Altiris 7

Planning & Implementation Guide

Version 1.1

27-Feb-09

Table of Contents

Date	***Version***	***Author***	***Changes***
25-Feb-09	1.0	Brian Sheedy	
25-Feb-09	1.1	Brian Sheedy	Formatting

1 Introduction

The Altiris 7 Planning and Implementation Guide provides capacity recommendations, design models, scenarios, test results, and optimization best practices to consider when planning or customizing an Altiris 7 Infrastructure for your organization. This guide identifies different facets of capacity planning and provides best practices for designing a scalable system specific to organizational requirements and management practices. This document will be updated continually as products are upgraded, test reports completed, and design practices refined.

Successfully implementing an Altiris 7 Infrastructure requires detailed planning. It is important that you understand the planning and readiness process. You must allocate appropriate resources and time to the planning phase. You must thoroughly document, and validate your plan in a test lab before you deploy Altiris 7 in your production environment. Proper planning can help you ensure the greatest return on your investment. You should not rush to implement management solutions, such as Altiris 7 or parts of Altiris 7 such as Client Management Suite or Server Management Suite.

Important: The design strategies and capacity guidelines in this document are provided as general recommendations when planning Altiris 7 solutions for your environment. Because of the many variables present when designing a management system, use the provided capacity numbers and recommendations only as baseline examples when customizing an Altiris 7 Infrastructure. Your requirements and results will vary depending on resources, configuration, and organizational model.

2 Altiris 7.0 Architecture Design

2.1 Overview

As the primary designer of an Altiris 7 Infrastructure, you will be asked many questions related to the technical implementation of the management platform and associated solutions. It is important to understand how to design such an infrastructure to best meet the needs of your organization. However, designing an Altiris 7 implementation is not nearly as simple as installing and configuring the software. Additional information is needed.

2.2 Where to Start?

It is the knee-jerk reaction to immediately deconstruct the architecture discussion into the technical pieces necessary to place components on the network and configure the software. Creating a design is the ability to optimally configure a piece of software or to tune an entire system for the optimal configuration for the environment.

However, the optimal configuration for an environment is not just a technical answer. It requires the careful assessment of the organization's business needs and constraints. These business requirements MUST factor into the final design. A technically well-designed infrastructure that does not meet the company's business needs is ineffective. It is the job of the designer to marry both the technical and business constraints of the environment into an architecture that is appropriate for your organization.

2.3 Architecture Design

When investigating an environment with the end goal of architecture design, keep these points in mind:

- The optimal Altiris 7 design will be a combination of business and technical factors.
- Designs will vary from organization to organization even if said organization has the same network topology and similar numbers of nodes.
- Designs must evolve over time; leave enough room for growth.
- Converse with various groups within your organization to understand the business needs and requirements for the architecture.
- Occasionally the business drivers and requirements will take priority over the best technical design

The remainder of this section will be devoted to talking about the technical aspects of the Altiris 7 architecture; however, do not lose sight of the fact that business requirements will play as much of a factor in the design as the technical components.

2.4 Symantec Management Platform

The Symantec Management Platform (SMP) 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, task management and Configuration Management Database (CMDB) data.

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. SMP is installed as part of a solution (the products that run on the platform) or suite (a group of solutions) installation, such as Altiris Client Management Suite or Altiris Server Management Suite. The platform provides the following services:

- Role-based security
- Client communications and management
- Event and scheduled task and policy execution
- File deployment and installation
- Reporting
- Centralized management through a single, common interface
- Configuration Management Database (CMDB)
- Computer and User-based Policy
- Client-side Maintenance Windows

2.5 Altiris 7 Components

In order to appropriately architect a solution for your organization, it is essential to know the individual components, also known as the building blocks that can be used as part of the solution. It would be impossible to discuss all of the solutions within the context of this guide; therefore, the discussion will be limited to the main solutions found within Client Management Suite (CMS).

These Altiris components consist of the following:

- Database Server
- Notification Server
- Site Server
  - Package Services
  - Task Services
- Altiris Agent
- Inventory Solution
- Software Management Solution
- Patch Management Solution

The above list is not meant to be an exhaustive list of technologies, but covers the most common components used in a CMS implementation. The descriptions of each component follow; these cursory descriptions are not meant to be exhaustive but to provide context for the architecture discussion.

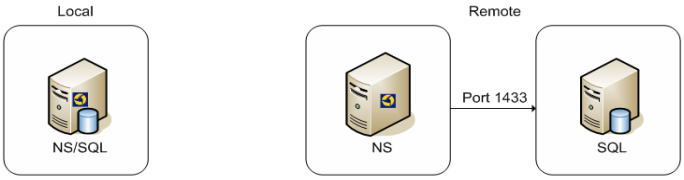
2.6 Database Server

The database server is the most critical component of the Altiris 7 Infrastructure. This component acts as the central data repository for the solution. Just about every solution uses the database server as a place to store configuration, task, job, and result information. Without the database server, Altiris 7 cannot be installed.

There are different database architecture options depending upon the solutions being utilized in the environment. Currently, Altiris requires a specific Relational Database Management System (RDBMS) in order to function. The specific database software versions than can be used as a data repository is as follows:

- Microsoft SQL Server 2005 (Standard, Enterprise, etc.)
- Microsoft SQL Express 2005

There are 2 general configurations for the database server when used with Notification Server. These configurations are as follows:



- **A local database server configuration** means the database server is located on the same machine as the Notification Server. This is the recommended configuration for small environments since there will be minimal contention of resources between the Notification Server and the database server.

- **A remote database server configuration** means the database server is located on a different machine from the Notification Server. This is recommended for larger environments since the workload of the database server can be offloaded from the machine handling the Altiris Agent requests. However, the database server and Notification Server must have a very high speed network connection between them (1GB Ethernet is recommended).

2.7 Notification Server

The Notification Server is the primary server component within the Symantec Management Platform installed in the Altiris 7 infrastructure and is responsible for coordinating the various solutions, providing the primary user interface, policy-based administration, reporting and notification. This server is complimented by Site Servers which extend the architecture and drastically improve distribution efficiency and reduce network bandwidth requirements. From the Notification Server Web-based management console, you can fully manage the components in your Altiris Infrastructure.

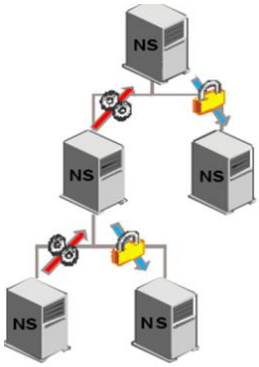
The Notification Server is responsible for managing the predefined policies and tasks that are available in each installed solution. These policies and tasks activate components of Notification Server that process and store inventory and asset data, trigger automatic actions, and complete many other tasks. Notification Server tasks include:

- Discovering resources on the network
- Installing and configuring the Altiris Agent on the endpoints
- Collecting client-reported information and storing it in the Notification Database
- Installing and configuring Altiris solutions from the Symantec Installation Manager
- Generating detailed Web Reports
- Sending policy information to the endpoints
- Distributing software packages

2.8 Notification Server Functions

2.8.1 Replication

Replication can be configured to replicate data outside the hierarchy structure, for example, by sending data to an external server that collates particular information for reports. Replication is the bi-directional transfer of data between two Notification Servers. Replication lets you replicate the following between Notification Servers:



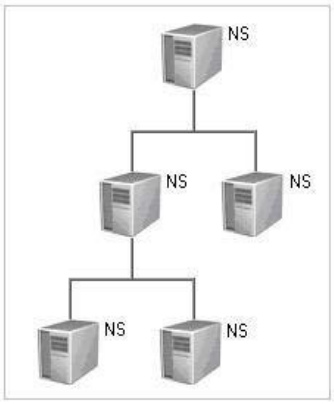
- Configuration & management items (reports, targets, policies, tasks)
- Resources, such as computers, users, and packages
- Events, such as Software Delivery Execution
- Security settings, such as roles, privileges, and permissions

Replication can be configured to replicate data to an external server that collates particular information for reports. Ownership is not applied to replicated items so Notification Servers are able to overwrite data that has been replicated down from the parent Notification Servers. All replicated data can be edited on the destination Notification Servers since ownership settings are not applied

2.8.2 Hierarchy

Hierarchy is a technology designed to reduce the total cost of ownership (TCO) of managing Altiris software and solutions across multiple Notification Servers. Hierarchy reduces the TCO by supplementing the Notification Server system with centralized management capabilities. Hierarchy uses replication to copy and synchronize shared objects and data between Notification Servers within the same hierarchical structure. At scheduled intervals, each server within a hierarchy synchronizes objects and data with its immediate parent and immediate children.

Hierarchy defines the information flows across multiple Notification Servers in an enterprise. If you have multiple Notification Servers, you can use Hierarchy to define collections of Notification Servers that share common configuration settings and data. Hierarchy can distribute and synchronize any changes that are made to the shared configuration settings and data.

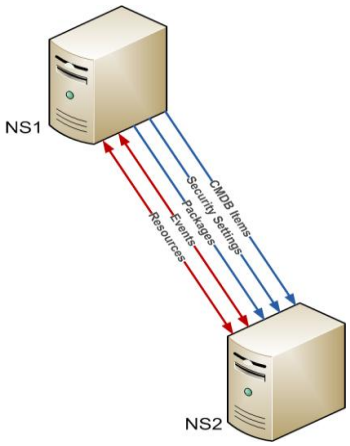


This lets you manage your Altiris solutions across multiple Notification Servers from a central location. Some solutions, such as Inventory Solution, Patch Management Solution, and Software Management Solution, are set up to participate in hierarchy.

Both Notification Servers must have a package server available within their respective sites. The package server is required for performance reasons. You cannot create a hierarchical relationship between two Notification Servers if either one does not have a package server available.

2.8.3 Replication within Hierarchy

When you add a Notification Server to a hierarchy topology you can specify what to replicate to the parent Notification Server and to any child Notification Servers. Hierarchy uses the replication services to synchronize all data items by their GUIDs, so anything that was published on a child Notification Server cannot be overwritten by data replicated down from its parent.



Replication of resources and events within a hierarchy topology is configured using replication rules. These rules define the data that you want to replicate to other Notification Servers. You need to create all the rules that you require, and then enable those that you want to use. You can disable a replication rule at any time—it is not deleted—then enable it again later.

Replication rules can be replicated down or up the hierarchy topology. You can set up your replication rules at the root level Notification Server and then replicate them to all child levels. You may want to do the same for security roles and privileges.

Lower-level Notification Servers cannot change the replicated security items or replication rules, but they can add new ones when necessary. Any new security items or replication rules would apply only to the local Notification Server, but they could be replicated down.

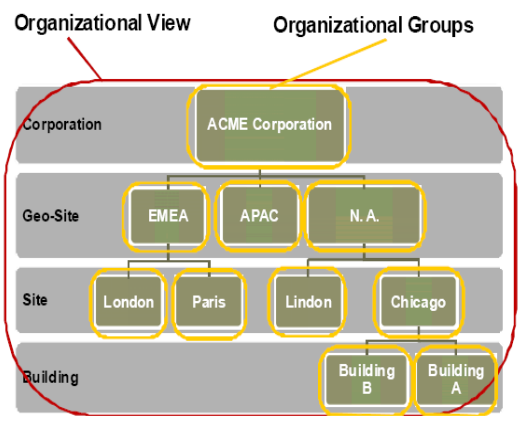
2.8.4 Resource Scoping

Resource scoping provides a secure means of segregating resources into manageable, well structured units. These units are generic in nature so they can be arranged to suit a wide variety of organization's organizational requirements, as well as being securable with the familiar NT security inheritance model that is currently in use throughout the Notification Server.

Resource scoping provides the following:

- **Logical partitioning of resources into structures** (organizational groups) consistent for use in administrative management tasks. One of the primary goals of resource partitioning is to simplify the user experience when administering various managerial activities in the Notification Server. The ability to create and extend organizational groups provides a way for organizations to customize their system to suit their particular requirements.
- **A consistent way of enforcing security on resources**. Unlike previous versions, there is no longer a disjoint way of securing resources throughout the Notification Server. Rather than securing both standard collections and resource folders, security can now be applied at a single location on the organizational groups.

Organizational Views let you group a particular type of resource into a hierarchal organization of groups (called Organizational Groups) for management and security purposes. The hierarchy can be one or multiple levels deep. The number of levels depends on the number of resources of a particular type you have, how you want to manage security on the resources, and other needs of your organization. For example, you can create an organizational view for locations. This view can be divided into organizational groups for different countries; the countries can be further divided into organizational groups for sites.



Resources are added to Organizational Groups and cannot be added directly to an Organizational View. Notification Server includes a predefined Organizational View named Default. This group includes all of the predefined resources. You can use this view, but this view cannot be edited.

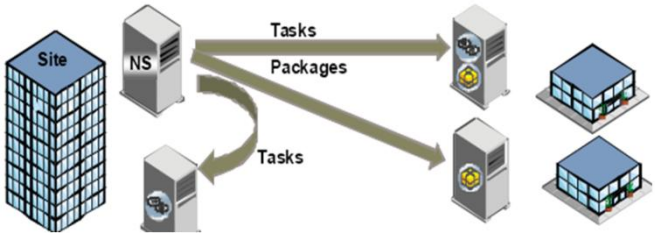
You can create additional views. A resource can be included only one time in a particular organizational view but can be in multiple Organizational Views. Departments, cost centers, and locations are examples of common Organizational Views.

You can use Organizational Groups to specify the resources that a task or policy applies to. When an Organizational Group is selected, all of the resources within the group (along with all of the resources within the groups that are within the selected

group) are also selected. You can assign security roles to Organizational Groups. Security roles provide the users in a security role with access to the resources in that group (and to all groups that are children of that group).

2.8.5 Site Management

Site Servers use middleware components installed on computers other than the Notification Server, and act as the first point of contact for the Altiris agents, thus reducing the load on Notification Server. The official name for any Altiris middleware component is “Site Service”. Any computer that hosts a site service is known as a Site Server. A site server can have one or more site services installed on it. For example, if you install the package server site service (usually referred to as the "package service") onto a computer, that computer becomes a site server.



Altiris Site Servers with the Package Services option enabled act as local file servers for devices that have the Altiris Agent installed. A package is defined as a collection of files, scripts or a command line that is created by Software Management Solution that must be delivered from the Notification Server to the client. When the administrators enable packages on the Notification Server, the packages are replicated to all of the Site Servers that are known by that Notification Server.

Once the replication is successful, Altiris Agents attempt to download these files from the Site Server instead of the Notification Server. This helps reduce the load on the Notification Server and helps to reduce network traffic by allowing the package to replicate once per site. Altiris Site Servers with the Task option enabled provides task sequencing and automation for Altiris solutions. The functionality is similar to what Altiris Deployment Solution software provides with its Job engine, but it is built on the Notification Server infrastructure allowing the rest of the Altiris solution catalog to take advantage of its powerful features, such as:

- Executing multiple Tasks in a defined sequence called a Job
- Letting users provide logic to handle task errors or other return codes
- Including powerful command line and VBscript capabilities
- Providing out-of-the-box Power Management task
- Supporting executing client-side and server-side tasks
- Providing instant gratification features such as “Run Now” options with status feedback
- Letting tasks be reused in multiple Jobs or cloned and modified as desired

The Task Service is very lightweight and can work concurrently on a Site Server with Package Services enabled. As Altiris solutions release updates to their own default tasks, the Task Server service will become more powerful, letting you create jobs that allow solutions to work together to accomplish complex tasks. The Task Service lets you distribute your jobs and tasks to different computers on your network where Altiris Agents reside. Distributing jobs and tasks reduces the load on the Notification Server and reduces network traffic, since the Altiris Agent accesses the closest Site Server to it for job and task downloads.

2.9 The Altiris Agent

The Altiris Agent enables communication between the Notification Server and managed computers. The Altiris Agent is pushed or pulled from the Notification Server and installed on Windows-based computers (there is a separate Unix Linux and Mac Agent for non-Windows-based computers installed during Solutions installation which acts in a similar manner as the Altiris Agent for Windows computers. The Altiris Agent waits for instructions and configuration settings from the Notification Server, and sends collected information back to the Notification Server for processing and storage.

All communication starts with the Altiris Agent, including downloading files and packages from the Notification Server (or Site Server), updating configuration information, and any other task necessary to keep managed computers up-to-date. The Altiris Agent is responsible for all communication between the managed computer and the Notification Server. There are many beneficial configuration options that can make your Altiris 7 implementation more efficient, features such as:

- **Bandwidth Throttling:** Bandwidth throttling is a method of ensuring the Notification Server limits ("throttles") the number of requests it responds to within a specified period of time. Bandwidth throttling provides quality of service (QoS) by limiting network congestion and server crashes. The Altiris Agent includes settings that let you specify how and when to throttle information being passed between the managed computer and the Notification Server.
- **Checkpoint Recovery:** Checkpoint recovery is a common technique for imbuing a program or system with fault tolerant qualities. It allows systems to recover after some fault interrupts the system, and causes the task to fail, or be aborted in some way. Example: If a computer loses connection with the server while downloading a software package, the next time that computer connects the download starts where it left off. All packages downloaded through the Altiris Agent use checkpoint recovery.
- **Package Multicasting:** Multicasting deploys packages simultaneously to a select group of computers and improves Site Server performance on large networks by making a managed computer the master of a multicast. The package is sent to the master computer a portion at a time. Each portion is then forwarded to other managed computers using multicast technology.

  This reduces the load on Site Servers by reducing the number of Altiris Agents that connect to a single Site Server. Multicasting can reduce WAN traffic in remote sites that do not have dedicated Site Servers. Only the first managed computer to download the package actually gets the package across the WAN (this computer becomes the master computer). Other managed computers at the same site download the package from the master computer using multicast.

2.10 Inventory Solution

Obtaining and analyzing accurate inventory data is an important part of managing and securing your network. Inventory Solution lets you gather inventory data about computers, users, operating systems, and installed software applications in your environment. Inventory tasks are easily configured and managed using a central Web console. After you have gathered inventory data, you can analyze the inventory data using pre-defined or custom reports. The inventory data is stored in the Altiris CMDB. This provides a central store of data that can be utilized across the Symantec Management Platform.

