Linux and UNIX Management Guide with Symantec™ Server Management Suite 7.6 powered by Altiris™ technology
performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com
Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

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

**Licensing and registration**

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


**Customer service**

Customer service information is available at the following URL:


Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals
Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan           customercare_apac@symantec.com
Europe, Middle-East, and Africa  seema@symantec.com
North America and Latin America  supportsolutions@symantec.com
Technical Support ........................................................................................................... 4

Chapter 1 Introducing UNIX/Linux Management in Symantec Server Management Suite 7.6 powered by Altiris Technology. ................................................................. 14
  About this Guide .......................................................................................................... 14
  Symantec Server Management Suite 7.5 SP1 powered by Altiris technology: UNIX and Linux management capabilities ........................................ 15

Section 1 Provisioning UNIX and Linux Servers .................................................. 19

Chapter 2 Setting up Linux client computer ..................................................... 20
  About Deployment Solution .................................................................................... 20
  Components of Deployment Solution ............................................................... 21
  Creating and deploying Linux disk images ....................................................... 22
    Preparing to capture an image .......................................................................... 25
    Creating a Linux image .................................................................................. 26
    Deploying a Linux image .............................................................................. 28
    Scheduling a deployment job or task .......................................................... 31

Chapter 3 Server configuration ............................................................................. 32
  Creating system configuration settings .............................................................. 32
  Creating or modifying tokens in Deployment Solution ...................................... 33

Section 2 Discovery and Inventory of Linux and UNIX Servers .......................... 34

Chapter 4 Discovery and Inventory ...................................................................... 35
  About Network Discovery .................................................................................... 35
  Discovering UNIX and Linux computers ......................................................... 36
  About Inventory Solution ........................................................................................ 37
  About software inventory on UNIX/Linux servers ............................................. 38
About Inventory Pack for Servers ................................................................. 39
Viewing MySQL and Oracle Database inventory ........................................ 39
About Apache HTTP Server inventory ......................................................... 40
Gathering inventory on UNIX/Linux servers ............................................. 41
  Installing the inventory plug-ins on UNIX and Linux computers ........... 42
  Gathering inventory using predefined policies or tasks ......................... 43
  Gathering and viewing software inventory of the native UNIX/Linux package system .......................................................... 45
  Viewing inventory data in reports ......................................................... 45
About custom inventory data classes ......................................................... 46
Custom inventory sample script for UNIX, Linux, and Mac ....................... 47
Gathering custom inventory on UNIX/Linux servers ............................... 48
  Creating and configuring a data class .................................................. 49
  Creating a custom inventory script task .............................................. 51
  Configuring the custom inventory sample script for UNIX, Linux, and Mac .......................................................... 53
About software inventory using the filescan.rule file ............................ 54
Running software inventory on UNIX, Linux and Mac computers using the filescan.rule file .......................................................... 55

Chapter 5  Agentless inventory of UNIX and Linux servers ................. 57
About gathering agentless inventory ....................................................... 57
Gathering agentless inventory ............................................................... 58
  Creating agentless inventory tasks using the wizard ........................... 59
  Manually creating, scheduling, modifying, and stopping agentless inventory tasks .......................................................... 60
  Viewing agentless inventory results .................................................... 62

Section 3  Configuration Management ................................................. 63

Chapter 6  Installing the Symantec Management Agent for UNIX, Linux, and Mac ....................................................... 64
About the Symantec Management Agent for UNIX, Linux, and Mac ......... 64
About agent registration ....................................................................... 65
Methods of installing the Symantec Management Agent for UNIX, Linux, and Mac .......................................................... 66
Installing the Symantec Management Agent manually on UNIX, Linux, and Mac computers .......................................................... 67
Creating a CSV file for importing UNIX, Linux, and Mac computers ....................................................................... 68
Symantec Management Agent for UNIX, Linux, and Mac installation prerequisites .................................................... 69
Creating an agent registration policy .......................................................... 70
Specifying the Symantec Management Agent for UNIX, Linux, and Mac installation settings .............................................. 72
Installing the Symantec Management Agent for UNIX, Linux, and Mac with a manual pull ...................................................... 73
Manually installing the Symantec Management Agent for UNIX, Linux, and Mac using the aex-bootstrap file ...................................................... 74
Manually installing the Symantec Management Agent for UNIX, Linux, and Mac using native packages .................................. 76
Viewing and managing the agent registration status .................................................................................. 76
Configuring the Symantec Management Agent using the configuration policies ................................................................. 80
Configuring the global agent settings ...................................................................................................................... 81
Configuring the targeted agent settings ...................................................................................................................... 81
Configuring maintenance window policies .............................................................................................................. 83

Chapter 7  Patch Management for Linux ........................................... 86

About Patch Management Solution for Linux ........................................... 86
Differences in patching Red Hat Linux and SUSE Linux ........................................... 87
Patching Linux with Patch Management Solution ........................................... 87
Installing the software update plug-in ........................................... 88
Configuring the system assessment scan interval ........................................... 89
Selecting software channels for Linux ...................................................... 90
Scheduling the import of patch metadata for Linux ........................................... 90
Installing software updates for Linux ........................................... 91
Viewing the software update delivery report ........................................... 92
Advanced configuration ................................................................................................................................. 93
Creating and assigning custom severity levels ........................................... 93
Configuring software updates download location ........................................... 94
About Linux kernel patching .......................................................................................... 94

Chapter 8  Software Management for Linux ..................................... 96

About Software Management Solution ........................................... 96
What you can do with Software Management Solution ........................................... 98
Implementing Software Management Solution ........................................... 99
About the agents and plug-ins that Software Management Solution uses ................................................................. 100
Installing or upgrading the Software Management Solution plug-in ................................................................................ 101
Performing a quick delivery of a single software resource ................. 103
Creating a Quick Delivery task with the Quick Delivery wizard .................. 105
Creating a task in Software Management Solution .................................... 106
Scheduling a task and selecting computers in Software Management Solution ...................................................... 107
Running a Software Management Solution report ................................ 108
About advanced software deliveries .................................................... 110
Delivering multiple software resources and tasks sequentially ........... 111
Creating a Managed Software Delivery policy with the Managed Software Delivery wizard .................................................. 113
Creating a Managed Software Delivery policy ........................................ 114
Selecting the delivery destinations for a Managed Software Delivery policy ........................................................................ 116

Chapter 9 Virtualization Management ........................................ 118

About Virtual Machine Management on UNIX and Linux systems .......... 118
About server virtualization ................................................................. 120
Permissions that Virtual Machine Management requires ....................... 121
Getting started with the Virtual Machine Management component .......... 124
Installing the Virtual Machine Management Task Server Plug-in ......................... 125
Discovering and adding a single vCenter or host ......................................................... 126
Discovering and adding multiple vCenter or hosts ........................................... 127
Gathering inventory on the host .................................................................. 128
Creating a virtual environment ............................................................... 130
Creating a virtual machine on a host .......................................................... 131
Creating a virtual disk on a host ................................................................. 138
Creating a virtual network on a host ........................................................... 139
Creating a snapshot .................................................................................. 140
Best practices to prevent protocol replacement ........................................ 141
Deployment of ESX or ESXi servers ......................................................... 142
Tables populated during the Network Discovery and Run Inventory tasks ........................................................................ 142
About Log Viewer .................................................................................. 144
Generating ad-hoc reports with the IT Analytics Monitor Metrics cube .................................................................................................................. 180

Section 5 Process Automation ...................................................... 181

Chapter 13 Built-in Workflow capabilities ...................................... 182

About Symantec Workflow integration with UNIX and Linux clients .................................................................................................................. 182
Pieces of Symantec Workflow ..................................................................... 184
What you can do with Symantec Workflow ........................................... 187
Executing scripts on UNIX and Linux systems through SSH .................... 189
About Process Manager reporting .......................................................... 190

Section 6 Centralized management .................................................. 192

Chapter 14 Topology View ................................................................ 193

About Product Name Portal page ............................................................. 193
Viewing the Server Management Suite Portal page .................................. 193
About Topology View Web Part ............................................................ 195
Topology View Web part options ............................................................ 197
Viewing network topology ........................................................................ 196
Topology View Web part options ............................................................ 197

Chapter 15 Remote Management ..................................................... 199

Methods for remotely managing UNIX/Linux servers ............................ 199
About Server Resource Manager Home page ........................................ 200
Accessing the Server Resource Manager Home page ................................ 201

Chapter 16 Package server for Linux ................................................. 203

About package server for Linux ............................................................. 203
About integrating Apache Web Server with package server for Linux ........ 204
About detecting the Apache Web Server ................................................ 205
Requirements to configure package server and the Apache Web Server .................................................................................................................. 206
Requirements to configure HTTPS and HTTP ........................................ 207
Package server configuration example that uses main web directory for package server links .................................................................................................. 208
Package server configuration example using an alias for package server links ................................................................................................................. 211
Index ................................................................. 214
Introducing UNIX/Linux Management in Symantec Server Management Suite 7.6 powered by Altiris Technology.

