recommendations for medium environments

The first important scale-out recommendation is to move SQL off-box. A medium sized environment can still justify SQL Server on-box but attention needs to be given to ensure that SQL does not become disk I/O bound or that the service does not get memory starved by the SQL service. The task server intervals should be increased to at least 10 minutes. Also, if unusually large numbers or size of packages will be employed, such as deployment scenarios, then a site servers should be utilized.

When the Notification Server computer and SQL Server are on the same server:

Hardware	Recommendation
CPU	8 Cores
CPU Speed	2.4 GHz
Memory	8 GB, DDR2
Cache	6 MB L2
Network	Gigabit
Disk	10 GB free. 10,000 RPM SCSI or better with RAID 5 or 1+0.
OS	Windows 2003 Server Enterprise (32 Bit)
SQL	SQL Server 2005 on box.
	See Microsoft KB for optimal SQL configuration.

When the Notification Server computer and SQL Server are on separate servers:

NS Hardware	Recommendation
CPU	4 Cores
CPU Speed	2.4 GHz
Memory	4 GB, DDR2
Cache	8 MB L2
Network	Gigabit
Disk	10 GB free. 10,000 RPM SCSI or better with RAID 1, 5 or 1+0
OS	Windows 2003 Server 32 Bit)
SQL	SQL Server 2005 off box.

SQL Hardware	Recommendation
CPU	4 Cores
CPU Speed	2.4 GHz
Memory	8 GB, DDR2
Cache	8 MB L2
Network	Gigabit
Disk	10,000 RPM SCSI or better with RAID 5 or 1+0.
OS	Windows 2003 Server Enterprise (64 Bit preferred)
SQL	SQL Server 2005 on box.
	See Microsoft KB for optimal SQL configuration.

Memory Recommendations

- **Medium Environments:** When SQL is on-box ensure that PAE and AWE are enabled. If SQL is off-box ensure that AWE is enabled.

Recommendations for large environments

The recommended hardware requirements in a large environment are significantly higher than for smaller environments. In a large environment, you need to ensure adequate user performance, manage bandwidth, and expedite data loading processes. Remember that during installation when Symantec Installation Manager performs a readiness check, it does not verify that these requirements are sufficient for a large environment.

Note: We do not support running Symantec Management Platform on a virtual machine in a large environment.

In large sized environments consider creating site servers with Task & package services loaded and your SQL implementation off-box. The Agent configuration request interval should be increased to at least 2 hours.

NS Hardware	Recommendation
CPU	8 Cores
CPU Speed	2.4 GHz
Memory	8 GB, DDR2
Cache	6 MB L2
Network	Gigabit
Disk	10 GB free. 10,000 RPM SCSI or better with RAID 5 or 1+0.
OS	Windows 2003 Server Enterprise (32 Bit)
SQL	SQL Server 2005 off box.

SQL Hardware	Recommendation
CPU	8 Cores
CPU Speed	2.4 GHz
Memory	8 GB, DDR2
Cache	6 MB L2
Network	Gigabit
Disk	10,000 RPM SCSI or better with RAID 5 or 1+0.
OS	Windows 2003 Server Enterprise (64 Bit preferred)
SQL	SQL Server 2005 on box. (64 Bit Version)
	See Microsoft KB for optimal SQL configuration.

Memory Recommendations

- **Large and Very Large Environments:** Use AWE and PAE or use 64-bit SQL.

symantec.