To help maximize your investment, Inventory Solution goes beyond simple data gathering. By providing a Web-based management console, policies to alert you about critical information, and professional quality Web reports, Inventory Solution includes the tools you need to transform your inventory data into useful information. Inventory Solution also:

- Supports zero-footprint configuration
- Operates in always connected, sometimes connected, and stand-alone computing environments.
- Can be installed to run on a recurring basis in conjunction with the Altiris Agent.
- Posts data through SMB and/or HTTP

You can use the application metering feature within Inventory Solution to monitor the use of and control the availability of applications on managed computers. You can meter applications that are running on Windows-based managed computers. When metering applications, you define the applications you want to monitor or deny by creating application definitions. The rules for metering applications are controlled through Notification Server policies. The Application Metering plug-in, which runs within the Altiris Agent on the managed device, enforces the properties of the policies. An Application Metering policy can meter one or more applications.

You can use the Application Metering features of Inventory Solution to do the following:

- **Discover applications:** Records the first time an application starts. This lets you identify the software, including the version, that is used on managed computers. After applications are discovered, you can use this information when you create monitoring policies.
- **Monitor Specific applications:** You can create policies to monitor applications that do the following:
- **Monitor Activity:** Track when an application is started, stopped, or both to determine duration.
- **Deny Usage:** The use of the application can be denied and can have a denial event sent to the Notification Server
- **Harvest unused software licenses:** Determine which applications are not being used so you can reuse licenses elsewhere.

2.11 Software Management Solution

Altiris Software Management Solution provides secure, bandwidth-sensitive distribution and management of software from a central console. The product intelligently leverages known relationships that are defined in the Altiris Definitive Software Library to ensure that the correct software gets installed, remains installed, and can operate free from interference from other software. Software Management Solution also lets end users directly download and install approved software or request other software.

Software Management Solution integrates with the Software Catalog and the Software Library that are defined in Software Management Framework. This integration lets your administrators focus on delivering the correct software instead of defining the packages, command line, and so on for each delivery. Software Management Solution combines the functionality of earlier versions of Software Delivery Solution, Application Management Solution, Wise Integration Component, and Wise Toolkit.

Software Management Solution works in conjunction with Notification Server and the Altiris Agent to define and deploy software packages and run programs. Programs can be run once or based on a schedule. To deploy a package, which consists of any collection of program files, start by using the Altiris Console to define a package. Once the package has been defined, create a Software Delivery task to deploy the package and to run programs within the package. The Software Delivery task also specifies when a program is to run, the security context used when a program is run, and the collection of computers to which the Software Delivery task applies.

2.12 Patch Management Solution

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

Key features include a comprehensive software repository that automates downloads from the vendor site before distribution without administrator intervention. The repository provides comprehensive data on software bulletins, software updates, inventory rules, technical details, severity ratings, and number of executables. The process of populating the information repository from the Microsoft Patch Management Import files starts after installation is complete.

To reduce labor, the software update agent automatically analyses managed computers and gathers patch-specific inventory for determining supported operating systems, applications and the associated service pack level, and whether a patch is required or not. Inventory results populate predefined collections based on the returned data. The software update task wizard automatically assigns software updates to computer collections that need them. The wizard also simplifies the management of distribution tasks, so instead of creating a task for each individual software update, you create a single task for the relevant software bulletin.

You can automate all or part of the entire patch management work flow, from downloading new software updates to distribution to managed computers. Integration with Notification Server 7.0 includes features such as hierarchy and maintenance windows, that let you configure patch management features and settings for a single notification server, then pass those settings down to any child notification servers. Patch Management provides the following benefits:

- **Proactive Management** – Assess your vulnerabilities and deploy the appropriate patch automatically.
- **Centralized Patch Assessment** – View and manage all your patches from one easy to use web interface.
- **Comprehensive Patch Assessment** – Patch Management provides the ability to automatically assess vulnerabilities in Windows Operating Systems and hundreds of applications.
- **Targeted Distribution** – Choose which computers the patch will be applied to.
- **Automated Patch Distribution** – Support for LAN/WAN, remote, or occasional connections are included, as well as bandwidth throttling, state management to ensure the patch stays applied, and the ability to pick up the download of the patch if it is interrupted.
- **Flexible tracking and reporting --** Patch Management Solution includes a variety of Web Reports that summarize which patches are available, identified vulnerabilities, and the status of distributed patches.

3 Environmental Factors Influencing Architecture

As mentioned previously, there are a number of factors in every environment that will impact the final design and architecture of the Altiris infrastructure. These factors include both technical and business requirements that must be balanced in the design process.

There are times when the business requirements will override the technical "best practices", and it is the designer's job to know when this might occur. For example, there might be some business needs that drive a 5,000 node environment to a three (3) Notification Server configuration. Such an environment can easily be managed by a single Notification Server from a technical perspective; however, there may be a compelling business reason to go against the technology best-practice.

The above example is certainly an extreme case; however, it is not outside the realm of possibility. But most of the time the designer will be able to use the technical constraints as the backbone of the solution and adapt it to the business requirements. The most common factors that influence the Altiris infrastructure architecture are included in the list below. This list is not meant to be an exhaustive one. There are many more factors a designer should consider as part of the design process.

- Network bandwidth and topology.
- Network security requirements.
- Managed node count.
- Installed and actively used solutions.
- Concurrent use of the Altiris Console.
- Proportional component cost.
- Organizational structure.
- Future Growth.

3.1 Network Bandwidth and Topology

Network bandwidth and topology is one of the bigger factors in Altiris infrastructure design. The architect needs to be able to identify the organization's WAN links, to assess the bandwidth of those WAN links, and to assess the impact of Altiris traffic on those WAN links. A misaligned architecture can cause severe degradation of network performance for the organization. The following points should be considered and implemented when designing an Altiris infrastructure to accommodate the WAN links:

- Locate the core components (i.e., Notification Server and Deployment Server) in the organization's central network location. This will be the hub location in a standard hub and spoke network topology.
- Site Servers at remote network sites to lessen the impact of package download traffic associated with Software Management Solution and Patch Management Solution
- Utilize Site Servers for image distribution when using Deployment Server.
- Use Altiris Agent bandwidth throttling to control the amount of traffic on the WAN links.
- Configure individual solution agents to utilize the network at non-peak hours.

3.2 Network Security Requirements

Network security is taking a front-seat in the design process since many organizations are looking to make their infrastructures more protected against unauthorized access. Different organizations will have different levels of risk aversion when it comes to security, which means there may be some very interesting design discussions in high-security environments.

Some points to consider around network security are listed below. This list really represents a minimal security discussion; however, it will provide a starting point for you:

- Look for data communications encryption requirements (i.e., SSL) in the organization.
- Identify any communications port restrictions that are enforced across the enterprise.
- Determine firewall location across the network, as these appliances will dictate component placement for the Altiris infrastructure.

Using SSL to encrypt traffic on the network will affect the number of nodes that can be managed by the Notification Server. This is due to the CPU utilization necessary to perform the encryption and decryption functions. Look to off-load this processing onto SSL hardware appliances, if possible.

You will also need to consider the implications of "punching holes" in the organization's firewalls. Consider placing components around the firewalls to accommodate the network security requirements and minimize the amount of communication through these points. The vast majority of CMS solutions will work well through a firewall assuming it is configured properly. Investigate these more complex solutions to see if they can be accommodated through the existing firewall policies.

3.3 Managed Node Count

The managed node count will clearly impact the number of components required to build the infrastructure. It will also impact the placement of those components based upon the node distribution on the network.

Remember that each Altiris component has a recommended maximum managed node count. Avoid exceeding these recommended maximums. See ***Section 6.3.3*** for recommended specifications

3.4 Installed and Actively Used Solutions

The number of installed and actively used solutions will affect the above mentioned limits. For example, a Notification Server with only Inventory Solution installed can exceed the 25,000 managed node limit. This is due to the fact that Inventory Solution does not pose a large load on the Notification Server.

Conversely, a Notification Server with all CMS 7 solutions installed that are also heavily used may experience performance issues long before it reaches the 10,000 managed node limit. This may be due to how the solutions themselves are configured or being used. There are no concrete recommendations to be made around the design point, but the designer will be able to gauge the impact of this design point with appropriate experience and exposure to the solutions.

3.5 Concurrent Use of the Altiris Console

Many of the recommendations made in this section are made using the assumption that there is not a lot of additional processor utilization required through heavy use of the Altiris Console. One of the powerful features of the Symantec Management Console is the ability to create custom reports that can be used by administrators to view information about the environment.

However, many of these custom reports are written with advanced Structured Query Language (SQL) statements that require significant database processing power. Having many people run these reports concurrently on the Notification Server can severely degrade its performance.

If the organization requires heavy custom reporting, consider implementing a separate Reporting Notification Server to satisfy this requirement. While it does mean the organization needs to invest in an additional server, it will provide for the separation of duties in the infrastructure. The Notification Server responsible for managing end-nodes will be able to dedicate its processing to that function. The Notification Server responsible for providing reports will dedicate its process to that other function.

In this configuration, replication should be used to send the resource inventory information from the agent-facing Notification Server to the Notification Server responsible for reports or in the case of a centrally managed model, from the highest parent in the hierarchy. Another consideration is the memory cost of each of the concurrent Altiris 7.0 console sessions from IIS on the notification server. This memory requirement can be calculated at about 20MB per console connection and subtracts from the Notification Server's available memory.

3.6 Proportional Component Cost

It is the designer's job to balance the technical needs with the business needs of the infrastructure. Therefore, the designer should work with the organization to ensure the infrastructure components are in line with the organization's budget and planned investment. Based upon the server sizing guidelines in the previous section, it is easy to see the Notification Server will likely be the most expensive component to the infrastructure. This is followed by the Deployment Server. The remaining components (Site Servers with Task, Package or OOB Services) can likely be deployed on existing hardware already deployed in the organization environment.

Consider how to balance the investment in new hardware with the re-appropriation of existing hardware already owned by the organization. Also consider methods for leveraging less expensive components rather than more expensive ones. For example, imagine a simple hub and spoke network topology with 500 managed nodes at each

remote WAN location. One possible solution might be to locate a Deployment Server at each remote site to minimize the impact on the WAN. This is a valid solution.

However, another solution would be to centralize the Deployment Server and use Site Servers at each remote location to act as the main image distribution point. Both architectures are technically sound, but the Site Server solution represents less cost to the organization in hardware due to the proportional component cost.

3.7 Organizational Structure

The organization's organizational structure may dictate the component placement and design of the infrastructure as much as the technical factors. This is due to how the organization's staff works on a daily basis and how the business process is established. Consider the following points when reviewing the organization's organizational structure:

- Different groups and roles managing end-nodes may require Notification Server role and scope based security, which poses additional server load on the Notification Server.
- Different branches of the organization may be managed separately giving rise to distinct NS management domains.
- Security requirements may dictate separate management domains.
- Different geographical regions may dictate separate management domains.

Consider the use of resource scoping with organizational views and groups or in some cases, additional Notification Servers to accommodate the organization's organizational structure, if necessary.

3.8 Future Growth

A good architect will always provide room for growth in the design. The architecture should reflect the current organization and the vision for the organization for the next 3 years, if possible. Designing an infrastructure to accommodate this is a tall order for any architect; consider these points when dealing with future growth:

- Leave enough room for growth on the components to accommodate business evolution. Try to understand the organization's business needs and project those needs out into the future.
- Avoid approaching node count ceilings on core components by introducing multiple components to balance the load.
- Always have a plan for evolving the architecture in the design.

4 Common Design Models

To design and optimize an Altiris 7 infrastructure, you will need to understand organizational features and requirements such as SQL server resources, security policies, network infrastructure, and other environmental settings and variables. For most organizations this will require a basic assessment of the environment:

- **Assess your site environment and resources.** Evaluate your system infrastructure, including network resources, operational processes, management reporting needs, administration requirements of the IT department, and other pertinent aspects of IT resource management.
- **Identify opportunities and challenges for automating procedures and easing problem areas.** Prioritize your needs and integrate Altiris 7 solutions to optimize a comprehensive design for present and future needs. It is a good time to assess and confirm your IT management goals.
- **Implement a system by first setting it up in a test environment** before migrating the Altiris system to the production environment.
- **Test capacity, bandwidth usage, and the general health of you management system** using Altiris 7 load testing and reporting tools to optimize your configuration and define management priorities specific to your environment.

Use this section to get a basic understanding of solution components and infrastructure requirements for the design models in your organization. Then devise and implement a strategy specifically for your needs based on these suggestions. In general, this design and optimization guide allows you to extrapolate required settings and configurations for your specific needs. It introduces major issues that administrators face based on general design models and suggests management strategies for implementing a solution or combination of solutions for each model.

To provide comparable data for optimization and scalability practices, example scenarios of organizational types are used throughout this section to standardize environmental variables and provide a structure for baseline statistics. Generic organizational models are used to reference standard practices and illustrate common problem areas for each solution or suite.

4.1 General Design Models

To better provide planning and optimization recommendations specific to your environment, this guide uses standard design models to identify and list advantages and problem areas that administrators may encounter in installing and operating an Altiris 7 system. These basic design classifications include:

- **Large Enterprise model.** This includes sites with 10,000 or more managed computer devices, generally distributed with numerous mobile users.
- **Small to Medium Business (SMB) model.** This includes sites with 99 to 9,999 managed computer devices, moderately centralized with few mobile users.

4.2 Large Enterprise Models

The following challenges and requirements characterize large enterprises:

- Shared resources
- Staff is segmented and specialized
- Hardware is shared
- Altiris system must integrate and operate with other vendor solutions
- IT team requires adoption buy-off from multiple groups

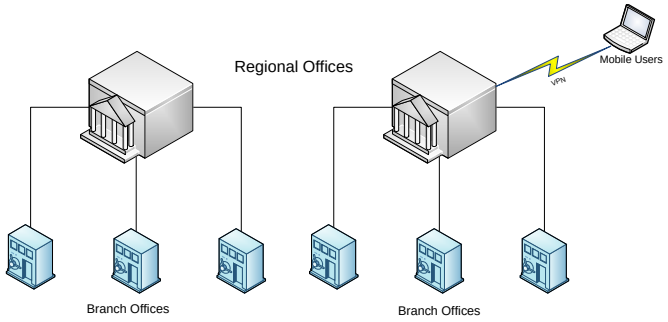
4.2.1 Centralized or Decentralized Management

Management of distributed or centralized systems refers to the IT management structure in place. If an organization distributes management to local IT administrators, then they may require more Notification Servers or Site Servers than strict capacity guidelines dictate. In dealing with these operational challenges a number of considerations must be made, such as:

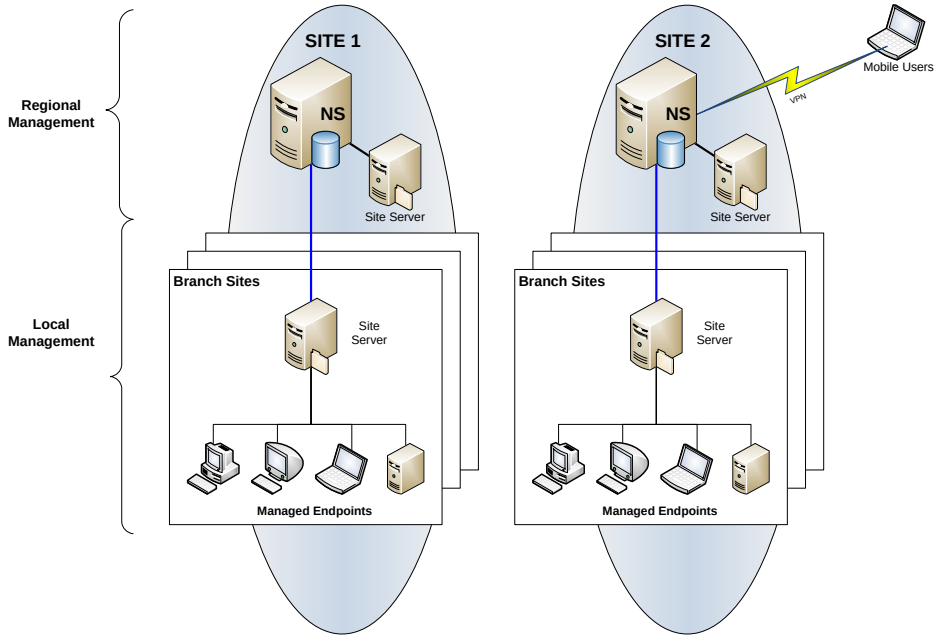
- **Scoping the range of management functions.**
  - What is owned centrally vs. at the site?
  - How many levels – Tier 1- N?
- **Determine all Connectivity ranges.**
  - Tier 1 sites well connected and tier 2 sites may be poorly connected.
  - Traveling users may dial in or VPN from different locations.
- **Central Management** can ease correlation of information from the notification servers but it also creates a single point of failure.
- **Decentralized Management** can be a source of inconstancy but it can be a more resilient option.
- **In a large enterprise model it is usual to have elements of both,** with their combined benefits and drawbacks. For example:
  - Who should be responsible for managing notification servers, site servers, databases and other operational items?
  - Who should receive status information and at what levels?
- **Often a regional or local group can take care of issues on their own level**, but there are times when central management is more effective for company governance and mandated tasks.

4.2.2 Distributed Model for Large Enterprises

The distributed model (sometimes called the "fan out" model) consists of dispersed sites or network segments supporting subordinate sites or network segments. This model provides network load balancing for companies with equally distributed locations.



The distributed model has direct management through both Notification Server and Altiris 7 solutions for day-to-day management of local computers from both regional and local branch offices.



Notification Servers: A Notification Server will be located at each regional office:

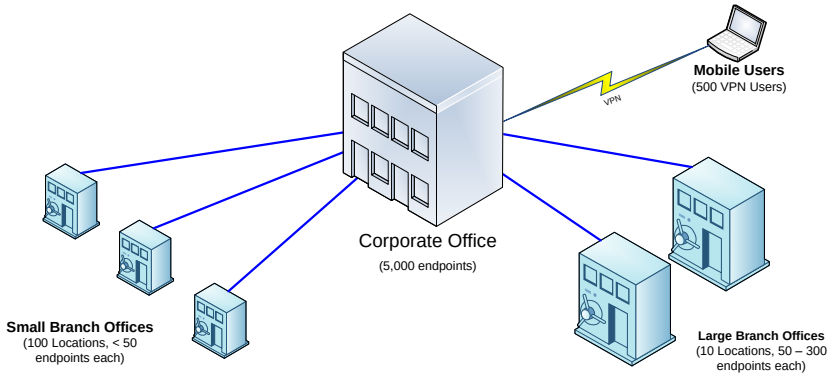
- Each Notification Server has its own database, although these databases can exist on a common Microsoft SQL Server provided they are placed in individual instances.
- Mobile users will access a Notification Server at designated regional offices.
- Software Delivery Solution will be the primary method of package distribution

Site Servers: Site Servers will reside in each branch office.