This chapter includes the following topics:

- About this Guide
- Symantec Server Management Suite 7.5 SP1 powered by Altiris technology: UNIX and Linux management capabilities

About this Guide

The number one goal of server administrators is to ensure uptime of their servers and to avoid any business interruptions. This guide offers an overview of the tools that Altiris Server Management Suite from Symantec provides towards those goals, specifically in a UNIX and Linux server environment.

Server Management Suite provides an integrated set of tools for managing servers, on a common platform. Each tool or "solution" extends the capabilities of the system. Here is a list of solutions and components that this guide covers, with emphasis on their out-of-box capabilities.

- Symantec Deployment Solution
Symantec Management Agent
- Symantec Inventory Solution
- Symantec Inventory Pack for Servers
- Symantec Patch Management Solution
- Symantec Software Management Solution
- Symantec Virtual Machine Management
- Altiris Monitor Solution for Servers from Symantec
- Altiris Monitor Pack for Servers from Symantec
- Symantec Workflow
- Altiris IT Analytics Solution from Symantec

Each solution builds on another, without putting additional demands on the architecture. Each solution also leverages the information that is collected by the previous solution. This capability is made possible through the use of the CMDB, a single repository of data, logic, and automated processes, including access rights.

This guide takes you through all aspects of managing UNIX/Linux servers, from the moment the hardware is received, through configuration management, patching, software management, and server health monitoring, to process automation (workflow) and integration by centralized management.

Symantec Server Management Suite 7.5 SP1 powered by Altiris technology: UNIX and Linux management capabilities

Server Management Suite was designed with cross-platform management in mind. You discover and manage UNIX and Linux computers in much the same way that you discover and manage Windows or Mac OS X computers.

In the table, a "Yes" in the UNIX, Linux, Mac OS X or Windows column indicates that the capability exists for that platform. Unless all Linux or UNIX platforms support a capability, the table also specifies which UNIX or Linux platforms do.
### Table 1-1: Key cross-platform capabilities of Server Management Suite

<table>
<thead>
<tr>
<th>Server Management Suite capability</th>
<th>UNIX</th>
<th>Linux</th>
<th>Windows</th>
<th>Mac OS X Server</th>
</tr>
</thead>
</table>
| Heterogenous OS support           | IBM AIX<sup>1</sup>  
Oracle Solaris<sup>1</sup>  
HP-UX<sup>1</sup>  
Novell SUSE Linux<sup>2</sup>  
Redhat Enterprise Linux<sup>2</sup> | Novell SUSE Linux<sup>2</sup>  
Microsoft Windows Server 2003  
Microsoft Windows Server 2008 | Mac OS X Server 10.8  
Mac OS X Server 10.9  
OS X Server 10.10 | |
| Network discovery                 | Yes  | Yes   | Yes     | Yes             |
| Network discovery of virtual machines | No   | VMware | Hyper-V VMware | No             |
| Hardware, software, and user inventory | Yes | Yes   | Yes     | Yes             |
| Imaging                           | No   | Yes   | Yes     | Yes             |
| Scripted OS installation          | No   | Yes   | Yes     | Yes             |
| Software delivery                 | Yes  | Yes   | Yes     | Yes             |
| Intelligent software management   | Yes  | Yes   | Yes     | Yes             |
| Software detection rules          | Basic software detection rules  
Basic software detection rules for Linux .rpm packages | Basic software detection rules for Apple .dmg packages | |
| Remote control                    | Yes<sup>4</sup>  
Yes<sup>4</sup>  
Yes<sup>4</sup>  
Yes<sup>4</sup> | Yes<sup>4</sup>  
Yes<sup>4</sup> | |
| Automated software updates        | No   | Yes   | Yes     | Yes             |
| Advanced software inventory       | Yes  | Yes   | Yes     | Yes             |
| Custom inventory                  | Yes  | Yes   | Yes     | Yes             |
### Table 1-1
Key cross-platform capabilities of Server Management Suite (continued)

<table>
<thead>
<tr>
<th>Server Management Suite capability</th>
<th>UNIX</th>
<th>Linux</th>
<th>Windows</th>
<th>Mac OS X Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross-platform reporting</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Power control</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Server health monitoring</td>
<td>Monitor Packs for Solaris and AIX&lt;sup&gt;5&lt;/sup&gt;</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Event monitoring</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Workflow</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Agentless server monitoring</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<sup>1</sup> Server Management Suite supports the following UNIX operating systems:
- IBM AIX: 6.1, 7.1
- Oracle Solaris: 10 (SPARC, x86/x64), 11 (SPARC, x86/x64)
- HP-UX: 11i v3

<sup>2</sup> Altiris Server Management Suite from Symantec supports the following Linux operating systems:
- Red Hat Enterprise Linux: 5.10-5.11, 6.0-6.5, 7
- Novell SUSE Linux Server: 10, 11 SP1, 11 SP2, 11 SP3

<sup>3</sup> For OS X 10.8, server component of the system is installed with Server.app that is available from Apple Appstore.

<sup>4</sup> Server Management Suite supports the following methods for remote management:
- UNIX: VNC and custom right-click actions to leverage tools for xwindows, telnet, ssh sessions.
- Linux: VNC; custom right-click actions to leverage tools for xwindows, telnet, ssh sessions.


See “Symantec Server Management Suite 7.5 SP1 powered by Altiris technology: UNIX and Linux management capabilities” on page 155.
Provisioning UNIX and Linux Servers

- Chapter 2. Setting up Linux client computer
- Chapter 3. Server configuration
Setting up Linux client computer

This chapter includes the following topics:

- About Deployment Solution
- Components of Deployment Solution
- Creating and deploying Linux disk images

About Deployment Solution

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

The following are the key features of Deployment Solution:

- Lets you migrate to the latest Windows version; migrates user data, personality settings, and OS and application settings to the new operating system.
- Lets you configure each system based on standardized criteria, such as job function, user type, or location.
- Lets you change the system and the network settings.
- Lets you easily create the jobs and tasks that automate deployment and migration functions such as imaging, scripted OS installations, configurations, and software deployments.
- Supports industry-standard hardware-management capabilities such as Intel vPro, Pre-boot eXecution Environment (PXE), and Wake on LAN technologies.
- Lets you use role-based and scope-based security to secure management features from unauthorized personnel.
- Integrates with many Symantec products built on Symantec Management Platform. For example, Altiris solutions and security, backup and recovery, virtualization, data loss prevention, vulnerability assessment, and other products.

The following are the key benefits of Deployment Solution:
- Reduces the costs that are associated with deploying, migrating, and provisioning desktops, laptops, and servers throughout the organization.
- Saves time and reduces human error over traditional PC deployments.
- Reduces end-user downtime by automating the deployment process.
- Increases IT efficiency through automated, repeatable deployment tasks.
- Provides tools for zero-touch migrations to reduce the costs that are associated with moving to a new operating system.

Components of Deployment Solution

When you install Deployment Solution on Symantec Management Platform, the Deployment Solution components get integrated with Symantec Management Platform. The Deployment Solution leverages the platform capabilities to execute and schedule tasks, jobs, and policies, and set up site servers, use filters, and generate reports. The components of Deployment Solution help you manage the client computers in your environment.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment Plug-in</td>
<td>The Deployment Plug-in is installed on the client computers on which you want to execute deployment tasks. This plug-in lets you create and deploy disk images, perform remote operating system (OS) installation, change system settings, and migrate the personality settings. You can enable the Symantec firewall on the client computer and enable the Windows firewall on the Notification Server. However, to install the Deployment Plug-in by pushing it to computers, you need to disable one of these firewalls.</td>
</tr>
</tbody>
</table>
Table 2-1  Deployment Solution components (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation folder</td>
<td><strong>Note:</strong> Ensure that the Deployment plug-in of the specific operating system is installed on the client computer on which the automation folder is created.</td>
</tr>
<tr>
<td>Imaging tools</td>
<td></td>
</tr>
<tr>
<td>Boot Disk Creator</td>
<td>Boot Disk Creator (BDC) creates a boot disk using the Windows or Linux preboot operating systems. BDC can also create a bootable CD or USB.</td>
</tr>
<tr>
<td>Resource Import Tool</td>
<td>The Resource Import tool is used for importing the existing Windows and Linux images. The tool is also used for adding Windows-scripted OS installation files.</td>
</tr>
<tr>
<td>Driver Manager</td>
<td>Driver Manager provides the interface to perform driver operations such as adding and deleting data from the DeployAnywhere driver database and the Preboot driver database.</td>
</tr>
<tr>
<td>DeployAnywhere</td>
<td>DeployAnywhere lets you deploy the Windows operating system image to dissimilar hardware. DeployAnywhere also lets you perform a Windows-scripted installation on bare metal computer.</td>
</tr>
</tbody>
</table>

Creating and deploying Linux disk images

When you perform the **Create Image** task with **Disk Image** as the option, a Symantec Management Platform package is created for the captured disk image. The Disk image is stored on the Deployment share of the site server on which the Package Service runs. Each image is stored in a separate folder and has a GUID. Information about the image is also stored in the CMDB as an image resource. You can use this package to distribute the image to other Package Servers.

For Linux operating system, deploying disk images and back-up images does not support the ReiserFS file system. Image deployment supports only the SUSE Ext3 file system. If you have a ReiserFS partition, you must use the -raw switch when you image the partition to preserve its structure. Linux IDE images must be deployed.
on computers that have the Linux IDE disk. SCSI disk images must also be deployed on computers having the SCSI disk image.

The following process lists the steps that you must follow to create an image of a Linux client computer and to deploy the Linux image on other client computers.

Following are the steps that you must follow to create an image of a Linux client computer:

Table 2-2  Process for creating an image of a Linux client computer

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the Console</td>
<td>Launch the Symantec Management Console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can launch the console either from the Start menu of the Notification Server computer or from any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>computer of the network. To access the console from a different computer, you must type the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
<tr>
<td>Step 2</td>
<td>Prepare a reference computer for imaging.</td>
<td>Prepare the reference computer that contains the core software and settings that you want to be replicated on other computers.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Execute the Prepare for Image capture task</td>
<td>Execute the <strong>Prepare for Image capture</strong> task to ensure that the captured image does not contain any hardware-dependent data. You can then deploy a hardware independent image on other computers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Preparing to capture an image” on page 25.</td>
</tr>
</tbody>
</table>
**Table 2-2** Process for creating an image of a Linux client computer (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>Create an image of the client computer</td>
<td>Execute the <strong>Create Image</strong> task to create the disk image of the reference computer. You can either execute the task immediately by using the <strong>Quick Run</strong> option of the task that you have saved or you can schedule the task to be executed later on the reference computer. See “Creating a Linux image” on page 26. See “Scheduling a deployment job or task” on page 31.</td>
</tr>
</tbody>
</table>

Following are the steps that you must follow to deploy an image of a Linux client computer on client computers:

**Table 2-3** Process for deploying an image of a Linux client computer

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the Console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
<tr>
<td>Step 3</td>
<td>Boot the client computer in Automation environment</td>
<td>Create a <strong>Boot To</strong> task and add the task to the client job to boot the client computer to Automation environment.</td>
</tr>
</tbody>
</table>
### Table 2-3 Process for deploying an image of a Linux client computer (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>Deploy the image on the client computer</td>
<td>Create a <strong>Deploy Image</strong> task for the target client computers. You can either execute the task immediately by using the <strong>Quick Run</strong> option of the task that you have saved or you can schedule the task to be executed later on the reference computer. See “Deploying a Linux image” on page 28. See “Scheduling a deployment job or task” on page 31.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Boot the client computer to production</td>
<td>Boot the client computer to production using the <strong>Boot To</strong> task.</td>
</tr>
</tbody>
</table>

### Preparing to capture an image

For Windows, the **Prepare for Capture Image** task uses Sysprep utility to remove the computer name, Security Identifier (SID), the operating system license, GUID of the agent, and some hardware-dependent drivers. You must always run this task before creating a disk image. Sysprep also disables the built-in administrator account and clears the admin password.

For Linux, this task runs a preimage script to remove the configuration-related settings and prepare the computer for imaging.

You can choose several options while creating this task. You must create a deployment task before you run it.

**To prepare for image capture**

- Under the **Pre-Imaging** section, select either **Windows (using sysprep)** or **Linux** operating system.

  The fields and their descriptions are as follows:
<table>
<thead>
<tr>
<th>Task name icon</th>
<th>Displays the default task name as Prepare for Image capture. You can edit the default task name to specify a relevant task name. For example, Prepare for image capture_Linux.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-imaging</td>
<td>Lets you select the operating system for which you want to create a Prepare for image capture task. For Windows, you can select from the following:</td>
</tr>
<tr>
<td></td>
<td>■ OS type</td>
</tr>
<tr>
<td></td>
<td>Select the version of Windows operating system.</td>
</tr>
<tr>
<td></td>
<td>■ Product key</td>
</tr>
<tr>
<td></td>
<td>Enter credentials to rejoin a domain after capture is complete.</td>
</tr>
<tr>
<td></td>
<td>Lets you join back the client computer to the domain after the task executes. Specifying the credentials to join the domain in the <strong>User name</strong>, <strong>Password</strong>, and the <strong>Confirm password</strong> fields.</td>
</tr>
<tr>
<td></td>
<td>This option is applicable for the Windows operating system only.</td>
</tr>
</tbody>
</table>

### Creating a Linux image

Deployment Solution lets you create disk images and backup images of Linux client computers. A disk image is an image that contains the application and settings that are present on a computer disk. Backup images retain the data and software of a specific computer. A backup image contains a snapshot of the hard disk of a computer. The difference between a disk image and a backup image is that a disk image can be used to deploy on multiple client computers whereas the backup image must be restored only to the computer that it was captured from. The image has the same name as the computer from which it was captured. You execute the **Create Image** task of Deployment Solution to create disk images and backup images.

---

**Note:** To create an image, if the Package Server is in a domain different from the SMP domain, then ensure that you add the SMP users to the Administrator group of the Package Server. All the users that you add must have read and write permissions on the Package Server.

---

**To create an image**

1. Launch the Symantec Management Console.
2. In the Symantec Management Console, from the **Manage** menu select **Jobs and tasks**.
3. In the left pane, do either of the following:
Right-click **System Jobs and Tasks** and select **New > Task**.

The fields and their descriptions are as follows:

- **Task name**
  - Icon that displays the default task name as **Create Image**. You can edit the default task name to specify a relevant task name. For example, Create Image_Linux.

- **Image name**
  - Enter a name for the image to be created. Image name supports only ASCII characters. If you use a token for image name, ensure that it is a valid predefined token. In case you use an invalid token, then either an error is displayed on the task or the image package is created with the task name.

- **Description**
  - Enter a description, if required.
Image type

Select from the following two types of computer images:

- **Disk Image**
  A disk image can be deployed to multiple computers. These images are saved in a package on the package server and are replicated to other package servers. Ensure that the **Prepare for Image capture** task is executed before the image is created.

- **Backup image**
  A backup image is used to back up a single computer. These images must be deployed only to the same computer where they were created from. They must not be deployed to multiple computers. These images are not saved in a package and cannot be distributed to other package servers through the replication process. In case you want to image only a data disk that is a disk without an operating system or partition of a data disk, select the **backup image** option.