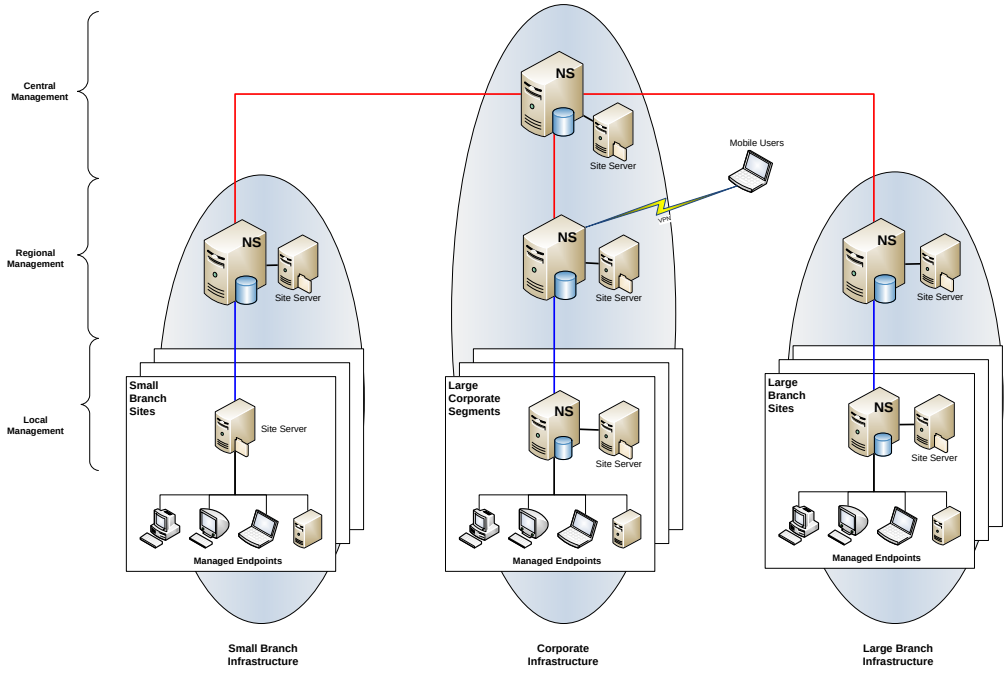
- Packages will be automatically distributed to the Site Servers from the Notification Servers
- Clients will access packages from the closest Site Server.

4.3 Centralized Model for Large Enterprises

The centralized model provides direct management from regional offices with regional Notification Servers and also allows reporting and management at a central office using a central Notification Server. In many cases it consists of a corporate office with thousands of managed computers, large branches with more than 50 managed computers, small branches with less than 50 computers, and remote access users.



Multiple design scenarios are possible for large enterprises using a multi-tier reporting model. In most cases, this model includes a main campus, small and large remote locations, and itinerant users that connect across the WAN. The following graphic represents a multi-tiered approach for a large enterprise to manage resources and generate reports, providing regional and corporate management across the WAN and local management across the LAN.



Hierarchy of the Centralized Model

Altiris 7 supports a hierarchy of Notification Servers and Site Servers to integrate and scale for software distribution, resource management, and client inventory tasks. Organizations can use the Centralized model (or any applicable segment) to provide management capabilities for locations that require responsive administrative control at the site or corporate level.

This model also increases overall scalability of the system since the data processing load is distributed across multiple servers. All Altiris 7 solutions installed into the system benefit from this hierarchy. You can install multiple Site Servers to keep your software packages close to your managed computers. Security Roles can be configured at the top level to limit remote location administration to ensure that regional administrators can manage only the objects in their local area of responsibility.

Each Regional Notification Server will replicate all information to a parent Notification Server to scale both management and inventory capabilities. From a Regional perspective, an administrator can be set up to manage and report on all managed computer resources in the organization. Reporting resource data from each region provides central administration and reporting capabilities to administrators at corporate headquarters. This multi-tiered architecture is a common design for Altiris 7 systems.

This model works well because it can all be installed on one server for a small to medium company (99-5,000 nodes), for small-large enterprises (5,000 - 25,000+ nodes), or for organizations with a combinations of large sites, branch offices, and dial-in remote users.

As new offices or users get added, administrators can add new servers to meet emerging needs. With Altiris 7, you simply deploy another Notification Server or Site Server based on your needs, management design, or network topology. You can also add new solutions to each Notification Server to meet emerging requirements for each network segment or site.

Notification Servers: NS installations will be located at headquarters for central reporting and management of dial-up users, at each large international site, at a regional site to manage small branch sites, and at the main campus.

- A Central Notification Server will be located at the corporate headquarters
- A Notification Server will be used to manage all mobile/remote connections and serve as the parent node for the management of all corporate segments
- A Notification Server will be used on each corporate segment and serve as the child nodes of the Notification Server placed at the corporate level.
- A Notification Server will be used to manage all Large Branch Sites
- A Notification Server will be used to manage all Small Branch Sites
- A Site Server will be placed on each Small Branch Site
- A Notification Server and Site Server will be placed on each of the Large Branch Sites.
- Important Inventory data flows from the lower level NS servers to the next tier level and eventually ends up at the Central Notification Server.
- Downward flow of packages, advertisements, and policies occurs from the Central Reporting Notification Server to the lower level NS servers.

Inventory Solution: Inventory will be reported on individual managed computers to the assigned Notification Server. Inventory data will be forwarded to the Central Reporting Notification Server for centralized reporting.

Software Delivery Solution: Software Delivery Solution will be the primary method of package distribution to headquarters and international locations. Packages will be automatically distributed to the Site Servers and users will access packages from the closest package server.

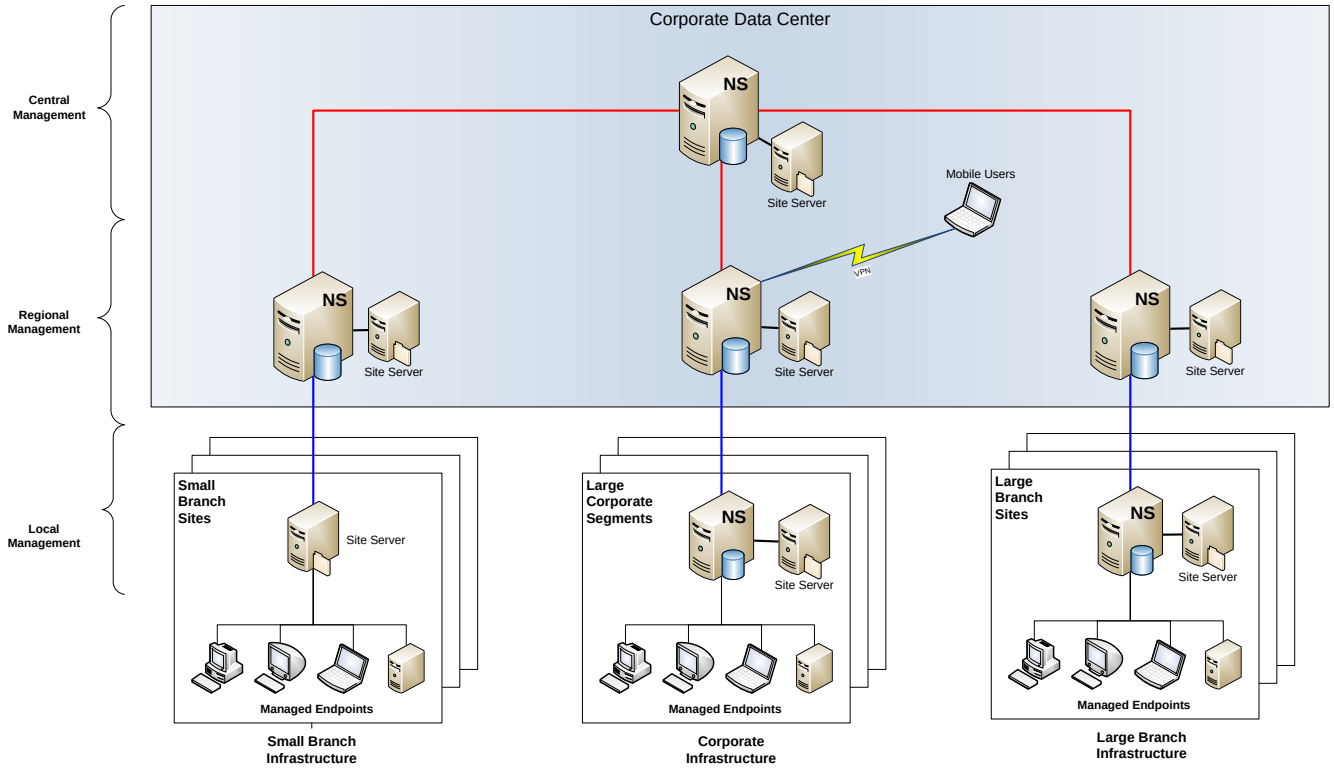
Site Servers: Packages will automatically be distributed to the Site Servers. Clients will access packages from the closest package server.

To plan a strategy for your organization, identify a model (Enterprise model, Branch model, Low bandwidth Model, etc.) defined within this comprehensive example and extrapolate differences in specific environmental variables for your organization.

Other Considerations

In some cases there may be a need to centralize all management, reporting and distribution from a central data center. If this is the case, all Altiris 7 management elements can be brought into the corporate location without losing the ability of regional or local management. This model has its advantages where the support model of all Altiris 7 servers and databases must be managed from a single location:

The following diagram illustrates how the Centralized model demonstrated above could be modified for central support and disaster recovery.



4.4 Small to Medium Business (SMB) Models

For medium or small-sized organizations, you can set up Altiris servers in a variety of ways depending on the structure of the organization, selected Altiris solutions, and needs of the IT team. You can distribute the installation of Notification Servers and Site Servers for each network segment or site, or install all Altiris servers on a single server. Even within each solution, different components such as the database, web and Windows consoles, Task Services, Package Services, PXE Servers, web servers, and Client Access Points can be installed on either the same or separate computers.

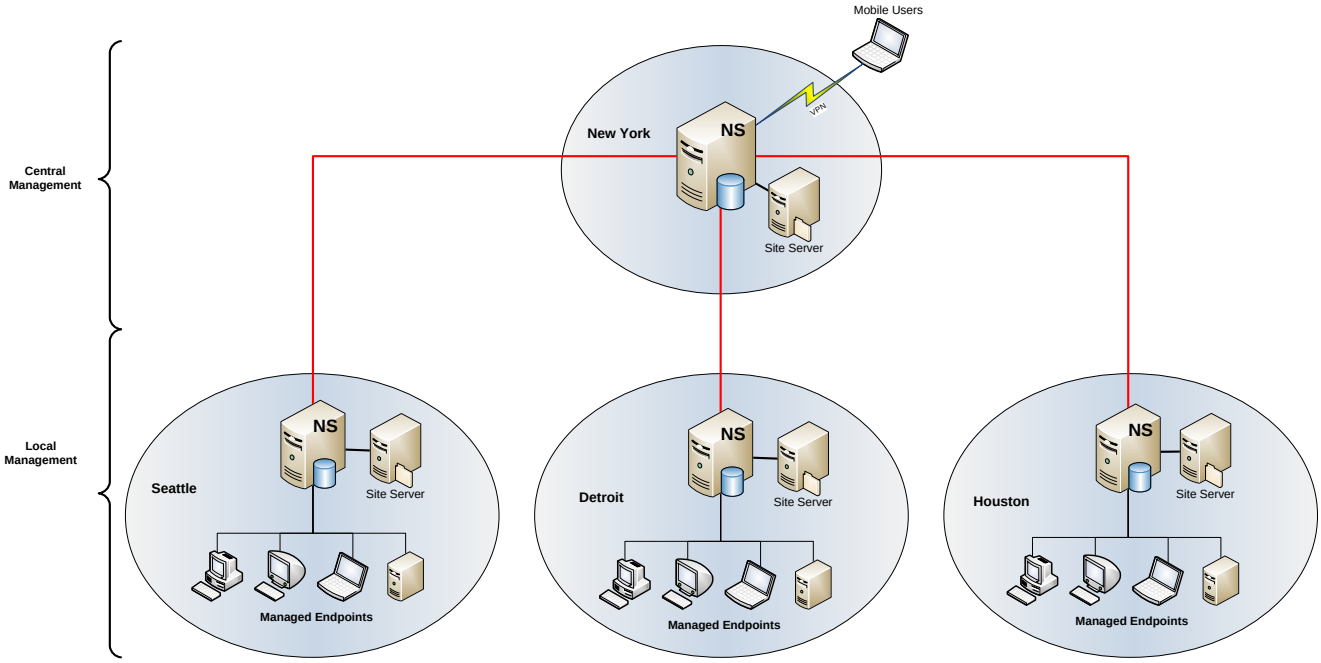
The following issues and requirements characterize small and medium enterprises:

- **Fewer resources available.** IT departments have a broader scope with fewer dedicated resources
- **Limited hardware**. In many cases, the network infrastructure is a lightweight infrastructure with lower bandwidth.
- **Limited funds.** Less capital for training and PSO.
- **Centralized administration.** IT team may need to manage multiple sites.
- **Variable Connectivity ranges.** Like large enterprises, small to medium organizations may need to manage both a single LAN site with multiple WAN sites**.**

From the regional level, web monitoring, inventory, software delivery, reporting and other comprehensive management features can be accomplished from the Symantec Management Console running on the Notification Server. Multiple web solutions can be installed as needed to manage, report and set policies from the Altiris Solution Center for management over the WAN.

Medium to Large Sites with Distributed Servers

For an organization with multiple sites (medium and large) or network segments, Notification Servers can be distributed at individual sites with a database at each site. From the Central Notification Server, IT personnel can then generate reports and set policies, manage solutions and distribute software packages for the entire organization.



Notification Server: Notification Server installations will be located at a head office site for central reporting and management of all remote users and the head office endpoints. Notification Servers will also be placed on all local sites.

- A Central Notification Server will be located at the corporate headquarters. This Notification Server will be used to manage all mobile/remote connections as well as the head office managed endpoints. It will serve as the parent node for the management of all remote sites.
- A Notification Server and Site Server will be used on each remote site and serve as the child nodes of the Notification Server placed at the head office.
- Important Inventory data flows from the lower level NS servers to the Central Notification Server
- Downward flow of packages, advertisements, and policies occurs from the Central Reporting Notification Server to the lower level NS servers.

4.4.1 Small Branch Sites with Mobile Users

Small organizations can install Altiris 7 on a single server, or distribute Altiris servers across multiple servers to manage clients. With one or more Altiris Servers, you can set up local peer servers on a single computer or distributed across multiple computers to manage a site.

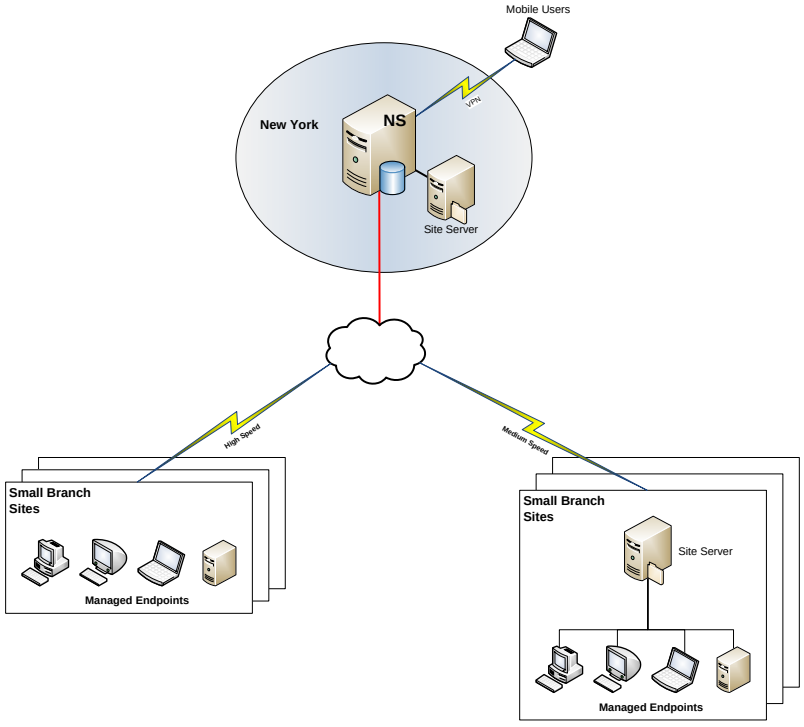
For organizations with remote sites and personnel, Altiris servers can be configured to manage satellite locations from a regional Notification Server. If the branch site is small and has no resident IT person, Package Servers can be installed to download software and image packages deployed from a local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

5 Capacity Planning Guidelines

The purpose of this section is to provide some general guidelines for recommending hardware specifications for Altiris 7 Infrastructures with a limited set of management features (Inventory, Patch Management, and Software Management Solutions). The actual hardware to be purchased or appropriated by the organization will vary from organization to organization; however, making recommendations based on these guidelines will provide an educated specification that will have a high probability of meeting the organization's needs.

Testing was performed using a release candidate of Symantec Management Platform 7.0 SP1 with Inventory, Application Metering and Software Management Solutions installed. The information and recommendations in this document are given as-is with no warranty implied or given. However, as similar tests are performed with future Symantec Management Platform releases an update to this document may be given.

5.1 Notification Server Sizing Guidelines

The biggest use of resources on the Notification Server is due to the database processing. Therefore, it is important to determine if the infrastructure will be using a local database configuration or a remote database configuration. A Notification Server with a local database is going to need many more resources than a Notification Server with a remote database configuration. The database requirements themselves are going to be driven by the number of solutions installed on the Notification Server and the manner in which they are being used. It is also dependent upon the number of nodes being managed by the Notification Server.

Important Note - The recommendations given in this section are noticeably higher than the minimum system requirements. The goal is to provide recommendations that will sustain the transitions inherent to a long-term deployment of the Altiris 7 Infrastructure and full management feature implementation. One key to choosing hardware and database requirements for any given installation is the number of managed endpoints. A second key is the choice of the SQL Server version and whether or not SQL Server will be on the same box as the Notification Server. Lastly, the Suites and Solutions included in the deployment should also be taken into account.