6. On the **Create Image** page, you can set the **Advanced** imaging options. Following are the options that you can set with the description:

7. Click **OK**.

If you are reading this procedure as a part of a process, return to the process by clicking on the following link:

See “Creating and deploying Linux disk images” on page 22.

**Deploying a Linux image**

Before you perform the **Deploy Image** task, you must know the following:

- If the computer has the Deployment plug-in installed, the computer configuration is saved and restored after the image is applied. The computer configuration contains the computer name, network settings, and domain.

- If the computer is a member of a domain, supply the appropriate credentials to rejoin the domain. You can create an image that retains its data and software by creating a backup image.
To create a deploy image task

1. Launch the Symantec Management Console.

2. In the Symantec Management Console, select Manage > Jobs and Tasks.

3. In the left pane, do either of the following:
   - Right-click System Jobs and Tasks folder and select New > Task.

4. Enter the following:

   **Task name**
   Displays the default task name as Deploy Image. You can edit the default task name to specify a relevant task name. For example, Deploy Image_Linux.

   **Image Name**
   Enter the name of the image file to deploy.

   *Note*: For Linux, only the **Name** and **Image Name** fields are necessary. All of the other fields are optional.
6 Click the **Advanced** tab to set the following:

**Partition**
Lets you decide the partitions on which you deploy the image. You can change the destination partition size by clicking the partition number.

For Linux, only Data Partition deployment is supported.

**Command-line**
Lets you add command-line options for the imaging tool.

For Ghost partition deployment, following command lines must not be used:

```
MODE, Size, SRC and DST values should not be used for command line.
```

**Note:** Ensure that you do not specify the switch -SZEE and select the Resize partition option simultaneously for the deploy image task.

**Multicasting**
Lets you configure the number of computers on which you want to multicast the image. You can override the default multicast settings that were set in **Settings > Deployment > Image Multicasting**. If the threshold count is 2, there must be at least two client computers and one master computer before multicasting is used in this session.

Deployment Solution does not support Multicast and Unicast options simultaneously if you use the Ghost imaging tool.

**File Preservation**
Lets you specify the files and folders that you want to preserve when the image is restored.

This option is not supported if the client computer is installed with Linux operating system.

**HTTP**
Lets you add the credentials that are required to deploy an image, which was obtained from an HTTP site.

7 Click **OK**.

If you are reading this procedure as a part of a process, return to the process by clicking on the following link:

See “Creating and deploying Linux disk images” on page 22.
Scheduling a deployment job or task

Deployment Solution lets you schedule a task that you have created. You can schedule the task to run immediately or a specific time. You can also select the computer on which the task is executed.

To schedule a task

1

2 In the left pane, select the task that you want to schedule.

3 (Optional) If you want to execute the task immediately, in the right pane, click Quick Run. Select the name of the computer that you want the task to run on, and then click Run.

   You can schedule the task to run on only one computer using the Quick Run option.

4 If you want to schedule the task to run at a later time or you want to schedule multiple computers, click New Schedule.

5 Select the date and time that you want to schedule for the task to execute.

   You can also select the task to run at specific intervals.

6 Select the computers that you want the task to run on.

7 Click Schedule.
Server configuration

This chapter includes the following topics:

- Creating system configuration settings
- Creating or modifying tokens in Deployment Solution

Creating system configuration settings

The system configuration setting of a client computer comprises of the network setting, domain name, computer name, IP address, and so on. Deployment Solution lets you create system configurations to apply on the client computers after they boot to the production environment from the preboot environment or automation environment. For example, after you boot 50 client computers to the production environment, you might want the computer names to be modified and also join a common domain. This task can be performed through the system configuration that you create and apply on the client computers.

You either create a new system configuration setting for the client computers or update an existing system configuration. Deployment Solution lets you apply system configurations on the managed client computers that are already imaged or on which a Deploy Image task is executed.

To create system configuration settings

1. In the Symantec Management Console, on the Settings menu, click Deployment > System Configurations.
2. Click New system configuration.
3. Click OK.
Creating or modifying tokens in Deployment Solution

In Deployment Solution, a system token is a type of variable, which is replaced with unique deployment-related data that is retrieved from the database. You can insert these variable tokens in scripts or answer files to extract information from the database. Deployment Solution provides you with the option to create tokenized scripts through the console as well as has predefined tokens to use.

You can add or create a new token, edit the SQL query of an existing token, or delete a token that you have created. You are not recommended to modify an existing token name.

To create new tokens through the console
1. In the Symantec Management Console, on the Settings menu, click Deployment > Tokens.
2. Click New token.
3. Enter a name for the token in the Token name field.
4. Enter the SQL statement for the token.
5. Click Validate SQL to validate the SQL statement.
6. Click Save changes.

To modify an existing token
1. In the Symantec Management Console, on the Settings menu, click Deployment > Tokens.
2. Select an existing token that is listed in the table and double-click it.
3. In the SQL statement field, modify the SQL query of the token.
Discovery and Inventory of Linux and UNIX Servers

- Chapter 4. Discovery and Inventory
- Chapter 5. Agentless inventory of UNIX and Linux servers
Discovery and Inventory

This chapter includes the following topics:

- About Network Discovery
- Discovering UNIX and Linux computers
- About Inventory Solution
- About software inventory on UNIX/Linux servers
- About Inventory Pack for Servers
- Viewing MySQL and Oracle Database inventory
- About Apache HTTP Server inventory
- Gathering inventory on UNIX/Linux servers
- About custom inventory data classes
- Custom inventory sample script for UNIX, Linux, and Mac
- Gathering custom inventory on UNIX/Linux servers
- About software inventory using the filescan.rule file
- Running software inventory on UNIX, Linux and Mac computers using the filescan.rule file

About Network Discovery

Network Discovery lets you discover all IP devices that are connected to your network. Network Discovery lets you find new network devices and find the network devices whose discovery properties have changed.

Network Discovery is included in Symantec Management Platform.
Network Discovery can discover routers, switches, hubs, network printers, Novell NetWare servers, and the computers that are running Windows, UNIX, Linux, and Macintosh. You can use a variety of protocols to discover devices, such as AMT, SNMP, WMI, and others.

The information that is collected can help you do the following:

- Plan for imaging
- Updating drivers on specific types of hardware
- Configuring changes to routers or switches
- Identifying the computers that are running the operating systems not currently supported by the Symantec Management Agent

You can also update categories so that the new devices that are added to the network can be identified during discovery.

Because Network Discovery integrates with Symantec Management Platform, when devices are discovered, they are automatically created as resources in the platform’s central database (CMDB). Using the platform’s task management component, you can schedule discovery tasks to run when it best meets your needs.

You can also discover Windows-based computers through domains or importing through Microsoft Active Directory.

Discovering UNIX and Linux computers

You can discover the computers that are not yet managed by the Symantec Management Agent. When the computers are discovered, resource objects are created for them in the Configuration Management Database (CMDB). You can then gather inventory on the discovered computers.

You can discover computers during the first time setup or with the network discovery wizard.

See “About Network Discovery” on page 35.

To discover computers using network scan during first time setup

1. Enable SNMP on your Linux or UNIX server computer.

2. In the Symantec Management Console, on the Home menu, click First Time Setup.

3. On the first time setup page, in the left pane, under Step 1 - Discover, click Discover Computers.

4. In the Discover Computers wizard, on the wizard navigation bar, click Step 2 Network.
5 On the **Step 2 Network** page, check **Discover networked computers and devices (ping sweep)**, and then enter a ping sweep range.

For a first-time setup, you may need to include all subnets to ensure that you identify every device. However, you can limit the scope as needed. For example, you can run multiple scans on specific subnets.

6 (Optional) If you want to communicate with network devices and classify them more accurately, click **Turn on additional protocols**, and then, on the **Define Group Settings** page, do the following:

- In the **Define Group Settings** dialog box, enable the protocol. At the upper right of the protocol section, click the colored circle, and then click **On**.
- In the protocol section, click the **Add** symbol.
- In the **Add Credential** dialog box, in the **Credential type** drop-down list, click **SSH credentials**, and then configure the credential information according to your needs.
- Click **OK**.

7 In the **Discover Computers** wizard, click **Discover**.

**To discover computers using network discovery wizard**

1 In Symantec Management Console, on the **Home** menu, click **Discovery and Inventory > Network Discovery**.

2 On the **Network Discovery Home** page, in the **Network Discovery Quick Start Actions** web part, click **Launch Discovery Wizard**.

3 In the **Discover network devices through network communication** wizard, follow the steps to configure the discovery task according to your needs.

4 Click **Finish**.

### About Inventory Solution

Inventory Solution lets you gather inventory on Windows, UNIX, Linux, and Mac computers.

The inventory data is stored in the Configuration Management Database (CMDB). The CMDB provides a central store of data that is used across the Symantec Management Platform.

You can gather the following types of inventory data:

- Basic inventory data: Computer name, domain, installed operating system, etc.
## About software inventory on UNIX/Linux servers

Software inventory collects information about the applications that are installed on your managed computers to help you analyze different aspects of your resources.

See “About software inventory using the `filesan.rule` file” on page 54.

See “Running software inventory on UNIX, Linux and Mac computers using the `filesan.rule` file” on page 55.

For example, you can identify the computers that do not meet minimum security requirements. You can collect information about the computers that do not have antivirus software or application updates installed. You can also prepare for a software license audit by finding out the number of installed instances of an application.

<table>
<thead>
<tr>
<th>Type of Inventory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard inventory data</td>
<td>Hardware and software components, file properties, etc.</td>
</tr>
<tr>
<td>Custom inventory data</td>
<td>Additional data beyond the predefined data classes in Inventory Solution.</td>
</tr>
<tr>
<td>Inventory for Network Devices</td>
<td>Inventory data from the discovered devices in your network.</td>
</tr>
</tbody>
</table>

Inventory Solution provides a web-based management console, policies to alert you about critical information, and predefined or custom reports that let you analyze gathered inventory data.

Inventory Solution also has the following features:

- Supports zero-footprint configuration.
- Operates in always connected, sometimes connected, and standalone computing environments.
- Can be installed to run on a recurring basis with the Symantec Management Agent.
- Posts data through SMB and/or HTTP.
- Lets you meter, track, or deny the usage of one or more software applications and harvest unused software licenses.

Symantec™ Inventory Pack for Servers powered by Altiris™ technology is a separate product that lets you gather server-based inventory data from servers.

See “About Inventory Pack for Servers” on page 39.

Additional Symantec products let you gather inventory data from managed computers, network devices, and Windows, UNIX, Linux, and Mac servers.
Software inventory policies and tasks scan the target computers for the available software applications and report the collected information to Notification Server. You can collect information about both standard applications and custom software applications that are installed on your UNIX or Linux servers.

See “Gathering inventory using predefined policies or tasks” on page 43.

About Inventory Pack for Servers

Inventory Pack for Servers is a separate product with a separate license. It runs on top of Inventory Solution and uses the Inventory Pack for Servers Plug-in.

Inventory Pack for Servers is part of the Server Management Suite.

You can use different methods to gather inventory data about server-class software that is installed on servers.

You can gather the following types of server-based inventory data:

- ORACLE
- Microsoft SQL Server
- Microsoft SQL Server clusters
- MySQL
- Microsoft Exchange Server
- Microsoft DHCP server
- Microsoft DNS server
- Microsoft RAS server
- Microsoft IIS
- Apache
- Network load balancing
- System DSN

See “About Inventory Solution” on page 37.

Viewing MySQL and Oracle Database inventory

See “About software inventory on UNIX/Linux servers” on page 38.

To obtain all possible MySQL or Oracle Database information, your environment must meet the following requirements:
Database services and instances must be up and running.

You must specify valid credentials for the inventory process to be able to log in and retrieve the info.

When you specify multiple credential sets, multiple Oracle Database instances can be detected and their configuration reported. Specifying multiple credential sets is also the best way to ensure proper database logon when a user is not sure which credentials are the right ones.

To view database-related information in the Symantec Management Console

1. In the Symantec Management Console, on the Reports menu, click All Reports.

2. In the left pane, under Reports, expand Discovery and Inventory > Inventory > Server > Database Servers.

3. In the left pane, under Database Servers, you can do the following:
   - Expand MySQL, and then click Servers running MySQL Database Server to view the report.
   - Expand Oracle, and then click Oracle Databases mounted to Oracle Instance or Servers running Oracle Database Server to view the reports.

You can also view the reports in the Resource Manager.

---

**About Apache HTTP Server inventory**

Inventory Pack for Servers provides the predefined server inventory policies that let you gather data about Apache HTTP Server 2 or higher.

See “About software inventory on UNIX/Linux servers” on page 38.

You can gather data only about the following types of Apache HTTP Servers:

- Apache HTTP Servers that are part of an initial operating system distribution and that are installed from a native package.
- The first discovered Apache HTTP Server among multiple Apache HTTP Server installations that reside in different locations on the target computer.

You can view the inventory that is gathered from Apache HTTP server in the Resource Manager.


You can use the default server inventory policies to collect data.

See “Gathering inventory using predefined policies or tasks” on page 43.
Gathering inventory on UNIX/Linux servers

To gather inventory data, run automated policies and tasks on managed computers. To do this, you need to install the Symantec Management Agent and the Inventory Plug-in on managed computers. The inventory policies and tasks use the Inventory Plug-in to perform the inventory scan on the managed computer and send the inventory data to the Configuration Management Database.

You can also use Inventory Pack for Servers, which is a separate product, to gather inventory data from servers. If you have Inventory Pack for Servers installed, it uses the same type of inventory policies.

See “About Inventory Pack for Servers ” on page 39.

Inventory policies let you gather inventory on a recurring schedule. You can use the predefined inventory policies or you can create and configure your own inventory policies to gather different types of inventory. For example, you can have one policy collect hardware inventory daily and another policy collect software inventory weekly.

Table 4-1  Process for gathering inventory on UNIX/Linux servers

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Install the inventory plug-ins on UNIX and Linux computers.</td>
<td>To gather inventory from UNIX and Linux computers, you must install the Inventory plug-in on managed computers. Note: To gather server application data or other inventory specific for servers, you have to also install the Inventory Pack for Servers plug-in. See “Installing the inventory plug-ins on UNIX and Linux computers” on page 42.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Gather inventory on managed computers.</td>
<td>Turn on the predefined policies or create clones of those and configure them. Symantec recommends. See “Gathering inventory using predefined policies or tasks” on page 43.</td>
</tr>
</tbody>
</table>
Table 4-1  Process for gathering inventory on UNIX/Linux servers (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Gather the inventory of the native UNIX/Linux package system.</td>
<td>Collect software data on UNIX or Linux computers by querying the native package system. See “Gathering and viewing software inventory of the native UNIX/Linux package system” on page 45.</td>
</tr>
<tr>
<td>Step 4</td>
<td>View the inventory results.</td>
<td>See “Viewing inventory data in reports” on page 45.</td>
</tr>
</tbody>
</table>

Installing the inventory plug-ins on UNIX and Linux computers

To gather inventory from UNIX and Linux servers, you must install the Inventory plug-in and the Inventory Pack for Servers Plug-in. Without the Inventory Pack for Servers, you can see only basic inventory details. Before you install the plug-ins, you must install the Symantec Management Agent for UNIX, Linux, and Mac computers.

To install the Plug-in, you configure the policy that installs the Plug-in on target computers. You specify the group of computers on which the policy runs and the time when it runs. If you choose a group that contains a computer that already has the plug-in installed, the task is ignored on that computer. When the policy is turned on, the plug-in is automatically installed on any new computer that is a member of the target group.

By default, no plug-in installation policies are turned on. If you install Inventory Solution for the first time, you must manually turn on the policies to install the Inventory Plug-in.

Before performing this task, you must install the Symantec Management Agent on target computers.