5.1.1 Small <500 Managed Endpoints

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.

5.1.2 Medium <3000 Managed Endpoints

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 Altiris 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 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 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.

5.1.3 Large <10,000 Managed Endpoints

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.

5.2 Memory Management

Memory Management is very important especially when SQL is running on the same box as the Altiris Service. The following guidelines give basic understanding of the means by which to manage memory and recommendations are given based on the values shown in the Quick Guide found on page 3. If your memory is configured differently make sure you understand these options well. For a more comprehensive understanding please consult Microsoft documentation.

- **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.

5.2.1 Memory Recommendations

- **Small Environments:** Use the /3GB switch and SQL Maximum Server Memory is set to 1.2GB RAM.
- **Medium Environments:** When SQL is on-box ensure that PAE and AWE are enabled. If SQL is off-box ensure that AWE is enabled.
- **Large and Very Large Environments:** Use AWE and PAE or use 64-bit SQL.

5.3 Database Size Considerations

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

As a rough guideline for database size, consider allowing three-quarters to 1 MB per client in the Notification Server database. This sizing does not account for database fragmentation beyond initial creation. Actual sizes will vary based on the solutions installed and the regularity of configured policy, tasks, and schedules. Also, the database maintenance strategy employed will affect actual database size.

When Client Management Suite, Server Management Suite, or other solutions are installed in a large environment, it is reasonable to expect the Symantec Management database to grow to the 6 to 12 GB range. 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 database after initial installation.

IMPORTANT: If a SQL Cluster is proposed for a shared database infrastructure, it is very 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 exist on a separate instance. This is recommended to avoid TempDB contention.

5.4 Summary

The following table depicts the recommended hardware and software specifications for all of the scenarios mentioned in this section.

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

6 Notification Server Core Design

6.1 Notification Server

6.1.1 Requirements

Section 3 states the hardware and software specifications required for planning your Altiris 7 Infrastructure, however there are more specific software components required to fulfill the requirements. Again, these specifications should be used as a guide and the following items should be included in your design:

Notification Server

Item	Specification
.NET	Microsoft .NET 3.5
Web browser	Microsoft IE 7
Web Server	IIS 6.0

Altiris 7 Console System

Item	Specification
Web browser	Microsoft IE 7

6.1.2 Assessment

Before you install and run Symantec Installation Manager, you should develop an installation plan. As you develop an installation plan, you should answer the following questions:

- **What type of installation should you perform?**
  You must determine if the installation is a first-time installation or an upgrade. If the installation is an upgrade, you need to determine if it is an on-box upgrade or an off-box upgrade. For both a first-time installation and an upgrade, you must also determine whether the computer can have an Internet connection. Although the overall process for each of these types of installations is very similar, the type of installation affects how you install the product.
- **How many computers do I plan to manage with the Symantec Management Platform products?**
  You configure the installation differently depending on the size of your environment. For example, in a large environment you would not install SQL Server on the same computer where you install the Symantec Management Platform products.
- **Does the computer meet the system requirements?**
  During the installation process, Symantec Installation Manager performs a readiness check to determine if the computer is ready for the installation. However, this check only verifies that the computer meets the minimum requirements. Before you begin the installation, you should make sure the computer meets the system requirements that are appropriate for your environment.
- **Is the installation for a production environment or for evaluation purposes?**
  If you are an evaluator, you can quickly install and begin testing the products. In a production environment, we recommend that you install the products in a test environment before you install them in a production environment.

6.1.3 Design Considerations

- **Schedule server-side tasks to occur off-hours when possible** – This will aid in allowing for increased console performance during the hours you truly manage your infrastructure.
- **Stagger schedules where possible** – whenever you are scheduling management items be sensitive to replication schedules and other critical operations.

- **Leverage "Internal Schedules Calendar" and performance reports** to identify and optimize potential bottlenecks

  NOTE: Policies are not always run at the times shown in the calendar. Policies are not as deterministic as tasks, so may be subject to delay. Tasks and jobs are always run at the times that are shown in the calendar.

- **Review Role and Scope based security** - Try to leverage existing privileges and permissions where possible when creating new roles

- **Use Purging Maintenance** - Enable Purging on dataclasses that make sense.

- **Adjust Agent Configuration and Collection Update intervals immediately -** Review agent configuration intervals and collection update intervals. The top two sources of processing load are caused by agent configuration requests, and collection rebuilds. For production purposes, Altiris agent configuration intervals should be no less than 1 hour, with most enterprise environments using 2–6 hour check-in intervals.

  Delta and Policy Change collection update intervals should be no less than 30 minutes, with most enterprise environments using 1–3 hour update intervals. A general rule of thumb is update collections twice as frequently as the Altiris Agent interval. Stagger the start times on the collection update schedules by 10–15 minutes to avoid concurrency problems. The full collection update schedule should remain at once per day.

6.2 The Altiris Agent

6.2.1 Requirements

If any of the solutions you installed are used to help manage other computers (most solutions are), you must install the Altiris Agent on the computers to be managed. The agent facilitates communications between the managed computer and the platform and solutions. The agent also receives tasks from the platform and solutions, helps install software, and sends data that is collected from the managed computer to the platform. Verify that each managed endpoint will meet the Altiris Agent installation prerequisites as listed below:

Item	Specification
Operating System	Windows 2000 SP4, Windows 2003 (any 32bit; any x64bit except SP2, Windows XP SP2/SP3, Windows Vista (any), Windows 2008 (any)/Not Core Option
Hard disk space	60 MB minimum
RAM	64 MB minimum (128 MB recommended)
Internet Explorer	IE 5.0 or later
Access rights	Account used to install agent must have Local administrator rights
Windows XP Items	Turn off simple file sharing and Open Port 80 and/or 445 directed to the Notification Server IP

6.2.2 Assessment

In order to properly assess the Altiris Agent requirements, the following questions should be asked in order to determine what items need to be configured and to gain consensus on the design:

- Do you wish to ensure that end users have a minimal amount of interruption?
- Do you want Agent shortcuts in the Task tray?
- Do you want to see Altiris start menu items?
- Do you want the agent icon to be invisible to the user?
- Should client communications be reduced to a minimum during the day, if so when?
- Should the agent conserve bandwidth wherever possible
- Do you require Wake on LAN and Power Management options?
- Do your local subnets allow multicast traffic?

6.2.3 Design Considerations

6.2.3.1 Deployment of the Altiris Agent

The discussion continues as to the best way to deploy the Altiris Agent. This topic has been of special concern for computers running Microsoft Windows XP* that have not joined a Microsoft Domain as "Simple File Sharing" is enabled on these computers by default. This setting does not allow one to push the Altiris Agent onto such a computer and, in a small business/remote office environment, it is often not desirable or practical to deploy a computer, then send a technician on-site or require the computer owner to change this "Simple File Sharing" setting in order to push the Altiris agent to the computer.

As with most things, there is no single "best method" that covers every situation. Each deployment situation is unique with its own set of requirements and limitations. As a result, this article will not try to address the "best" method; rather, this article hopes to discuss various methods that can be used to install the Altiris agent without sending a technician on-site or requiring knowledge of the operating system by a computer's end user. Also, it will touch on planning for future deployment of the Altiris agent. This way those managing the Altiris Notification Server implementation can choose what methods might be best for their specific environment.

Planning an Altiris Agent Deployment

When planning an Altiris agent deployment, there are at least two groups of computers to consider: the computer already deployed and in service, and those that will be deployed in the future. Although those computers that are already in service tend to be the computers of most concern, those that are yet to be deployed should not be overlooked.

With a little planning, the future deployment of "Altiris Ready" computers will save considerable time and effort, especially when using such solutions as Asset Management and/or where tracking computer assets are important. The idea of a computer reporting in as soon as it connects to the network allows such tracking to occur.

In many environments, computers are "built" with a corporate software image or at least a standard base list of software before the computer is deployed to the end user. This is sometimes done by the IT group using such tools as Altiris DS or Ghost, and it may be contracted out, or sometimes it is even installed at the OEM factory before shipment to the end user. No matter the method, adding the Altiris image to this build can save considerable time and effort.

The Altiris Agent can be completely preinstalled, placed in a directory with a "Run Once" operating system directive, or it can be installed by using the various scripting mechanisms available. If it is undesirable to add the Altiris Agent to the build, and a "Push" deployment is still considered the best way to install the Altiris Agent, then changing the image to disable the Simple File Sharing option should be included so that future intervention by either a technician or computer end user is not needed.

Building Computers from Scratch

If a computer image is not being utilized in a business environment, computers will need to be built from scratch by either a technician or end user. If utilizing a technician, he or she is already working on the computer and thus bypasses the purpose of this article (the purpose again being not requiring a technician's intervention or limiting the end users required computer knowledge). The technician could manually install the agent, disable Simple File Sharing, or utilize the methods discussed for end-user building as a procedural process of building the computer. Having the end user build the computer also by-passes the purpose of this article.

A script (electronic or printed) is probably utilized to help the end user, and this script could be modified to include the installation of the Altiris Agent or disabling Simple File Sharing. Disabling Simple File Sharing could be accomplished via the normal operating system GUI, or by running a simple executable that changes the registry setting. The ability of the agent to be "Pulled" as well as "Pushed" should also be considered.

Using "Push" or the "Pull" methods for in-service computers

Most people think of pushing the Agent when deploying a Notification Server environment. This is relatively simple, requires no outside intervention, and can be automated for after hour's deployment. Although this is probably the method most commonly used for deploying the agent to computers already in service, it is not the only method available. The mechanism used by the push is actually contacting the client computer and initiating a pull that requests the agent from the Notification Server.

This is where Simple File Sharing setting comes in and why it is required to be disabled for a push. With Simple File Sharing enabled, the client computer still has the ability to initiate this request itself.

As a result, there are various ways to pull the agent from the Notification Server that would allow Simple File Sharing to be enabled and still install the Altiris Agent. For example: By utilizing e-mail, either a simple script can be e-mailed to an end user, or a Web link can be sent such that by clicking on the link or running the script, the agent can be pulled. This would require no knowledge on the end user's part, other than how to open e-mail and how to click on a link. (Instructions to do so could be included in the e-mail if needed).

Manual Installation of the Altiris Agent

The manual installation of the Altiris Agent is like any other Software Deployment. If you understand the command-line switches to use, you can script the install any way you'd like. This section reviews the Altiris Agent installer, and its command-line parameters, and also gives an example.

The Altiris Agent installation program extracts the Altiris Agent installation files into a temporary location and then runs the Altiris Agent installation setup on a single computer. The Altiris Agent bootstrap program usually downloads and runs the Altiris Agent installation program.

6.2.3.2 Agent Upgrade from 6.0 to 7.0

You can configure the Altiris Agent Upgrade and Altiris Agent Uninstall policies to suit your requirements. Both policies use the Altiris Agent package, but use different programs. Notification Server provides some default filters that you can use in scheduled agent installation operations and in agent upgrade and agent uninstall policies. These filters are stored in the Altiris Agent Rollout folder, the default filters are as follows:

- Computers with Altiris Agent version less than NS 7 Altiris Agent installed
- Windows computers requiring Altiris Agent upgrade
- Windows computers with NS 7 Altiris Agent
- Windows 2000/XP/2003/Vista/2008 computers with no Altiris Agent installed

By default, the Altiris Agent Uninstall policy is applied to the "All clients with no additional agents" filter, and the Altiris Agent Upgrade policy is applied to the "Altiris Agent Upgrade" filter. You need to be careful when you are performing Altiris Agent upgrades based on resource targets. In a large environment you may prefer to stagger the upgrades by using a trial target first, and then a staggered rollout through suitable targets, rather than perform them all at once.

A staggered upgrade also helps to manage the load on the network as the agents typically need to request data from Notification Server as soon as they have been upgrade. When upgrading 6.0 Agents to 7.0 it is advised that you follow these guidelines before attempting the upgrade:

- The Computers should exist in the NS 7.0 database before upgrading agents – This can be achieved by:
    - **Importing them from an exported NS 6.0 server process** - To prevent new GUIDs from being generated in the case of a NS 6.0 to 7.0 migration, you should import them using the process defined in Section 8.
    - **Using Active Directory Import** – Import Computer Resources from specific domains
    - **Redirecting the NS 6.0 Agents to the NS 7.0 Server** - (If a migration is not planned)
- You must enable the Agent upgrade policy on the NS 7.0 Server for the process to take place. NS 6 Agents do not communicate with NS, except to begin the upgrade.
- **The Agents will be upgraded as they check in with the new server** and will follow this process:
    - The client is detected by the NS 7.0 Server
    - The Altiris Agent is upgraded to 7.0
    - All 6.0 Agent plug-ins are disabled, as well as the old 6.0 policies and tasks.
    - The Altiris Agent 7.0 plug-ins are installed

NOTE: Plug-in installation\upgrade is entirely dependent on what is enabled at the time of the agent upgrade

6.2.3.3 Agent Configuration

The default Altiris Agent configuration settings are suitable for a small Notification Server environment. As your environment grows, or if your organization has particular requirements, you need to make the appropriate configuration changes. Some configuration options to consider are as follows:

- Enable Power Management settings if you need to turn managed computers on for any solution tasks.
- Clone the default policies and divide the targeted systems between these policies in larger environments.
- Make sure that each managed node has a single Altiris Agent policy applied
- Increase the Agent communication parameters as node count increases. A general rule of thumb may be one hour for every 2,500 nodes.
- Utilize bandwidth throttling where WAN or LAN links are highly utilized or slow
- Have the communication startup delay set to 1 hour in larger node counts as this will prevent server contention when a large number of managed computers turn on every day.
- The “All Site Servers" policy will affect the Site Servers deployed throughout the environment. This policy should be set to communicate regularly with the Notification Server and receive updates with a reduced bandwidth throttle.
- The “All Windows Mobile” policy will affect all Windows workstations which primarily connect to the network via a WAN/VPN connection. This policy should be set to communicate with the notification server every hour so you have a better chance of allowing the managed system to receive and download packages. The Agent should also be set to not Download packages if the available bandwidth is less than 100Kb/sec
- Do not use non-ASCII characters in the files and directories names when you configure installation settings.
- The Default installation of the Notification Server has NO maintenance window policies enabled.
- When multiple Maintenance Window policies are applied to a computer, task execution is permitted during any available window. Agent checks to see if any windows are “activated” at time of scheduled execution
- If there is no maintenance window policy and\or expired maintenance window policy then task execution permitted at any time Unless specified by schedule to “not run if no maintenance policy is applied”

It is not advised that you run a large distribution of the Altiris Agent during implementation; a best practice is to create specific filters that call a smaller subset of the systems that need an agent and build in dynamic elements that take them out of this filter once the Altiris Agent has been installed.

6.3 Site Management

DISCLAIMER: This section called "Site Management" has not been tested by Symantec Labs and is under review, the values and specifications for Site Servers and their respective recommendations will be included in a later version of this document.

6.3.1 Requirements

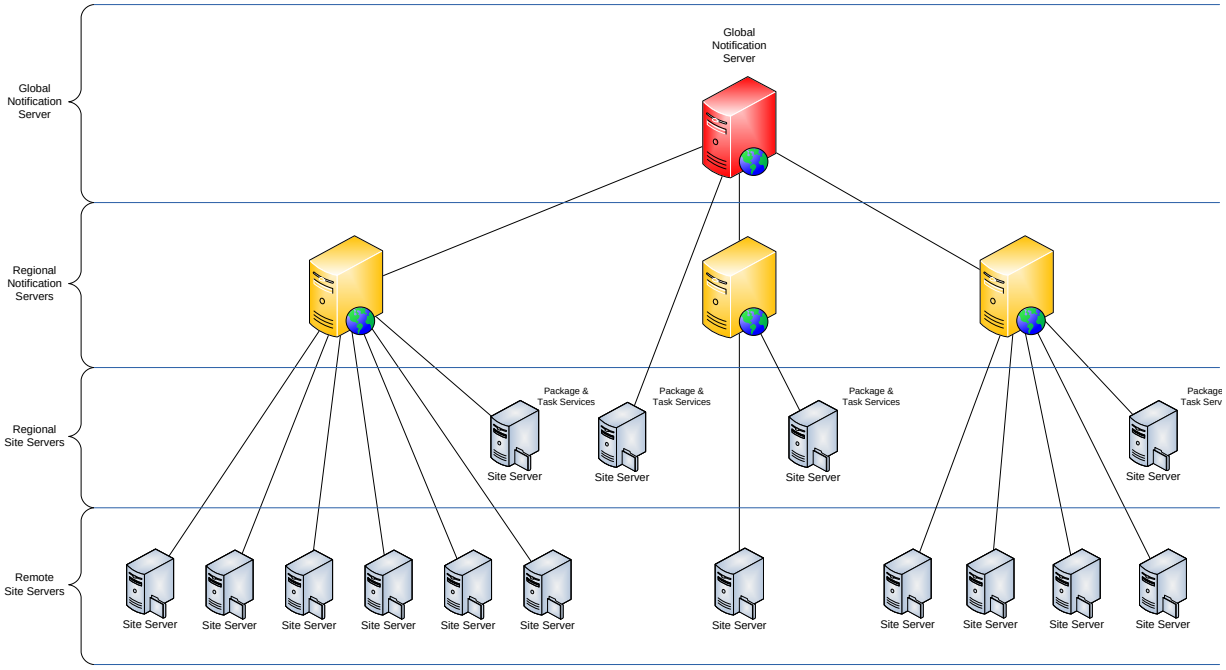
The amount of managed endpoints that a Site Server can serve depends on the hardware and software of the Site Server itself. These recommendations are based on the minimum hardware recommendations and reflect a Site Server with Package and Task Services enabled.

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	Altiris Agent 7 installed Microsoft .NET Framework 1.1 TCP Ports 50120-50124 opened	Altiris Agent 7 installed Microsoft .NET Framework 1.1 TCP Ports 50120-50124 opened

6.3.2 Assessment

Site servers help simplify the management of your Notification Server environment. Notification Server can use other computers to distribute its workload processes. Any managed computer that has a service plug-in installed on it and runs one of these services is a site server. Notification Server can then reduce its workload and minimize network traffic by delegating package downloads and tasks to site servers.