This task is a step in the process for preparing managed computers for inventory.
To install the Inventory Plug-in

1. In the Symantec Management Console, on the Actions menu, click Agents/Plug-ins > Rollout Agents/Plug-ins.

2. In the left pane, expand Discovery and Inventory > Windows/UNIX/Linux/Mac, and then click the policy for the plug-in that you want to install.

   For example, to install Inventory Packs for Servers Plug-in on UNIX and Linux computers, in the left pane, under Agents/Plug-ins, expand Discovery and Inventory > Windows/UNIX/Linux/Mac, and then click Inventory Pack for Servers Plug-in Install.

3. On the policy page, turn on the policy.

   At the upper right of the page, click the colored circle, and then click On.

4. On the policy page, under Applied to, click Apply to, and then choose the computers on which you want to install the plug-in.

5. On the policy page, under Schedule, click Add schedule, and then specify the time for the policy to run on target computers.

6. Click Save changes.

To install the Inventory Pack for Servers Plug-in on UNIX and Linux computers

1. In the Symantec Management Console, on the Settings menu, click Agents/Plug-ins > All Agents/Plug-Ins.

2. In the left pane, under Agents/Plug-ins, expand Discovery and Inventory > Windows/UNIX/Linux/Mac, and then click Inventory Pack for Servers plug-in Install.

3. In the right pane, under Applied to, on the toolbar, click Apply to, and then choose the computers on which you want to enable the policy.

4. Turn on the policy.

   At the upper right of the page, click the colored circle, and then click On.

5. Click Save changes.

   The policy will install the Plug-in next time the Symantec Management Agent checks for policy changes. By default, the agent checks for new policy updates at least once a day.

Gathering inventory using predefined policies or tasks

You can use predefined inventory polices to gather inventory data. You can turn on the predefined policies and configure them according to your needs. If you want
to configure predefined policies, Symantec recommends that you clone an original predefined policy and then configure the copy.

See “Installing the inventory plug-ins on UNIX and Linux computers” on page 42.

To gather inventory with policies or tasks, you must install the Inventory Plug-in on target computers.

This task is a step in the process for gathering inventory on managed computers.

To turn on predefined inventory policies

1. In the Symantec Management Console, on the Manage menu, click Policies.
2. In the left pane, expand Discovery and Inventory > Inventory, and then click the predefined inventory policy that you want to use.
   (Optional) On the policy page, configure the policy according to your needs.
3. On the inventory policy page, turn on the policy.
   At the upper right of the page, click the colored circle, and then click On.
4. Click Save changes.
5. (Optional) After you turn on an inventory policy, you can force the policy rollout by doing the following:
   In the Symantec Management Console, on the Settings menu, click Notification Server > Resource Membership Update, and then, under Complete update schedule, click Run.

To clone and configure predefined inventory policies

1. In the Symantec Management Console, browse to the predefined inventory policy that you want to clone.
2. Right-click the policy, and click Clone.
3. Give the cloned policy a unique name, and then click OK.
4. On the inventory policy page, configure the policy options according to your needs.
5. (Optional) Click Advanced to configure the data classes, policy run options, or the software inventory rules, and then click OK.
6. On the inventory policy page, turn on the policy.
   At the upper right of the page, click the colored circle, and then click On.
7 Click **Save changes**.

8 (Optional) After you configure an inventory policy, you can force the policy rollout by doing the following:

   In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Resource Membership Update**, and then, under **Complete update schedule**, click **Run**.

Gathering and viewing software inventory of the native UNIX/Linux package system

The majority of software data on UNIX or Linux platforms can be collected by querying the native package system for the OS. This action is comparable to gathering Add/Remove programs on Microsoft Windows platforms. You can either create a new policy or by modify or clone the default inventory policy.

**To gather software inventory of the native package system**

1 In the Symantec Management Console, navigate to **Manage > Policies > Discovery and Inventory > Inventory**

2 Right-click the **Collect Full Inventory** policy and select **Clone**.

3 Modify the schedule to include a daily, weekly, monthly, or custom inventory schedule.

4 Select **Software - Windows Add/Remove Programs and UNIX/Linux/Mac software packages**.

5 Apply this policy to the UNIX or Linux servers of your choice.

After a software inventory of the targeted systems has been gathered, you can view the results.

**To view software inventory results**

1 In the Symantec Management Console, navigate to **Reports > Discovery and Inventory > Inventory > Cross-platform > Software/Applications > Software**.

2 Double-click the **Installed Software** report.

   Note that you can also create a modified report that includes software version information.

**Viewing inventory data in reports**

You can view a number of predefined reports or you can create custom reports according to your needs.
Most reports let you filter the information that you view. For example, there is an inventory report that lists computers with their BIOS information. You can view the BIOS manufacturer, version, and release date. You can also filter the report to view the computers in a certain domain. You can also filter the list of computers by using wildcards.

To view inventory data in reports

1. In the Symantec Management Console, on the Reports menu, click All Reports.
2. In the left pane, under Reports, expand Discovery and Inventory > Inventory.
   To view usage tracking or application metering reports, in the left pane, under Reports, expand Software > Application Metering.
3. Browse the report categories and select the report that you want to view.

About custom inventory data classes

A data class is a table in the Configuration Management Database (CMDB). For example, the Processor_Ex data class is the Inv_Processor_Ex table in the CMDB. Each data class has a set of attributes that define its properties.

Table 4-2 Example of attributes of the Processor Extension data class

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device ID</td>
<td>Specifies the unique index that is used to identify the device.</td>
</tr>
<tr>
<td>L2 Cache Size</td>
<td>Specifies the size of the Level 2 processor cache in kilobytes.</td>
</tr>
<tr>
<td>L2 Cache Speed</td>
<td>Specifies the clock speed of the Level 2 processor cache in megahertz.</td>
</tr>
</tbody>
</table>

You can create a data class, and then add, edit, or delete its attributes. A configured data class is referred to as a custom data class.

See “Creating and configuring a data class” on page 49.

After you configure a data class, you can create a task, configure the task script, and roll it out to the managed computers.

See “Creating a custom inventory script task” on page 51.

The custom inventory script task that runs on the managed computers generates a Notification Server Event (NSE) that contains inventory for a data class. A unique GUID identifies each data class. The inventory in the NSE is coupled with the GUID of a data class.
Note: The script that gathers inventory on Windows computers contains a reference to the GUID of a custom data class. Every time you create or edit an existing custom data class, a new GUID is assigned to this data class. You must manually update the script with the new GUID, if it refers to the older GUID for the same custom data class.

Custom inventory sample script for UNIX, Linux, and Mac

The sample inventory script for UNIX, Linux, and Mac does the following:

- Includes a helper script that implements the logic of creating NSE and posting it to Configuration Management Database (CMDB).
- Specifies the data class.
- Specifies delimiters for use in parsing the data that is returned from the command that runs.
- Specifies the data type and length of each column.
- Specifies the column names. The column names are only required when the command that runs does not already include column headings.
- Runs the desired command. In this case, appropriate platform-specific commands run.

See “Configuring the custom inventory sample script for UNIX, Linux, and Mac” on page 53.

The following is a sample script:

```
. `aex-helper info path -s INVENTORY`/lib/helpers/custominv_inc.sh
#
# Sample script for custom inventory
# The first line of code should be always included at the begin of the script
# Actual script for collecting inventory data begins after the following label:
# SCRIPT_BEGINS_HERE
#!/bin/sh
echo UNIX_PS_List
```
Gathering custom inventory on UNIX/Linux servers

To extend the type of inventory data that you gather, custom inventory lets you create the new classes that are not included by default.

Table 4-3  Process for gathering custom inventory on UNIX/Linux servers

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Prepare managed computers for gathering custom inventory.</td>
<td>Make sure that the Inventory Plug-in is installed on all managed computers on which you want to gather custom inventory. See “Installing the inventory plug-ins on UNIX and Linux computers” on page 42.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Create and customize data class.</td>
<td>To extend the type of inventory you gather, you can create new classes or edit the existing one. See “Creating and configuring a data class” on page 49.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create a custom inventory script task.</td>
<td>After you have created the custom inventory data class, you create a script task that gathers the custom inventory. See “Creating a custom inventory script task” on page 51.</td>
</tr>
</tbody>
</table>
Table 4-3  Process for gathering custom inventory on UNIX/Linux servers (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>Customize the custom inventory sample script for UNIX and Linux.</td>
<td>Custom inventory scripts let you modify the output of the script.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Configuring the custom inventory sample script for UNIX, Linux, and Mac” on page 53.</td>
</tr>
<tr>
<td>Step 5</td>
<td>View custom inventory results.</td>
<td>See “Viewing inventory data in reports” on page 45.</td>
</tr>
</tbody>
</table>

Creating and configuring a data class

In the Symantec Management Console, you can create a custom data class, add, edit, and delete data class attributes, and change the position of the attribute. You can also find the GUID and view the data in the data class.

Note that every time you modify an attribute and save the changes, a new GUID is assigned to this data class.

See “About custom inventory data classes” on page 46.

Before you perform this step, ensure that you have prepared managed computers for inventory.

To create and configure a data class

1. In the Symantec Management Console, on the Settings menu, click All Settings.
2. In the left pane, under Settings, expand Discovery and Inventory > Inventory Solution, and then click Manage Custom Data classes.
3. To create a data class, do the following:
   - On the Manage Custom Data Classes page, click New data class.
   - On the New Data Class page, type a name and a description for the data class, and then click OK.
     The name of the new data class must be unique.
4. To configure a data class, on the Manage Custom Data Classes page, in the data classes list, click the data class.
   You can add data class attributes, edit, or delete them.
5. (Optional) To add an attribute to the data class, do the following:
On the toolbar, click **Add attribute**.

In the **Data Class Attributes** dialog box, specify the details of the attribute. To add an attribute that uniquely defines a row in the data class, in the **Key** drop-down list, click **Yes**. After you do this, the attribute always has a unique value that is other than NULL.

To add an attribute that should never be empty or blank, in the **Data required** drop-down list, click **Yes**.

If, in the **Key** drop-down list, you click **Yes**, the **Data required** option is automatically set to **Yes**. To change this option, in the **Key** drop-down list, click **No**.

Click **OK**.

6  (Optional) To edit or delete the data class attributes, the attribute, and then, on the toolbar, click the **Edit** or **Delete** symbol.

7  (Optional) To let the data class store inventory of multiple objects, on the **Manage Custom Data Classes** page, check **Allow multiple rows from a single computer resource**. The data class can store the inventory of services, user accounts, files, network cards, and other objects.

8  (Optional) To specify the sequence of the attributes, on the **Manage Custom Data Classes** page, click an attribute, and then click the up arrow or down arrow.

When you report inventory values for the columns in a Notification Server Event (NSE), the attributes are identified by the column ID instead of the column name, so the order of attributes in a data class must be correct.

9  Click **Save changes**.

---

**Warning:** It is very important that you save the changes. When you create any data class or add any attributes, all the information is stored in memory. Nothing is created in the database and on details page, no GUID is yet assigned. As a result, a 00000000-0000-0000-0000-000000000000 GUID is displayed in the property of the data class. Only after you click **Save changes** on the **Manage Custom Data Classes** page, the data class is saved in the database, and the GUID is generated. Note that the GUID changes every time you make changes to the definition of the data class and save it.

10  (Optional) Copy and paste the GUID of the data class that you created for further use.

The next step is to create a custom inventory script task.

See “Creating a custom inventory script task” on page 51.
Creating a custom inventory script task

After you have created the custom inventory data class, you create and configure a custom inventory script task that gathers the custom inventory.

See “Creating and configuring a data class” on page 49.

To create a custom inventory script task, you can clone a sample script task and configure it with the custom data classes that you created. You can also create and configure a custom inventory script task on the Jobs and Tasks portal page.

When you configure your custom inventory script, you can insert tokens in the script and create or edit tokens.

To clone a sample custom inventory script task

1. In the Symantec Management Console, on the Manage menu, click Jobs and Tasks.

2. In the left pane, under Jobs and Tasks, expand Samples > Discovery and Inventory > Inventory samples > Custom.

3. Right-click the sample custom inventory script task, and then click Clone.

4. In the Clone dialog box, give the cloned script a descriptive name and click OK.

5. (Optional) Configure the sample script, and then click Save changes.

See “Configuring the custom inventory sample script for UNIX, Linux, and Mac” on page 53.

6. Under Task Status, do one of the following:
   - To schedule the task to run on managed computers, click New Schedule.
   - To perform a quick run of the task on managed computers, click Quick Run.

7. Click Save changes.
To create a custom inventory script task

1. In the Symantec Management Console, on the Manage menu, click Jobs and Tasks.

2. In the left pane, navigate to the folder where you want to create a custom inventory script task, right-click the folder, and then click New > Task.

   For example, to create a task in the Jobs and Tasks folder, right-click Jobs and Tasks, and then click New > Task.

   To create a task in the Inventory folder, expand Jobs and Tasks > System Jobs and Tasks > Discovery and Inventory, right-click Inventory, and then click New > Task.

3. In the Create New Task dialog box, in the left pane, click Run Script.

4. In the right pane, type a descriptive name for the task.

5. In the Script type drop-down list, click the script type.

6. Enter your own script or copy a sample custom inventory script to the script editor.

   To insert a token to your custom inventory script, do the following:
   - In the Insert token drop-down list, click the token that you want to insert.
   - Click Insert.

   To access a sample custom inventory script, do the following:
   - In the Symantec Management Console, on the Manage menu, click Jobs and Tasks.
   - In the left pane, under Jobs and Tasks, expand Samples > Discovery and Inventory > Inventory samples > Custom.

7. (Optional) In the Create New Task dialog box, in the script editor, configure the script.

   See “Configuring the custom inventory sample script for UNIX, Linux, and Mac” on page 53.

8. (Optional) To configure the advanced options for running the custom inventory script task, do the following:

   - Click Advanced, and then, on the Script tab, configure the options according to your needs.
   - In the Task options tab, configure the settings for running the script task, and the maximum possible length of the script task.
   - Click OK.
9 In the Create New Task dialog box, click OK.

10 On the Run Script page, under Task Status, do one of the following:
   - To schedule the task to run on managed computers, click New Schedule.
   - To perform a quick run of the task on managed computers, click Quick Run.

11 Click Save changes.

The next step is to wait for the client computers to receive the new task and report the results, and then view the data that is stored in the Configuration Management Database (CMDB).

Configuring the custom inventory sample script for UNIX, Linux, and Mac

The custom inventory script for UNIX, Linux, and Mac generates a text output that contains the collected inventory data in a specified format. This data is used to create the NSE and is posted into the Configuration Management Database (CMDB). The logic of creating the NSE and posting the data is hidden from the user.

When you configure the sample script, you can modify the output that the script generates.

See “Creating a custom inventory script task” on page 51.

To configure the custom inventory sample script for UNIX, Linux, and Mac

1 Clone or open an existing sample of the custom inventory script task.
   Do not change the first lines of the script. Make changes after the # SCRIPT_BEGINS_HERE label.

2 Specify the data class.
   Example:
   ```
   echo UNIX_PS_List
   ```

3 Specify the delimiters.
   Example:
   ```
   echo "Delimiters=\" \""
   ```

4 Specify the data type and the length of each column.
   Example:
   ```
   echo string20 string20 string20 string256
   ```
Specify the column names.
Example:
```
echo PID Terminal Time Command
```
Note that the column names are not used in 7.x custom inventory. The column names are left for backward compatibility with 6.x Inventory Solution. You can leave this line empty in 7.x but keep the `echo` command intact.
Example:
```
echo
```

Specify commands to retrieve data from system.
Example:
```
ps -ef
```

Click **Save changes**.

**About software inventory using the `filesan.rule` file**

Software inventory using the `filesan.rule` file lets you collect information about the installed applications on your UNIX, Linux, and Mac computers.

A file scan agent that is included in software inventory uses the `filesan.rule` file to detect the applications that are installed on your managed computers. The `filesan.rule` file contains the data sets that represent information about different applications. The file scan agent compares each data set to the actual file system data to find out whether an application is installed.