The following diagram illustrates how site servers are typically configured throughout the hierarchy. You may find that you may want all options on a Site Server at the higher levels, but may only want Task Services on lower levels. You must determine the best option while balancing network utilization and Notification Server load.



6.3.3 Design Considerations

Site Server Design

The number of Site Servers required in any environment is based on your network topology and bandwidth. It also depends on the size and frequency of the packages to be delivered and the number of managed computers that can register to a Task Service. You must fully understand your own network topology (switches, subnets, and so on) and its network traffic capabilities before rolling out Site Servers. Knowing your environment and the size, frequency, and timing of Packages and Tasks will dictate your Site Server placement.

When designing your Site Server placement and configuration you should consider the following items as they will guide you in determining the best architecture for your organization:

- To balance the use of site servers in your environment, you should ensure that they are assigned to the appropriate sites. You can do this by using the following methods:
  - Manually assign the subnets that contain the site servers to sites.
  - Manually assign the site servers to sites.
  - Use Connector for Active Directory to perform the task.

    Connector for Active Directory overrides any subnets and sites that conflict with it. For example, if you manually assign subnets to particular sites that conflict with what is in Connector for Active Directory, the Active Directory information is used.
- Under normal operating conditions a Site Server will service the Altiris Agents that exist within the sites to which it is assigned. If no sites have been defined, all Site Servers are available to service all Altiris Agents (although this is not recommended).
- Stagger the deployment of Site Servers if Package Services are enabled.
- It is also important to know what the Notification Server is capable of supporting , use the following points to guide your planning:
  - A single Notification Server can manage up to 500 Site Servers
  - A single Notification Server can manage up to 5,000 Packages
  - Can deploy100 Site Servers with Package Services in 18 Hours
- Use the following table lists the minimum number of Site Servers you will need for the number of managed computers for a single Notification Server with both Task and Package Services enabled.

Managed Computers	500	1000	2500	5000	10000
Site Servers	1	1	1	2	4

Package Services Design

When considering Package Services design, placement and configuration you should understand the following factors that can affect the efficiency of the Altiris 7 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 Replication Functions are to be utilized, you must have at least one Site Server with Package Services installed on the same site as the Notification Server.
- 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 Altiris 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.
- 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 Altiris 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 Altiris 7 infrastructure:

- If a Notification Server 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 is managing 500 registered end points or less, Notification Server can have dual role as a managing Site Server with Task Services enabled.
  - If Notification Server 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.

6.4 Replication

The replication functionality described here is different than hierarchy replication, which defines the two-way information flow between two Notification Servers. Hierarchy replication provides reliable and scalable data synchronization between multiple Notification Servers. Replication can be configured to replicate data outside the hierarchy structure, for example, by sending data to an external server that collates particular information for reports.

6.4.1 Requirements

The following statements list the absolute requirements for the implementation of replication rules between notification servers:

- Network traffic must be routable between adjoining notification servers within the hierarchy.
- HTTP/HTTPS traffic must be permitted between adjoining notification servers within the hierarchy.
- Trust relationships must exist between adjoining notification servers within the hierarchy, or credentials for privileged accounts that facilitate trust must be known.
- Each notification server must be able to resolve the name and network address of any adjoining notification servers within the hierarchy.
- There must be sufficient bandwidth between Notification Servers to support package and data replication.
- Bandwidth and hardware required is determined by the size of your Hierarchy topology and the data replicated.

6.4.2 Facts

The following statements list factual information regarding Replication in the Altiris 7 infrastructure:

- Supports point-in-time recovery.
- Replication can occur independently across multiple NSs.
- Uses thread pool architecture, meaning it scales system performance.
- Only replicates items that have changed since last replication
- Network communications are authenticated and authorized.
- Supports transport encryption through HTTPS.
- Network communications are compressed.
- Optimized for asynchronous and discrete communications.
- Supports prioritized replication.
- Uses standard web protocols and ports.
- User editable configuration allows for optimized deployment.

6.4.3 Assessment

When assessing the replication requirements it is important to remember that this step is typically completed after you have determined your hierarchy replication requirements and you have found something that was not available or possible in those requirements. To assess your requirements for replication, you should consider the following items you have available to replicate as well as their source and target Notification Servers:

- Configuration and management items, such as reports, resource targets, policies, and tasks
- Resources, such as computers, users, and packages
- Events, such as software delivery execution
- Security settings, such as roles, privileges, and permissions

6.4.4 Design Considerations

When designing the Replication rules for your implementation you should consider the following items:

- **Replication could span a DMZ for remote/mobile users** – if this is the case special security considerations must be observed to ensure the protection of the data transmitted across the network.
- **Distance Latency on long haul circuits must be considered** – Slow network links between notification servers and or their assigned site servers can severely impact the schedule, quality and validity of the replicated data.
- **Always stagger Replication schedules per notification server** – staggering the schedules will minimize network load and data collisions.
- **Understand the impact to WAN and other management tasks depending on specific shared objects –** understand that if you impact the wan at specific times, you could be preventing the transmission of critical patches, software or inventory operations.
- **Replication rules are NOT cookie cutter across all NS's** – In most cases you will be developing specific rules for each of the notification servers.
- **Understand the differences between Replication and Hierarchy Replication** – Carefully plan replication rules so similar data is not passed in both directions. This will ensure that you do not duplicate efforts in multiple configuration areas.
- **Consider the possibility of replication fragmentation** – understand that replication results can be affected by other replication events running in parallel.
- **Determine the level and cost of replicated data validation** – a 100% validation of specific types of data, events or resources can either be overrun because of its run time or can be too costly on the resources of the notification server.

- **Minimize 'Event' replication** to summary information that can be used to create reports at the top level of the hierarchy (1st tier, or root NS). Remember this will allow drill down through the report results to a particular NS and access its event data. (details are not lost)
- **Each item has 'item attributes'**. These can be seen by right clicking on the item and going to the Properties. If the attributes of an item are either 'System' or 'No Replication' then the item should never be considered for replication.
- **Don't forget to enable the replication rules once they are created.**

6.5 Hierarchy

6.5.1 Requirements

The following statements list the absolute requirements for the implementation of a Hierarchical relationship between notification servers:

- Network traffic must be routable between adjoining notification servers within the hierarchy.
- HTTP/HTTPS traffic must be permitted between adjoining notification servers within the hierarchy.
- Trust relationships must exist between adjoining notification servers within the hierarchy, or credentials for privileged accounts that facilitate trust must be known.
- Each notification server must be able to resolve the name and network address of any adjoining notification servers within the hierarchy.
- There must be sufficient bandwidth between Notification Servers to support package & data replication.
- Bandwidth and required hardware is determined by the size of the Hierarchy topology and the data replicated.

6.5.2 Facts

The following statements list factual information regarding Hierarchy and Hierarchy Replication in the Altiris 7 infrastructure:

- Hierarchy supports n-levels - it may be as deep or shallow as you require.
- Joining a Hierarchy requires both the parent and the child to agree on each other's role.
- Hierarchy supports structures that span multiple workgroups/domains (trusted and non-trusted).
- Data integrity and consistency is maintained at all levels within a Hierarchy structure.
- Network communications:
    - Are authenticated and authorized
    - Are firewall friendly - uses standard web protocols and ports
    - Are reliable - supports point-in-time recovery
    - Support compression
    - Support transport encryption (via HTTPS).
- Hierarchy uses Replication to copy and synchronize shared objects and data between notification servers within the same hierarchical structure. At scheduled intervals, each server within a hierarchy synchronizes objects and data with its immediate parent and immediate children.
- A solution cannot participate within Hierarchy unless Hierarchy support has been explicitly enabled for the solution. If Hierarchy support is not enabled, then a solution's items, resources, events and security setting cannot be replicated or managed via Hierarchy.
- If you remove a parent notification server, its child notification servers are also removed from the Hierarchy
- If you remove the notification server at the top of a hierarchy structure, all its child servers become parent servers of their own hierarchy
- You can enable or disable Hierarchy replication on specific notification servers at any time.

6.5.3 Assessment

An enterprise environment may have multiple Notification Servers for many reasons. This may be due to both technical and non-technical considerations. Notification Server system version 6.0 provides very limited support for managing multiple servers.

By enabling Inventory Forwarding in NS 6, it is possible to define relationships between independent Notification Servers to facilitate centralized data gathering and reporting; however this technology does not allow configuration and security data to also traverse these same relationship structures to assist in the management of the system as a whole.

Assessing the applicability of Hierarchy in your design will come down to the following questions:

- Are you currently experiencing high loads on a single notification server?
- Are specific notification servers servicing too many clients?
- Are you duplicating actions across multiple notification servers?
- Do remote sites have large number of managed computers (>500)?
- Are there are slow or unreliable network connections preventing clients receiving packages?
- Does the WAN topology require multiple notification servers globally?
- Are there corporate, regional and/or branch office environments?
- Is there a need to split management duties across multiple notification servers?

6.5.4 Design Considerations

When designing an effective hierarchy, you should consider the following factors that can influence the outcome of your design:

- **Implement Hierarchy one level at a time –** this is one case where parallel implementation is not the best practice – aids in troubleshooting replication errors.
- **Business and Physical factors should drive design** – the structure you design should take into account the business management structure as well as the physical factors like WAN topology and supportable locations to place notification servers that will enact the hierarchical structure.
- **Notification Server topology could span a DMZ for remote/mobile users** – if this is the case special security considerations must be observed to ensure the protection of the data transmitted across the network.
- **Distance Latency on long haul circuits must be considered** – Slow network links between notification servers and or their assigned site servers can severely impact the schedule, quality and validity of the replicated data.
- **Consider available bandwidth and QOS policy for packages** – not having enough available bandwidth or a severely throttled transmission can result in the delay or absence of critical updated packages.
- **When a hierarchy conflict exists in your design remember that the conflict management functions will always allow the parent as having the priority.**
- **Always stagger hierarchy replication schedules per notification server** – staggering the schedules will minimize network load and data collisions.
- **Consider replication modes across the hierarchy (complete vs. differential)** – A complete replication mode will cause all the data to be replicated every time – best practice is to set it to differential for all rules, as it will do a complete replication on the first run.
- **Understand the impact to WAN and other management tasks depending on specific shared objects –** understand that if you impact the wan at specific times, you could be preventing the transmission of critical patches, software or inventory operations.

- **Hierarchy Replication rules are NOT cookie cutter across all** NS's – In most cases you will be developing specific rules for each of the lower level notification servers.
- **Understand the differences between Hierarchy Replication and Replication** – this will ensure that you do not duplicate efforts on the notification server in order to complete a single replication task.
- **Consider the possibility of replication fragmentation** – understand that hierarchy replication results can be affected by other replication events running in parallel.
- **Determine the level and cost of replicated data validation** – a 100% validation of specific types of data, events or resources can either be overrun because of its run time or can be too costly on the resources of the notification server.
- **Do not use the default hierarchy replication rule as your base** – All items are enabled by default and can unnecessary LAN utilization as well as database growth.
- **Replicate only what is needed** to meet your organizational requirements
- **Minimize 'Event' replication** to summary information that can be used to create reports at the top level of the hierarchy (1st tier, or root NS). Remember this will allow drill down through the report results to a particular NS and access its event data. (details are not lost)
- **Minimize verifying** large amounts of resource data on every replication by specifying a verification percentage in the replication rule.
- **Each item has 'item attributes'**. These can be seen by right clicking on the item and going to the Properties. If the attributes of an item are either 'System' or 'No Replication' then the item should never be considered for replication.
- **When a node is removed** from a hierarchy, all objects previously replicated are effectively reset, to be no longer hierarchy managed, enabling the user to take control of the object and delete, modify etc, if desired.
- **In large environments** - 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 / subnet NS belongs too before setting as a first step to setting up hierarchy.
- **Include a Hierarchy Admin role in your security design -** where this role is responsible for the topology to include adding, removing, reporting status, and managing replication within a hierarchy; thus limiting the scope of potential bad replication practices, adjoining an unauthorized NS etc..
- **If you include resource targets** in a resource replication rule, you need to be aware that only the contents (resources) of the target are replicated and resource scoping applies. Resources replicated depend on the owner of the resource target.

6.6 Resource Scoping

6.6.1 Requirements

Resource Scoping does not have any specific hard requirements of the external infrastructure as its functions are self contained within the application itself to manipulate and organize internal items within a defined structure.

6.6.2 Facts

- **Filters are conceptually similar to NS 6 collections** - Implemented differently as they are applied to Targets, not policies. They are simply resources joined together by a defined set of criteria
- **Targets Are the intersection of Organizational Groups and Filters** - Example: All computers in Finance (Group) that have less than 1GB RAM(Filter)
- **Targets are applied to policies and tasks** and can be pre-created or created at the time of application

- **Targets can only contain resources that the target creator has access to** and are not visible as objects anywhere in the console, but are accessible via the "Quick Apply" option within a task or policy.
- **Consider an Organizational View to represent an administrative security structure** or boundary which aligns with your IT environment.
- **Organizational Views provide a simplified and secure means to group and manage resources**
- **An Organizational View is a self-contained secure hierarchy of organizational groups**, which contain resources.
- **All Resources in an Organizational View (managed/unmanaged) are scoped by default**
- **There are two types of Organizational structures**:
    - Default Organizational View
    - Custom Organizational View
- **Organizational Views use a top-down security inheritance model**
- **Organizational Groups contain other OGs and Resources**
- **Security grants are assigned to OGs and are inherited from the OG above it**
- **Resource security is the combination of Scope, Security Role, and Permissions**
- **Resources obtain all their permission grants from the scope collections that they are a member of**. The grants are accumulative in nature and having permission to perform an action on a resource in one scope collection, ensures that the user/role can continue to perform this action regardless of whether the permission is applied to other scope collections containing the resource.
- **Security roles are user groups that let you assign privileges for administrative/worker responsibilities** and assign permissions for folders or items that those administrator/workers can view in the Symantec Management Console
- **Out of the box Roles are provided with a variety of privilege grants**, and Roles can be assigned anywhere within the OV/OG structure depending on the administrative scope you choose to grant.

6.6.3 Assessment

Resource scoping provides a secure means of segregating resources into manageable, well structured units. These units are generic in nature so they can be arranged to suit a wide variety of organizational requirements. In most cases assessing the resource scoping requirements within your design will come down to the following questions:

- Who should have full access to the Altiris 7 infrastructure?
- What roles exist within the management functions of day to day operations?
- What areas of functionality require specific roles and rights?
- Does Active Directory accurately reflect our management and/or business model?
- Do Active Directory groups exist that reflect the roles within the Altiris 7 architecture?
- What are the types of resources that need to be managed?

6.6.4 Design Considerations

- **Filters should be created from a single attribute** - Filters can be combined to create complex targets, and by using fewer criteria you get a higher chance of re-use and lower complexity results in a more efficient Notification Server.
- **Resource membership within the system default view is dynamically updated, and set at a 5 minute update interval**. Depending how you plan the creation and resource membership of your Organizational structure keep this in mind when identifying the overall impact of resource membership updates

- **You should set up security roles before performing any other console security tasks** and before Notification Server is deployed to your production environment.
- **Organizational Views only contain resources through the Organizational Groups.** An Organizational View cannot contain any resources directly. All newly discovered resources are automatically imported into the Default organizational view.
- **One resource item can belong to only one Organizational Group in each Organizational View**. When you add a resource to an Organizational Group, it is automatically removed from any other group to which it may be assigned.
- **Use Organizational Groups to apply a policy or task to selected computers, users, and resources.** To do this, use an Organizational Group in a target. In this instance, an Organizational Group functions as a filter, but provides security to ensure that only the resource to which the target owner has permission is included.
- **NS 7 allows multiple organizational views because administrators may have multiple ways of organizing resources.** Therefore, you can have both a view by function and by region.
- **Default Organizational View** - All resources are scoped and secure in this View, resources (managed/unmanaged) are grouped by type and the resource membership is dynamic.
- Only Symantec Administrator Role has "full access"
- **Mirror your Active Directory organizational model** by using Active Directory Import to avoid manual creation and population
- **Group your resources by Type**
- **There are various update processes in place**, and they should be considered when evaluating server performance:
    - Three Update Types (Filters, Targets, OG's)
    - Shared Schedules (Delta, Complete, Policy)
- **When designing your resource framework, use the following implementation checklist** to ensure that it is completed in the correct order:
    - Identify Users, Security Roles and Rights
    - Create Security Roles
        - Assign Rights
        - Assign User membership
    - Create Organizational Views and Groups structure
        - AD Import best practice
        - Group by Resource Type (User, Computer)
    - Assign Roles and Permissions to specific OV/OG
    - Generate Reports for baseline system view of resources
    - Backup the OV/OG structure via Export .XML

7 Altiris 7 Solution Design

7.1 Inventory Solution

7.1.1 Requirements

In order to utilize the Inventory Solution functions the following requirements must be met:

- Symantec Management Platform 7.0 must be installed
- Inventory Solution licensing should be in place
- The Altiris Agent should be installed on any resource you wish to inventory automatically
- The following table provides a general list of supported platforms:
  - Windows 2000
  - Windows 2003
  - Windows XP
  - Windows Vista
  - Solaris
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - SUSE Linux Enterprise Desktop
  - VMware ESX
  - UNIX/Linux
  - Mac OS X 10.3.9 and above

7.1.2 Facts

- **Common data classes** – inventory data classes are consolidated across all platforms based on the CIM standard. The result is a more consistent inventory and true cross-platform reporting. Most out-of-the-box reports have been reworked and are now cross-platform.

- **Application Metering is integrated with Inventory Solution** – Metering and Denial functionality is now part of Inventory Solution. Denial feature has also been integrated with the software catalog where you can right-click a software component and select Actions->Blacklist Application. Note: Application Metering plug-in needs to be rolled out separately for metering and blocking to work.

- **Application Management is integrated with Inventory Solution** - Integration of file and registry baselining is now part of this solution.

- **Application Metering denial functionality are integrated into item-actions** - A "Blacklist Application" right-click menu option available for software components in the Software Catalog this gives you the option to blacklist it by adding it into a "Blacklisted Applications" denial policy. You can go back to this policy (Software tab) if in the future you decide to allow this application to run in your environment.

- **Inventory task wizard is available** – A wizard-based approach helps simplify the creation of inventory tasks. A single inventory task can now be configured to run on Windows, UNIX, Linux, and Macintosh computers. Unique platforms settings can be set on the task.

- **There are three methods of gathering inventory available:**

  - **Agent-based inventory** – Standard inventory that fits most customers and provides the full breath of Inventory Solution functionality.

  - **Standalone inventory** – Administrator can create an Inventory package that can be run on a non-managed machines and gather software, hardware, OS and user inventory. Formerly known as zero-footprint (ZFP) inventory. Windows only.

  - **Agentless Inventory** - Is based on Inventory Solution for Network Devices. Also called Remote Inventory. Gathers inventory remotely through protocols like SNMP. Especially useful for server customers that cannot install management agents on their boxes. Note: you need to discover assets via Network Discovery first in order to use Agentless inventory.

- **Targeted Software Inventory** – It is now possible to inventory machines for particular software components instead of doing a full file scan. Customers can target one or multiple pieces of software focusing their software inventory on the most important applications.

- **Enhanced hardware and software inventory items** – Additional hardware data is collected for CPU, RAM, HDD and NIC. Antivirus software reports have also been improved.
- **Two-pass file inventory** – Network utilization and inventory processing time has been significantly reduced by a smart handling of file inventory data. On the first inventory run only basic file inventory is returned to the Notification Server. If needed, detailed file inventory can be brought in from a token system (instead of reporting duplicate data from all machines).
- **Includes SVS support** - Inventory 7.0 will detect and report virtual applications in Software Virtualization Solution layers whether they are active or not.
- **Inventory Solution can be used on both clients and servers** - Inventory Pack for Servers is a value add for server customers and provides incremental server specific inventory (server applications configuration etc.). Inventory Solution for Servers is just a bundle of Inventory Solution plus Inventory Pack for Servers.
- **Add/Remove Programs inventory is a separate** process - Software Management Framework (SMF) Agent is responsible for gathering Add/Remove Programs/MSI cache inventory.

7.1.3 Assessment

In order to properly assess the Inventory Solution requirements, the following questions should be asked in order to determine what items need to be configured and to gain consensus on the design:

- What are the various schedules to capture the appropriate inventory information?
- Is there a requirement to inventory Windows 95, 98, ME, or Windows NT systems?
- Do you need to inventory UNIX, Linux or Macintosh systems?
- Do you need to inventory servers as well as computers?
- Would you like to see precise system counts on Computers and Servers?
- Is there is a requirement to gather installed software counts?
- Is there a need to track changes in Hardware/Software?
- Are there any custom inventory items you would like to capture?
- Is there a need to alert you about computers not communicating, with low disk space, etc.?
- Is there a requirement for Application Metering of software applications?
- Which applications do you need to meter?
- Is there a need to deny usage of certain applications?

7.1.4 Design Considerations

Solution Design

- **Windows 95, Windows 98, Windows ME, and Windows NT platforms are no longer supported** in this release
- **Inventory Pack for Servers plug-in requires Inventory Solution plug-in to be present on the box before the install.**
- **Application Metering and Denial functionality is currently limited to Windows platform.**
- **Standalone Inventory (aka ZFP) is currently limited to Windows platform.**
- **Inventory Solution provides Hierarchy support and abides by the following rules:**
    - Tasks and Policies will be replicated from top to bottom.
    - Summary data classes will be replicated from bottom to top.
    - Agent rollout policy will be replicated top to bottom.
    - The following data classes will be replicated:
        - Hardware Summary
        - Operating System Summary
        - Monthly Summary

- **Neither Inventory reports nor web parts will work on the top level NS by default.** This is because only three summary data classes are enabled for hierarchy and replication.
- **Unless "Override Maintenance Window" checkbox is selected Inventory Solution will start its tasks only within the Maintenance Window.** This will allow customers to reduce impact on their users and production servers and limit inventory scans to off-hours maintenance intervals.
- **When considering customer impact from Inventory Tasks you should recognize that the Software/file inventory task can choose between Low, Normal, High and Very High priority** under "Set inventory process priority" (Run Options tab of Advanced settings). Use the following table to determine your desired state:

Priority	Windows	Linux	Unix	MAC
Low	25%	10	30	10
Normal	50%	0	20	0
High	75%	-10	10	-10
Very High	100%	-20	0	-20

- **The "Evenly distribute sending inventory over X hours" setting should be utilized in larger environments.** Setting this configuration located on the Run Options tab of Advanced settings the Inventory task will allow the inventory returning to the Notification Server to span over a specified time frame. Note: this functionality is currently available for Windows only.
- **For recurring inventory tasks, its best to use a policy -** Policies have more options to work around systems that may be powered off at the scheduled time Inventory Policies rely on tasks
- **Review all Inventory Tasks before enabling them** – Inventory Tasks have all items enabled by default, this can result in significant database growth in some cases the per client database footprint can increase to over 10-20MB.
- **Avoid over scheduling of inventory gathering activities** - Increasing the frequency of an inventory task in an attempt to hit an "online window" will only cause redundant data to be sent to the NS. This increases the workload on the NS as the duplicate data must be still be processed and then discarded. Schedule inventory tasks to occur at the desired data refresh rate. This will allow the Altiris Agent to locally manage the inventory collection process.
- **Prevent over usage of the Collect Full Inventory policy and its associated Inventory Task** - Another common misconception is the perceived need to run a Full Inventory on a frequent basis. A Full Inventory is only necessary when the Inventory Agent believes that the NS has more information about a computer than what truly exists in the NS database. It is recommended to run Full Inventory on a monthly basis, but use the "Inventory process priority..." and "Evenly distribute sending inventory..." options to throttle how fast or when that inventory comes in.
- **Use the Resource Framework components in multiple cloned inventory policies in Large environments** – using targets developed to separate inventory policies by geographical, departmental, or other categories can spread the timing and receipt of inventory on the Notification Server. Large groups of computers will still simultaneously post their inventory data to the server; however, the NS will be busy for a few minutes as opposed to several hours, there will a reduction of SQL deadlock warnings in the NS log, and there will be a reduction in network traffic caused by agents re-posting inventory data after receiving an IIS "Server too busy" message.

Upgrading & Migration

Inventory Solution 7.0 contains its own custom upgrade framework components. This will ensure that the important information for this solution is captured during the migration process. The following lists the items that are important to the importing and exporting of Inventory Solution:

- **Inventory Solution defines a successful migration from 6.x to 7.0 by the following rules:**
  - Default and custom 6.x inventory policies will be converted to 7.0 tasks. Schedule and advanced run options will not be migrated.
  - Configuration settings will be migrated to 7.0 configuration settings
  - Metering 6.x policies will be migrated and disabled by default

- Customers will be able to use the custom inventory scripts that they had created in 6.x.
- Default and custom 6.x reports will be migrated into the legacy folder and will still be functional.
- Data classes can be migrate into legacy 6.x data classes for reporting purposes.
- Standalone inventory 6.x packages will not be upgraded.
- Customers will be able to use the custom inventory scripts that they had created in 6.x. Once migrated Software Management Solution is required to roll legacy custom inventory scripts out.
- Inventory data will not be migrated from old data classes into the new cross-platform data classes during the upgrade. This is due to extensive changes in the database structure 6.x inventory data cannot be ported directly into 7.0 data classes.

- **Due to extensive changes in the database structure, 6.x inventory data cannot be ported directly into 7.0 data classes**. However, during the upgrade customers will be able to export inventory data and then import it into the legacy data classes in the 7.0 database. This would allow legacy reports to still work properly.
- **Due to extensive changes in the database structure, Application Metering, Baselining and Historical data is not migrated to the Altiris 7.0 database.**
- **Custom 6.x reports will be migrated into Legacy Folders on the Altiris 7.0 Notification Server.** These imported reports will be able to report on the 6.x data but should be recreated to reflect the new 7.0 dataclasses.
- **Standalone inventory 6.x packages will not be upgraded** – these packages must be regenerated.
- **NS 6 Custom Inventory will migrate to NS 7 provided the following steps are taken:**

Before you upgrade to Altiris 7

1. Back up all the custom inventory scripts that you use with Inventory Solution for Windows 6.1 SP2.
2. Back up all the stand-alone inventory packages that you had created/customized for gathering the custom inventory.
3. Back up all the ini files from NSCap\bin\Win32\X86and bin\Win32\X86\Inventory Solution that invokes the AeXCustInv.exe. These ini files are specified as a command line parameter to AeXInvSoln.exe on the "Go To Program" page->Command line" for the inventory tasks.
4. Back up the NSCap\bin\Win32\X86\AeXPkgEditor.exe

Upgrade Process

1. The upgrade will migrate the custom dataclasses that you had created to NS 7.0 along with the inventory stored in those.
2. The upgrade will remove the any custom inventory scripts at InstallDir\Altiris\Notification Server\NSCap\bin\Win32\X86andatInstallDir\Altiris\Notificationserver\NSCap\bin\Win32\X86\Inventory Solution
3. If you had created any task to gather the standard inventory as well as the custom inventory, the upgrade will create task to gather the equivalent standard inventory, but not the custom inventory. You will manually need to create a task to gather the custom inventory as described further in this document.
4. The upgrade will install a folder "%installDir %\Altiris\NotificationServer\NSCap\bin\Win32\X86\Inventory\Custom Inventory 6.1" which contains the new agent for custom inventory. This agent consists of following files:
   - AeXInvSoln.exe – Same file as that was provided in 6.1 SP2. This Launches AeXCustInv.exe and AeXNSInvCollector.exe as specified in AeXInvSoln.ini.
   - AeXCustInv.exe – This is a different file than that was provided in 6.1 SP2. It behaves in the similar way that it used to in 6.1 SP2, but have few bugs fixed.
   - AeXNSInvCollector.exe – This is a different file than that was provided in 6.1 SP2. This behaves similar way that it used to in 6.1 SP2 but with the only difference that now it generates the NSEs in the new format that is required for posting inventory to NS 7.0.

- AeXNSEvent.dll – This is a new file, it was not present in 6.1 SP2. AeXNSInvCollector.exe uses this file for generating the NSEs in new format.
- AeXInvSoln.ini – Specifies an example of how to launch the AeXCustInv.exe and AeXNSInvCollector.exe
- AeXCustInvStd.cit – Sample custom inventory script from 6.1 SP2.

5. Then, you will need to make sure that the data classes that your custom inventory scripts use exist. Normally, those would be migrated during the upgrade. If not, you can create new data classes by going to Settings -> All Settings -> Discovery and Inventory -> Inventory Solution ->Manage Custom Data classes.

Licensing

- When a computer is set to the 'retired' state (or any other state with an exception of Active), a license will be freed up, BUT all associated with this resource inventory data will be purged.
- You can use existing 6.0 licenses for Inventory 7.0.
- Application Metering will no longer be a standalone product. Customers will need just the Inventory license.
- Licensing Example: If customer owns X licenses of Inventory 6.x and Y licenses of App Metering 6.x the customer will receive Z licenses of Inventory Solution 7.0 equal to whichever is greater of X or Y. So in this example customer will receive 1000 node license for Inventory Solution 7.0.

7.2 Software Management Solution

The Software Management Framework is a key component of the Symantec Management Platform. It consists of two components: the Definitive Software Library and the Software Catalog.

The Definitive Software Library is a centralized, secure location used to store the authoritative versions of software packages managed by an organization. The Software Catalog is a repository used to store meta data related to both managed and un-managed software.

The Software Management Framework enables administrators to intelligently manage software, by providing a common way to identify and detect software as well as defining relationships between software resources.

7.2.1 Requirements

In order to utilize Software Management Solution functions the following requirements must be met:

- Symantec Management Platform 7.0 must be installed
- Software Management Solution licensing should be in place
- The Altiris Agent should be installed on any resource you wish to distribute software
- The following provides a general list of supported platforms:

  - Windows XP SP2or later x64/x86
  - Windows 2000 Workstation SP4
  - Windows Vista RTM and SP1 (all)
  - Mac OS X 10.3.9(PPC)
  - Mac OS X 10.4.x(Universal binary)
  - Mac OS X 10.5.x(Universal binary)
  - RHEL 3 - x86, x64
  - RHEL 4 - x86, x64
  - RHEL 5 - x86, x64
  - SLED 10 - x86, x64
  - Windows 2000 Server SP4
  - Windows Server 2003 (SP,2/R2) x64/x86
  - Windows Server 2008 x64/x86
  - RHEL 3 - x86, x64
  - RHEL 4 - x86, x64
  - RHEL 5 - x86, x64
  - SLES 9 - x86, x64
  - SLES 10 - x86, x64
  - Solaris 9 - Sparc
  - Solaris 10 - x86, x64, Sparc
  - VMware ESX 3.0.1, 3.0.2, 3.5

7.2.2 Facts

- **Software Management Solution now supports two primary methods of software delivery:** Quick Delivery and Managed Delivery.
  - **Quick Delivery** enables administrators to create a software delivery task by simply selecting a software package and the target to which the package is to be distributed. By default, the software delivery task is set to run as soon as possible.
  - **Managed Delivery** enables administrators to perform more complex delivery jobs by creating policies comprised of one of more tasks and software packages.
- **Software Management Solution enables administrators to create Package Deliveries and Legacy Software Deliveries -** Package Deliveries are similar to Software Delivery Solution 6.x software delivery tasks. Legacy Software Deliveries are similar to Software Delivery Solution 6.x Task Server tasks. While administrators can still create Package Deliveries and Legacy Software Deliveries, support for these two methods of software delivery will likely be phased out in favor of Managed Deliveries and Quick Deliveries.
- **Managed Delivery functionality leverages the meta data from the Software Catalog** - The Managed Delivery wizard alerts administrators of the relationships between software resources. The Managed Delivery wizard will also alert the administrator of situations in which there have been updates to the selected software. It will also alert the administrator in situations where the selected software has been superseded by another software resource.
- **Managed Delivery is much more band-width sensitive than traditional methods of software delivery.** Before downloading a software package to a particular computer, Managed Delivery policies can use the software's detection rule to determine if it is already installed on that computer. This results in bandwidth savings, by ensuring that software does not get downloaded to computers on which it is already installed.
- **The Symantec SVS agent can be delivered to those computers that are managed by Software Management Solution licenses** - The SVS agent does not get installed with the Software Management Solution agent. It must be installed separately. The SVS agent is included in the Software Catalog. The default command line associated with the package for the SVS agent includes the license key required to install the agent. The same license key will be used to install the agent on each computer.
- **The Software Management Solution can natively distribute software packaged in the .VSA package format used by Symantec SVS** - However, it is not necessary to repackage an application into the .VSA format in order to take advantage of the software virtualization technology.
- **The Managed Delivery wizard enables administrators to seamlessly virtualize software as part of the distribution process by simply marking a check box -** This enables administrators to virtualize Windows-based software without repacking the application into the .VSA package format.
- **Managed Delivery policy with a recurring schedule functions as both a delivery policy and a compliance policy.** The same detection rule that is used to determine if the software is installed prior to downloading a package to a given machine will be evaluated on a periodic basis to determine if the software remains properly installed. If not, the software will be reinstalled.
- **Management Solution also provides other application management functionality -** For example, it can be used to identify and remediate situations involving invalid source paths, which could interfere with the self-healing of Windows Installer applications.
- **The Managed Delivery method of software distribution enables administrators to create policies that target end users -** When an end user logs on to a computer, the Altiris agent will refresh any policies related to that user. Following the policy refresh, any Managed Delivery policies that target that user will run according to the schedule defined for that policy.
- **The Software Portal has been re-designed -** The user-facing portion of the portal no longer requires the installation of Active-X controls. As a result, the Software Portal now supports the use of the Safari and Firefox browsers on Mac clients.
- **There have been several usability enhancements to the software portal -** For example, administrators can now designate whether software is should appear on the "recommended" list with respect to a given user or group of users. Software designated as "recommended" appears at the top of the list of available software displayed in the portal. Another usability enhancement is that users can now cancel requests after they have been submitted.

- **The software portal approval process now provides administrators with more flexibility -** Administrators can now defer taking action on some outstanding requests for a particular piece of software, while choosing to approve or deny other requests for the same software.
- **Software Management Solution includes the Wise Toolkit -** It consists of two tools. One tool included in the Wise Toolkit is the WiseScript Editor, which can be used to perform general administrative scripting tasks on Windows-based machines. The other tool in the Wise Toolkit is Wise InstallTailor, which can be used to create transform (.MST) files to customize the installation of software packaged in the Windows Installer (.MSI) format.

7.2.3 Assessment

In order to properly assess the Software Management Solution requirements, the following questions should be asked in order to determine what items need to be configured and to gain consensus on the design:

- Is there a need to distribute corporate applications regionally and/or globally?
- Is there a need to distribute corporate files (video, documents, templates)
- Do you currently have a software repository? (Wise, etc)
- What applications would you deliver quickly or on a schedule?
- What applications would you distribute based on user or computer based criteria?
- Do you have a need to publish or provide self service installation to certain applications?
- Is Symantec SVS used in this environment?

7.2.4 Design Considerations

Solution Design

- **Customers can use their own file share to house the Definitive Software Library –** The Library should not reside on the same server as the Notification Server, in order to avoid potential performance issues.
- **The Definitive Software Library and Software Catalog can be populated using the following methods:**
    - You can manually import packages into the Definitive Software Library and create associated entries in the Software Catalog as part of the software delivery process
    - The Software Management Framework agent can detect the key executable files that get installed by a package and add that data to an existing entry in the Software Catalog.
    - In the future, it may be possible for customers to import packages and data from external sources, such as Wise Package Studio or third-party vendors.
        - Wise Package Studio would be an ideal candidate for supplying data related to proprietary, in-house developed software as well as software that has been re-packaged.
        - A third-party vendor could potentially supply data related to commercial off-the-shelf software.
- **By default, Quick Delivery tasks are configured to execute as soon as possible -** However, administrators can configure Quick Delivery tasks to abide by defined maintenance windows by simply marking a check box.
- **Managed Delivery policies are configured to execute according to the defined schedule by default -** Administrators can configure the execution of the task portions of a Managed Delivery to respect defined maintenance windows.
- **The baseline inventory functionality found in Application Management Solution 6.x is not included in Software Management Solution 7.0.** The baseline inventory functionality is part of Inventory Solution 7.0.
- **There are no client-side user interfaces for Managed Deliveries on Linux, Unix and Mac computers in Software Management Solution 7.0.**
- **The tools included in the Wise Toolkit are not currently localized and do not offer Unicode support.** In addition, the WiseScript Editor does not currently offer full support for managing computers running Windows Vista or 64-bit operating systems.

- **The SVS Admin tool found in the Symantec Software Virtualization Solution is not included in Software Management Solution 7.0.** This means that Software Management Solution does not include any SVS related software packaging tools. Customers can continue to use the software.
- **Software Management Solution 7.0 enables customers to create software delivery related notification policies, but does not include any default notification policies.** The default notification policies included in Software Delivery Solution 6.x are no longer applicable, due to changes in the underlying technology.
- **The reports included in Software Management Solution are based on the reports previously included in Software Delivery Solution, Application Management Solution, and Software Virtualization Solution -** Every report included in this product was reviewed, for the purpose of identifying opportunities to consolidate existing reports. The results of this exercise were as follows:
    - A handful of the 6.x software delivery reports (i.e. "Legacy Reports") were simply updated to work "as is" with the new report controls introduced in Symantec Management Platform 7.0.
    - The Legacy Reports will include software delivery data from both 6.x and 7.0.
    - Software Management Solution also contains several new reports. The new reports present the same type of data that was present in the 6.x reports, but are significantly fewer in number.
    - The new Application Management reports will not include data from 6.x, because Application Management Solution 6.x data cannot be migrated to 7.0.
    - The new Software Portal reports will not include data from Software Delivery Solution 6.x, because the software portal data cannot be migrated.
    - The new software virtualization related reports will not include data from Software Virtualization Solution 6.x.

Upgrade/Migration

- **Data from the following 6.x solutions can be migrated to 7.0:**
    - Software Delivery Solution (for Windows) 6.x
    - Software Delivery Solution for Linux, Unix and Mac 6.x
    - Software Virtualization Solution 6.x
- **Data from Application Management Solution 6.x cannot be migrated to 7.0.**
- **Software packages from Software Delivery Solution 6.x and Software Virtualization Solution 6.x are imported as Software Package resources -** Software programs from Software Delivery Solution 6.x and Software Virtualization Solution are imported as Program items. The association between a software package and program is maintained during the migration process.
- **Migrated software packages and programs do not get automatically associated with an entry in the Software Catalog -** Following the migration process, administrators can use the migrated software packages (and related program data) to create new entries in the Software Catalog or associate them with existing entries in the Software Catalog.
- **Software Delivery Solution 6.x tasks are migrated using the following rules:**
    - Software Delivery tasks are imported as "Legacy Software Delivery policies"
    - Software Delivery Task Server tasks are imported as "Package Deliveries"
    - Sequential Software Delivery tasks are imported as "Managed Deliveries"
- **Data related to software portal requests submitted by users and the policies created to fulfill requests cannot be migrated -** However, software portal configuration settings for a software delivery package (e.g. "Install Software" and "Install on Approval") can be migrated.
- **Software Virtualization Solution 6.x tasks are migrated using the following rules:**
    - Virtual Software tasks are imported as "Legacy Software Delivery policies"
    - SVS Task Server tasks are imported as "SVS Command tasks"
- **Application Management Solution 6.x installation state policies cannot be migrated to 7.0 -** They must be re-created as Managed Delivery policies.
- **Application Management Solution 6.x tasks to repair Windows Installer applications and tasks to update Windows Installer source paths must be re-created** as Application Management tasks in Software Management Solution.

Hierarchy and Replication

- **Software Management Solution supports the full and differential modes of replication.** The differential mode of replication only replicates those items which have changed since the last replication.
- **Software Management Solution supports full integration** - which means items will be managed and replicated by the hierarchy. This enables administrators to create tasks and policies at the top level Notification Server and replicate them to child level Notification Servers. The following items can be replicated:

Items	Replicate	Direction
Tasks (Quick Delivery, Package Delivery, Source Path Update, Window Installer Deliveries)	Yes	Down/Up
Policies (Legacy and Managed Deliveries)	Yes	Down/Up
Software Components	Yes	Down
Events	Yes	Up
Data Classes	Yes	Down/Up
SMS Agent Task, Package and Program	Yes	Down
Reports	Yes	Down/Up
Computer/user resources, collections	N/A	N/A
Security Permissions, Roles, Privileges	Yes	Down/Up
Items under folder (Software Catalog and Software Library Settings)	No	N/A
Items under folders (Software Portal Settings, Software Portal Agent Settings)	No	N/A
Items under folder (Application Management\windows)	Yes	Down

Licensing

- Software Management Solution is a cross-platform product that can be used to manage clients of servers. It is available as a standalone product and as part of Client Management Suite and Server Management Suite. In the future, Software Management Suite will likely also be available as part of Total Management Suite 7.x.
- If you are covered by Annual Upgrade Protection and own Software Delivery Solution for Clients licenses, but no licenses of Software Delivery Solution for Servers, the existing Software Delivery Solution for Clients licenses will enable them to use Software Management Solution.
- If you are covered by Annual Upgrade Protection and own Software Delivery Solution for Servers licenses, Symantec will provide them with a new license file that will enable them to use the Software Management Solution to manage their servers.
- If you are covered by Annual Upgrade Protection and own standalone licenses of the Application Management Solution that were not purchased as part of a suite and is using those licenses to manage computers that are not consuming Software Delivery Solution licenses, you may be able to exchange those Application Management Solution licenses for Software Management Solution licenses. Such situations will be handled on a case-by-case basis by the sales support center.
- If you are covered by Annual Upgrade Protection owns standalone licenses of the Application Management Solution that were not purchased as part of a suite and is using those licenses to manage baseline inventories on computers that are not consuming Inventory Solution 6.x licenses, you may be entitled to Inventory Solution 7.0 licenses in exchange for the Application Management Solution licenses. Such situations will be handled on a case-by-case basis by the sales support center.

7.3 Patch Management Solution

7.3.1 Requirements

In order to utilize Patch Management Solution functions the following requirements must be met:

- Symantec Management Platform 7.0 must be installed
- Patch Management Solution licensing should be in place
- The Altiris Agent must be installed on any resource you wish to distribute patches
- The Software Update Agent must be installed on any resource you wish to distribute patches
- The following provides a general list of supported platforms:

Platforms:

- Windows 2000 Professional SP4
- Windows 2000 Server SP4
- Windows 2000 Advanced Server SP4
- Windows XP all SPs (32/64-bit)
- Windows XP Tablet PC Edition 2005
- Windows Vista SPs (32/ 64-bit)
- Windows Server 2003 all SPs (32 /64-bit)
- Windows Server 2008
- Red Hat Enterprise Linux WS, ES, AS 3 (x86, x86_64)
- Red Hat Enterprise Linux WS, ES, AS 4 (x86, x86_64)
- Red Hat Enterprise Linux 5 (x86, x86_64)
- Red Hat Enterprise Linux Desktop 5 (x86, x86_64)
- SUSE Linux Enterprise Server 9 SP4
- SUSE Linux Enterprise Server 10 all SPs
- SUSE Linux Enterprise Desktop 10 all SPs

Languages:

- English
- Japanese
- Spanish
- Portuguese (Brazil)
- Simplified Chinese
- French
- German
- Dutch
- Russian
- Italian
- Swedish
- Chinese (Traditional)
- Czech
- Korean
- Norwegian
- Danish
- Polish
- Portuguese (Portugal)

7.3.2 Facts

- **Patch Management Solution takes inventory of managed computers to determine the operating system and application software updates (patches) they require.**
- **The solution then downloads the required patches and provides wizards to help you deploy patches** - Patch Management Solution also enables you to set up an automatic patch update schedule to ensure managed computers are kept up-to-date with the latest vendor security updates, and protected on an on-going basis.
- **A Comprehensive software repository automates the download from the vendor site before distribution without administrator intervention** - The repository provides comprehensive data on software bulletins, software updates, and inventory rules, such as technical details, severity ratings, and number of executables.
- **The software update agent automatically analyses managed computers and gathers patch-specific inventory for determining supported operating systems** - Applications and the associated service pack level, and whether a patch is required or not. Inventory results populate predefined targets based on the returned data. The
- **Compliance on all Notification Servers configured in a Hierarchy can be reported** on - A report is available that can be used from the top level of a hierarchy to view compliance numbers for each member of that hierarchy.
- **PMImport data replication** – With the use of hierarchy, PMImport data can now be replicated across multiple Notification Servers. The result is less time required to configure PMImport on individual Notification Servers. *Note: Patch Management for Linux 7.0 will not support data replication in the GA release – it is currently planned for 7.0 SP1.
- **Disable superseded updates** – An option was added to the Microsoft Patch Management Import task (PMImport), which will automatically disable ALL superseded updates. If enabled, this will run at the completion of any Import task.

- **Patch package cleanup task** – A new task is available to assist in maintaining a "clean" Patch environment with respect to Patch packages. Run this task on a regular basis to ensure all packages are in sync with console settings.
- **More intelligent Inventory Rule Web Service** – Client machines will only download pertinent inventory rule sets based on OS version and installed software, resulting in less bandwidth consumption and resource use during assessment scans
- **Quicker distribution of software updates** – Behind-the-scenes resource targeting has been re-factored to be more precise and efficient.
- **Support for patching SUSE Linux Enterprise has been added.**
- **Red Hat Satellite Server Requirement has been removed**

7.3.3 Assessment

When designing the patch management solution you should ensure that the following questions are answered in order to properly design your implementation:

- What OS languages do you support?
- Are there any Microsoft Applications absent from your environment (ISA Server, Office 97, etc.,)
- Is Vulnerability and compliance Reporting a critical requirement?
- Is there a requirement to centralize Patch management?
- Do you have a reboot policy in place?
- Would you consider Patch Management critical enough to override maintenance windows?
- Do you wish to notify the user of a patch?
- Do you wish to allow the user to defer a patch reboot or installation?

7.3.4 Design Considerations

Solution Design

- **Software Update Agent strictly abides by the configured Maintenance Windows -** This will allow customers to be able to patch servers and desktops within their respective maintenance window rather than just applying a patch to a wide grouping with a global agent policy. If desired, the user may choose to override a Maintenance Window and schedule an update for immediate installation.
- **When setting an installation schedule for software updates, several Time Zone options are available.**
    - Use agent time – Install updates based on the agents local Time Zone
    - Use server time – Install updates based on the Notification Server's Time Zone
    - Coordinate using UTC – uses Coordinated Universal Time to install updates
- **Patch Management Solution for Linux 7.0 will leverage Red Hat Network login credentials (provided by the customer) to access the Red Hat Network directly -** Red Hat errata will be stored locally in the Notification Server database as well as the physical RPM packages.
- **Patch Management Solution requires that customers have valid, up-to-date paid subscriptions to either the Red Hat Network and/or the Novel Customer Center -** Valid login credentials to these sites are required to access updates available for entitled machines.

Hierarchy & Replication

- The following functions are provided when Patch Management Solution is configured in a Hierarchy:
    - **Push the PMImport files to a Child NS -** Normally the PMImport file has to be downloaded from an Internet facing machine; we are now allowing a Child NS to have these files receive it from its Parent.
    - **Allows a subset of the PMImport languages to be distributed to the Child.** For example, the Parent can import up to 18 languages into the Database, the Child may request as few as one language, and only those languages requested from the Child will be sent out. If a Child NS is in a Hierarchy, the Parent will control whether they get the PMImport file from the Internet (normal behavior) or that it will pushed down from the Parent.

  - **Roll out of Updates (Called a Software Update Advertisement Set Policy) can be pushed down to Child NSs.** This means that a Parent NS can control which Bulletins or Updates have been tested for Distribution and Control the Reboot behavior and other distribution options. The Child NS can control the schedules that these updates occur on (i.e. Override Maintenance Window Behavior) and the Resource Targets, and Reboot options etc.
  - **A Parent NS can get a summary of Vulnerability and Compliance (From a Patching perspective) for its own resources AND all resources attached to its Child NSs (and grandchildren etc).**
- **When Hierarchy is enabled and the Patch Management Import (PMImport) data replication policy is enabled, "child" Notification Servers will download their PMImport data directly from their "parent" node -** If the customer is supporting multiple languages, all languages that the customer desires to support will have to be imported on the root node in the Hierarchy and then each individual NS can be configured to download all or a subset of those languages.
- **Patch Management for Linux will NOT support data replication within the Hierarchy** – due for a later release
- **Support for language selection within Hierarchy replication Requires parent to download <u>all</u> desired languages -** child NS's can request subset of languages.
- **Hierarchy structure for heavy Patch Management users in Large environments** - If you will be using Hierarchy and depend heavily on Patch Management and the ability to report on information from a top-level NS in the Hierarchy, we recommend that the structure remain as flat as possible. For performance concerns, we do not encourage customers to configure their Hierarchy in such a manner that multiple NSE's need to replicate data from other NSE's up the Hierarchy chain. We recommend that the data be replicated up through 1 level only.

Upgrade/Migration

- **Inventory Solution defines a successful migration from 6.x to 7.0 by the following rules:**
  - All Options for General Policies will be imported into 7.0 (includes details like Managed Languages, Resource Exclusions, Default Resource Targets, Package Defaults etc)
  - Agent Configuration Policies (and Clones) Imported into the 7.0 system – **Note** that any non-default Base Collections (6.x) Imported into 7.0 as Resource Targets
  - Every Software Bulletin Policy (6.x) imported into system as new Software Update Advertisement Set Policy (7.0) - Note that Packages / Programs / Advertisements are not imported – they are created again by the 7.0 version of Patch from the Imported Migration XML
  - Reports and Resource History will not be imported into 7.0
  - Old Inventory Policies are now obsolete and therefore will not be imported into 7.0
  - Old style Item Tasks (6.x) have now been converted into 7.0 Task Server Tasks – however the settings should be migrated across (where the options still remain in 7.0)
- **Agent upgrade: 7.0 Altiris Agent will NOT load 6.x agent plug-ins**
- **Inventory rule cache file will be recreated after Inventory Rule Agent upgrade** – This will result in a slight increase of network traffic

Licensing

- When a computer is set to the 'retired' state, a license will be freed up and made available for another node of Patch Management.
- You can use existing 6.0 licenses for Patch 7.0. However, the Patch Management EULA has been updated to include specific wording around entitlements.
  - If Patch Management Solution for Clients or CMS has been purchased you are entitled to patch client machines only.
  - If Patch Management for Servers or SMS has been purchased, you are entitled to patch servers only.

8 Migration to Client Management Suite (CMS) v7

8.1 Introduction

When you upgrade from Client Management Suite 6.0 to Client Management Suite 7.0, you can migrate resources and solution configuration data. If you perform the upgrade on a single computer, you must migrate all of your data during the migration process. If you upgrade from one computer to another, then you can perform partial migrations.

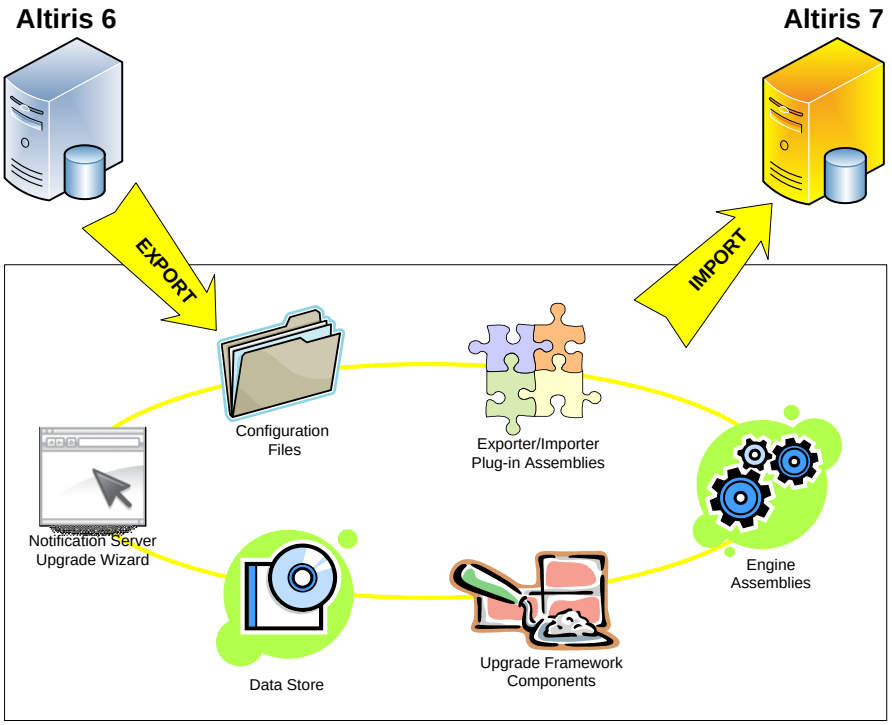
Upgrading from Client Management Suite 6 .0 to 7.0 is a major upgrade and involves comprehensive changes to the platform and solutions. The most significant change is that you create a new Notification Database or CMDB for Notification Server 7. Because of the new database and the changes it results in — moving data from one database to another— the upgrade is known as a migration.

To migrate Client Management Suite 6.0 data to a Client Management Suite 7.0 installed server, you use a data migration wizard. You use this wizard to export the data to a data store and then import the data to the Client Management Suite 7.0 server. Each individual solution has their own exporters and importers. These exporters and importers define what data you can migrate.

There are many considerations when you prepare for an upgrade, including gathering information, making decisions, and preparing your environment. Taking the time to prepare for the upgrade and understand the upgrade process can make the upgrade process run more smoothly and can help you mitigate any issues that arise during the upgrade.

8.2 Upgrade Framework Components

The upgrade framework performs the migration to Altiris 7. The Symantec Installation Manager (SIM) is a piece of software that installs everything during the migration. Installing SIM begins the migration process, and then SIM runs throughout the migration process performing checks, installing files and products, and starts the Altiris Notification Server Migration Wizard when needed.



The migration process in Altiris 7 has been redesigned to give you more control. For example, you can now specify the location of the installation files and a data store, which stores data files from the Client Management Suite 6.0 database. The Specific elements and processes are described below:

Configuration Files

Files that drive the export and import process. Each Altiris solution provides its own configuration files that list the exporters and importers that are needed to upgrade that solution. Configuration files are important because they provide the initial settings that direct the exporters and importers on how to initialize their filters.

Engine Assemblies

The core component that controls the export and import process. When initialized, the engine loads all the exporters and an importer defined in the configuration files and initialize them. The engine then determines the correct order that the exporters and importers should be called and directs each exporter or importer to perform a data export or import.

Exporter/Importer Plug-in Assemblies

The exporter plug-in assembly and the importer plug-in assembly are new features in Altiris 7. The exporter assemblies export the data from Client Management Suite 6.0 to a data store. After the Client Management Suite 7.0 installation is finished, the importer assembly imports the data from the data store into your clean Client Management Suite 6.0 database. The Exporter/Importers contain the following features to ensure a successful migration process:

- Uses filters to enable or disable data to be exported or imported
- NS upgrade framework conducts readiness checks to ensure required product are installed
- Warning messages display if there are issues
- User can still upgrade, even if some of the products are not ready

The exporters and importers are initialized from XML, and then use XML to configure a set of filters. In the Upgrade Wizard, a list of filters is displayed enabling you to determine the data to export and import. Although you have the ability to select the data to export from NS 6, best practice is to export all data. This recommendation is critical for an on-box migration because the export can only be run once. During the data import process, you can set filters and decide which data to import into the Client Management Suite 7 .0 database. You can also import multiple times.

The Data Store

The data store is a file or repository that holds data during the upgrade process. You use the exporter plug-in assembly and importer plug-in assembly to enter and remove data from the data store. The data store organizes the data it holds into tables by solution. This helps make the information easily identifiable and retrievable. The Data store performs the following functions:

- Stores data from multiple solutions
- Is a file for ease of use
    - Easy to copy and backup
    - Not dependent on SQL
- Tables in the data store have unique names
- The names identify tables for each solution <SolutionName>.<Store Table Name>

Symantec Installation Manager

Symantec Installation Manager (SIM) is software that installs all files for the migration. SIM gathers information about you for trade compliance and performs a readiness check on your system to ensure it is ready for the migration. After your system is ready, SIM downloads the files you need to perform the migration, guides you through the export, uninstalls Client Management Suite 6.0 if needed, installs Client Management Suite 7.0, and then guides you through the import.

The Upgrade Wizard

The Upgrade Wizard is the user interface component that guides the user through the export and import process. The Upgrade Wizard runs as part of the NS upgrade framework. Its purpose is to guide you through the upgrade process. This is one aspect of the upgrade process that has been redesigned to give an administrator more control. For example, the Upgrade Wizard lets you customize the export and import files, and determine the location of

the data store. As part of the export and import process, you can create filters to refine the types of data to export and import.

SIM starts the Upgrade Wizard as part of the migration when the data export needs to occur. After the Upgrade Wizard has completed the data export, it restarts SIM. After SIM has uninstalled Client Management Suite 6.0 (if needed) and installed Client Management Suite 7.0, it restarts the Upgrade Wizard. In the Upgrade Wizard import dialog boxes, you can define what data to import into the clean Client Management Suite 7.0 database.

Upgrade Framework Components Within Altiris Solutions

Each Altiris solution has its own NS upgrade framework components that are custom to that solution. This ensures that the important information for a solution is captured during the migration process. To upgrade, each Altiris solution:

- Has its own .MSI (Windows Installer file)
- Has its own configuration files
- Has its own exporter/importer plug-in assemblies
- Determines what information to export and import

8.3 Prerequisites

8.3.1 Installation Requirements

Before you can upgrade to Altiris 7, you need to verify that your Notification System, Altiris Agent, and Site Servers are version 7.0 ready. Compare your current environment to the requirements in this section to ensure you are prepared to upgrade to Client Management Suite 7.0

8.3.2 System Requirements

	Source Notification Server	Target Notification Server
Hardware	Sufficient storage space for NS 6.0 Data if the data file is to be saved on this server.	· Pentium 4 - 1.8GHz · 1 GB RAM · NTFS file system · 10GB free disk space · Space for Packages, DB
Software	· Notification Server 6.0 R8 · Altiris Agent 6.0 SP3 or later · Current Altiris Solutions (This can be found in the Solution Center under "Currently Installed Solutions". Look for the "Upgrade" Button on any of the solutions listed.)	· Windows 2003 32-Bit SP1 · MS SQL 2005 SP2, 32-Bit (64-bit Off Box) · 2005 Express Edition SP2 · .NET Framework 3.5 · Internet Explorer 7.0

8.4 Client Management Suite Migration Procedure

The type of upgrade you perform in your environment depends on where you plan to install Client Management Suite 7.0. If you are upgrading on the same server, you use an on-box upgrade. If you are installing Client Management Suite 7.0 on a different computer than where Client Management Suite 6.0 is, you perform an off-box upgrade.

	On-box Upgrade	Off-box Upgrade
Benefits	More automated process and You do not need an additional SQL & OS License	Faster installation because you do not need to uninstall NS 6 before installing NS 7. The NS 6 database remains intact.
Challenges	You do not have NS 6 as a safety net to return to if something happens to NS 7.	Running NS 6 and NS 7 concurrently requires an additional SQL & OS license.

8.5 Migration Planning

Pre-requisites will vary based on size and complexity of your current operational environment. If you are an organization with < 500 devices being managed by a single Notification Server (NS6) many of the data points below do not apply.

8.5.1 Common for any sized environment

Ensure you have the latest snapshot of the Client Management Suite 6.0 environment to include:

- Existing Notification Server 6.0 management and configuration settings
  - Custom Collections, Reports, Policies, and Dataclasses
  - Custom Console settings
  - Console Security settings
  - Sites (AD Import rules, or custom)
- Existing Database Server configuration and maintenance policies
- Existing Package Server deployment and hardware/software configurations
- Existing Task Server deployment and hardware/software configurations
- Managed endpoint versions (Windows, Unix, Linux, and Mac); total count and remote locations
- Network Topology (LAN, WAN, subnets etc), and existing communication ports/protocols (custom ports, HTTP, HTTPS, UNC)
- Active Directory implementation (Domains/Sites/OUs) and Workgroups
- Security Roles and Policies (Business Model)
- Solutions features implemented and planned (what is licensed, features enabled, new features planned etc...)

8.5.2 Two or more Client Management Suite 6.0 servers deployed; multi-location:

- Data Centers
- DMZ (NS deployed in DMZ dedicated to managing internet facing endpoints)
- Total number of endpoints assigned per Notification Server
- Total number of Package Servers assigned per Notification Server and Site assignment
- Total number of Task Servers assigned per Notification Server and agent assignment (via Collection model)
- If enabled - gather Inventory Forwarding Rules (data replicated, and flow)
- If enabled - gather Package Replication Solution enabled (data replicated, and flow)

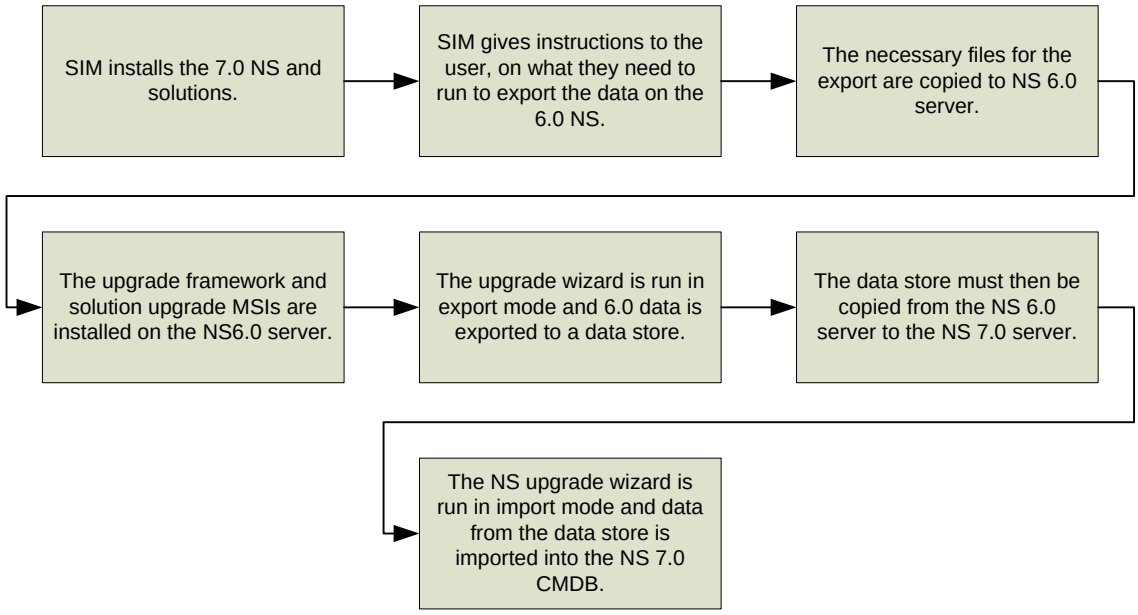
8.5.3 Off-box Upgrade Process Overview

An off-box upgrade is different from an on-box upgrade because the upgrade is not occurring on the same computer. The other differences are:

- Client Management Suite 7.0 solutions are installed before Client Management Suite 6.0 is decommissioned. This can occur because they reside on different computers.
- Symantec Installation Manager leaves the Client Management Suite 6.0 database intact and does not uninstall it. There is no need for Client Management Suite 6.0 to be uninstalled because Client Management Suite 7.0 is residing on a different computer.

A concern with off-box upgrades is how the .dll and configuration files for NS and each solution are installed on both computers. SIM addresses this by calling the Upgrade Wizard in the background to ensure that the .NET run-time environment files are installed on the Notification Server. To run SIM, you must have Internet access.

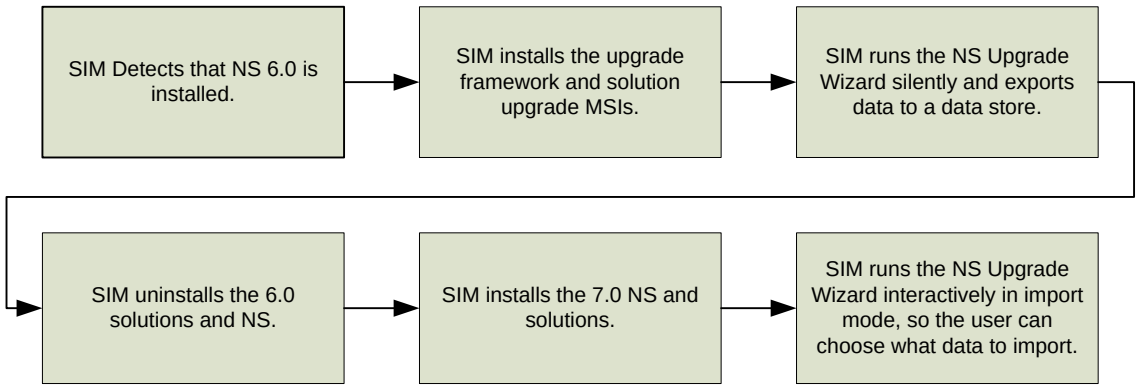
You can either run the upgrade on a computer with Internet access and that has SIM installed or copy the SIM installation to a computer that has Internet access and run the installation on that computer. The following diagram illustrates the process flow of the off-box upgrade:



8.5.4 On-box Upgrade Process Overview

The best practice recommendation is to perform an on-box upgrade when you are ready to upgrade Client Management Suite 6.0 to Client Management Suite 7.0. This ensures that all data is migrated. Additionally, this on-box upgrade prevents situations and potential performance issues with Client Management Suite 6.0 solutions running on Client Management Suite 7.0. Upgrading is designed to be performed once, so waiting until all plug-in applications for Notification Server are released is a recommended approach.

You can import incrementally and as needed, but you cannot export. Best practice is to only run the export once. You can run the export multiple times, but it is not recommended. Doing so means you risk putting old data or data you might not want in your clean database. During an on-box upgrade, the database remains intact. The following diagram illustrates the process flow of the on-box upgrade:



8.6 Migration of Client Management Suite 7.0 Solutions

All solution migration design considerations have been documented in their respective sections within this document. Please refer to Section 7 under the sub sections named “Design Considerations” for each solution to see a comprehensive overview of migration considerations.

8.7 Package & Task Server Migration Procedure

Package Servers may be upgraded in the NS 7 Upgrade, the following is a list of what will be upgraded:

- **SWDPackageServer:** The upgrade framework will only import user defined packages and will not import core packages. This means the version of the core package (in the SWDPackage table) will not be decremented. Having the data in the SWDPackageServer table for core packages is not a problem, because the importer will mark the status as 'Stale codebases' if the version is different. This will resolve itself once the package server has downloaded the package or the package refresh runs.
- **PackageServerSite:** All Items will be migrated as they are to NS7.0
- **SWDPackageSite:** All Items will be migrated as they are to NS7.0
- **PackageSiteActivityLog:** All Items will be migrated as they are to NS7.0
- **SWDPackageCodebase:** Only non NS codebases will be imported. All NS codebase will be regenerated in NS7.0 after package refresh schedule runs.
- **Constrained Package Servers:** All constrained package server will be migrated as they are to NS7.0
- **Sites and Subnets:** All Sites and Subnets as well as their associations will be as they are in NS6.X

8.8 Client Migration Procedure

Once the Notification Server is migrated to 7.0 there will be a need to upgrade existing agents. The Altiris Agent upgrade policy can simply be turned on and the NS 6.x agents will apply the policy and upgrade the agent to the latest 7.x version. In order for this process to complete successfully the following items should be observed:

- A resource with the Altiris 6 Agent does not communicate with the NS 7 server. If the database contains that specific resource, it will use this information to allow the NS 7.0 Agent Upgrade policy to target the resource for an upgrade.
- Verify that computer resources that already have the Altiris 6 Agent installed exist in the CMDB before the computers start communicating (i.e. The Resources have been imported into the NS 7.0 infrastructure). Overlooking this detail can result in the resources appearing new to the NS, which means that they will be assigned a new GUID and cause duplicate resources in the database or cause the old and new resources to merge.
- The Agent upgrade process uninstalls the NS 6.x agent and all of its sub agents, then installs the new 7.0 agent onto the resource. Rolling back the agent to 6.x would involve the automated uninstallation of the 7.0 agent and new push from a NS 6.x console or automated process.

8.9 Post Migration Configuration Adjustments

Collections, Reports, Data Classes, and Notification Policies

You can migrate collections, reports, data classes, and Notification policies from NS 6 to NS 7. These items change properties in NS 7, and collections and Notification policies also change names. The following considerations should be observed after migrating the server to NS 7:

- In the NS Upgrade Wizard, you have the ability to specify whether custom collections (in NS 7, called filters), reports, and data classes are migrated into NS 7. Once migrated, they become read-only and are stored in a folder titled Legacy.
- Test NS 6 reports after the upgrade to make sure that they run properly. Because several underlying tables have changed in NS 7 (such as the “Item” table), your report may be referring to a different table or table that no longer exists. Retest custom reports in particular. NS 6 reports that you migrate become read-only.
- The “Item” table in NS 7 is significantly different, as it no longer contains resource items.
- Notification policies are migrated, but they are replaced with automation policies and become read-only files stored in the Legacy folder. You can view these files using the Policies and Tasks Web pages.

8.10 Database and Tables

In NS 7, the required data from the "Item" table was partitioned into smaller tables that are specific to each resource type. This reduces the storage space and the load on the "Item" table. The following are the most significant changes to the database tables in NS 7 and may affect data you import into NS 7 and other Altiris solutions:

- In the "Item" table, the ClassGuid column has been removed. A new "ItemClass" table now contains a mapping of an item's GUID (Global Unique Identifier) to its Class GUID. All items, including resources, have a row in the "ItemClass" table.
- In the "ItemResource" table, the ResourceId column has been removed. The Guid, ResourceTypeGuid, and Deleted columns are still in the "ItemResource" table, but the data these columns store has moved to the new custom resource table.
- If the IsManaged column contains a resource type with an IsManageable attribute, then the data is stored in the "ItemResource" table. Otherwise, the data in the column is stored in the custom resource table. The "ItemResource" table still stores data for non-customized resource types. Customized resource types store their data in the custom resource table.
- The default database name is Symantec_CMDB. You can edit this name in the SIM console.
- Resources that have been partitioned move to new partition tables.
- Partitioning a resource type causes the NS upgrade to run slowly. The slowness occurs during the resource type registration, as the resource data for any resources that have been partitioned move from the existing database tables to the new partitioned tables.

8.11 Migration Best Practices

Before you start the upgrade process, there are some tips, tricks, and general information about upgrading that you should know that can help make your upgrade run more smoothly:

- Upgrade NS 6 and all Altiris 6 solutions simultaneously.
- If you have multiple NS's, you can stagger upgrades and only upgrade a specific NS at a time.
- If you do this, be sure to exclude the specific NS 6 from the export until you are ready to export all data. This is important because the export can only be run once for an on-box migration, and you want to run it when it can capture all data versus partial data.
- Upgrade NS 6 and all Altiris 6 solutions at the same time to get them to the required versions for export – The export can only run once (on-box).
- Do not attempt to install NS 7 on an NS 6 separately, as this is not recommended or supported.
- Reduce the size of your NS 6 database before upgrading to NS 7. Items that can be performed:
    - Reviewing the Purge Maintenance and History Tracking policies to acceptable levels like setting the data retention of data classes and History to 1 Month and 100,000 rows where appropriate.
    - Cleaning up Active Directory Users and Computers imported into NS 6
    - Deleting or 'Retiring' Computers that are no longer active in NS 6.0
    - Deleting unused reports
    - Deleting unused policies, tasks and packages
    - Deleting collections that are not in use
- Export Everything when exporting data, you will be able to choose what you want to import during the upgrade.
- Verify files for all Altiris 7.0 products are in the repository.
    - The Readiness check is skipped if they are all present
- Altiris Agent Upgrade: Verify that computer resources exist in the NS 7.0 CMDB before the computers start communicating (Results in duplicate resources)

8.12 Migration Resources

Refer to the following Knowledge Base articles to ensure you are prepared to meet the minimum and/or recommended requirements to migrate from Altiris 6.x to Altiris 7.0. As a basis to all solutions the Symantec Management Platform defines the supported and unsupported managed OS platforms, as well as NS server side OS platform and technology requirements:

References:

- http://kb.altiris.com
  - KB43648 – Support FAQ for Symantec Management Platform
  - KB37648 – Symantec Management Platform 7.0 Release Notes
  - KB19750 – Notification Server Maintenance
  - KB45092 – Improving Performance of your Symantec Management Platform
  - KB33867 – Notification Server and Non-Standard Ports
- Symantec Installation Manager Guide – Online help reference, and available when the Installation Manager is downloaded
- Symantec Management Platform User Guide – Online help reference