See “**Running software inventory on UNIX, Linux and Mac computers using the `filesan.rule` file**” on page 55.

Each data set in the `filesan.rule` file consists of two lines of data. The first line is the application description data, and the second line is the matching criteria data. The application description data consists of the product name, the manufacturer, the version, and the description of the application. The matching criteria data includes a file name or the absolute path to the file that is part of the application, file size, and cyclic redundancy check (CRC). When the file scan agent finds this file in the specified directories, the associated product is reported as part of the inventory on that system.

A data set that represents information about an application in the `filesan.rule` file looks as follows:
A default `filescan.rule` file is included in the Inventory Plug-in installation package for each platform. It contains an example list of some common applications.

Symantec recommends that you configure the default `filescan.rule` file to include the additional applications that the software inventory should report. You can also add entries for the applications that are developed in-house.

After you configure the `filescan.rule` file, you can create a Quick Delivery task to redistribute it to all managed UNIX, Linux, and Mac computers.

Running software inventory on UNIX, Linux and Mac computers using the `filescan.rule` file

To run the software inventory using the `filescan.rule` file, you must have the Symantec Management Agent and the Inventory Plug-in installed on your managed UNIX, Linux, and Mac computers. The Inventory Plug-in installation package includes a default `filescan.rule` file that contains an example list of some common applications.

You can configure the default `filescan.rule` file and add the applications that you want to be reported. You can also use the aex-filesurveyor utility to scan your UNIX, Linux, and Mac systems for executables. The output of the scan is formatted for use as a `filescan.rule` file. After you create or configure a `filescan.rule` file, you can distribute it to the managed computers.

The file scan agent uses the settings of the Inventory task or policy to scan the directories. If you want to change the set of the directories that are scanned, you must configure the advanced settings of the Inventory task or policy. If you do not specify any directories, then all local drives are scanned.

See “About software inventory using the `filescan.rule` file” on page 54.

Before you perform this step, ensure that you have prepared the managed computers for inventory.
To run software inventory using filescan.rule file

1. *(Optional)* Copy the default filescan.rule file from the managed computer to the Notification Server computer and configure it.

2. *(Optional)* To distribute the configured filescan.rule file to the managed computers, create a **Quick Delivery** task in the **Symantec Management Console**.

   Copy the filescan.rule file to the following folder:

   `/opt/altiris/notification/inventory/etc/`

   You can use the following universal path with custom installation directories:

   `\aex-helper info path -s INVENTORY\`/etc/

3. For the Inventory policy that gathers software inventory, ensure that you check the **File properties - manufacturer, version, size, internal name, etc.** box.

The next step is to view inventory results.

See “**Viewing inventory data in reports**” on page 45.
Agentless inventory of UNIX and Linux servers

This chapter includes the following topics:

■ About gathering agentless inventory
■ Gathering agentless inventory

About gathering agentless inventory

Inventory for Network Devices lets you gather agentless inventory data from the discovered SNMP network devices such as computers, network printers, network-attached storage devices, and network backup devices. To gather inventory, agentless tasks run on discovered devices and report the data to Notification Server. The data is stored in the Configuration Management Database (CMDB). You can configure the automated tasks that are scheduled to run at regular intervals to keep your inventory data current.

When you configure agentless inventory tasks, you specify the following:

■ Which devices to inventory
■ When to run the task

You can configure multiple tasks to meet your needs.

You can create and configure agentless inventory tasks in the following ways:

Creating a task with Agentless Inventory wizard. The wizard guides you through the creation and configuration of agentless inventory tasks. You can later edit the advanced settings and schedules of a task on the task page.

See “Creating agentless inventory tasks using the wizard” on page 59.
Creating a task manually

You can manually create tasks from the Agentless Inventory Tasks Web Part. This option lets you configure more advanced settings and schedules.

See “Manually creating, scheduling, modifying, and stopping agentless inventory tasks” on page 60.

You can only gather inventory from the SNMP-enabled devices on your network that are already discovered. Run the Network Discovery task to discover your network devices and create resources for them in the CMDB. Make sure that the connection profile of the Network Discovery task has the SNMP turned on.

See “About Network Discovery” on page 35.

Agentless inventory tasks use connection profiles to manage the protocols that are used to communicate with network devices. Connection profiles are components of the Symantec Management Platform. When a device is discovered, a resource for that device is created in the CMDB. The resource keeps a record of the protocols that were used to communicate with the device. When you use agentless inventory tasks, you do not specify a connection profile or protocols. Agentless inventory tasks automatically use the same protocols that were enabled when the device was discovered.

Gathering agentless inventory

You can gather inventory data of discovered SNMP devices such as computers, network printers, network-attached storage devices, and network backup devices. Agentless inventory tasks use connection profiles to manage the protocols that were used to communicate with network devices. When a device is discovered, a resource for that device is created in Configuration Management Database (CMDB). The resource keeps a record of the protocols that were used to communicate with the device. Agentless inventory tasks use the same protocols to gather the inventory.

Symantec recommends you to use the following workflow for gathering agentless inventory:
Table 5-1  Process for gathering agentless inventory

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Prepare computers for gathering agentless inventory</td>
<td>You can gather inventory of the SNMP-enabled devices on your network that are already discovered. Make sure that all the network devices for which you want to gather agentless inventory are already discovered. See “About Network Discovery” on page 35.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Create agentless inventory task using the wizard</td>
<td>Use the wizard to create and schedule agentless inventory tasks. See “Creating agentless inventory tasks using the wizard” on page 59.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Manually create or customize agentless inventory task</td>
<td>Create, configure, or stop agentless inventory tasks. See “Manually creating, scheduling, modifying, and stopping agentless inventory tasks” on page 60.</td>
</tr>
<tr>
<td>Step 4</td>
<td>View agentless inventory reports</td>
<td>View reports that were created by running agentless inventory tasks. See “Viewing agentless inventory results” on page 62.</td>
</tr>
</tbody>
</table>

Creating agentless inventory tasks using the wizard

The wizard guides you through the process of creating agentless inventory tasks and configuring basic settings. You can later configure the advanced settings and schedule the tasks on the task page.

This task is a step in the process of gathering agentless inventory from network devices.

Before you perform this step, ensure that you have mapped the SNMP devices to the data that you want to gather.

To create agentless inventory tasks for network devices using the inventory wizard

1. In the Symantec Management Console, on the Home menu, click Discovery and Inventory > Agentless Inventory.
2. In the Agentless Inventory Quick Start Web Part, click Run inventory wizard.
In the **Agentless inventory task creation wizard**, on the **Choose devices to inventory** page, do the following:

- Select **Choose devices**, and then, in the drop-down list, click the group of target devices that you want to gather inventory from.

- Under **Include Device Types**, check the types of devices that you want to gather inventory from.

- (Optional) To gather inventory from an individual device, in the wizard, select **Individual device**, and then, in the drop-down list, click the device that you want to gather inventory from.

This list includes all SNMP-enabled devices that have been previously discovered and have resources in the Configuration Management Database (CMDB).

On the **Inventory network task name** page, type a name for the task, and then click **Next**.

On the **Schedule task** page, configure the task schedule, and then click **Finish**.

See “To schedule agentless inventory tasks” on page 61.

(Optional) To view the created task, do one of the following:

- In the Symantec Management Console, on the **Home** menu, click **Discovery and Inventory > Agentless Inventory**, and then view the task in the **Agentless Inventory Tasks** Web Part.

  Note that to view the newly created task, you may need to click the **Refresh** symbol.

- In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**, and then, in the left pane, under **Jobs / Tasks**, expand **System Jobs and Tasks > Discovery and Inventory**.

The next step is to view the agentless inventory data.

See “Viewing agentless inventory results” on page 62.

Manually creating, scheduling, modifying, and stopping agentless inventory tasks

You can manually create, modify, and stop agentless inventory tasks on the **Agentless Inventory Home** page.

See “About gathering agentless inventory” on page 57.

This task is a step in the process for gathering agentless inventory.

Before you perform these steps, ensure that you have mapped the SNMP devices to the data that you want to gather.
To manually create agentless inventory tasks

1. In the Symantec Management Console, on the Home menu, click Discovery and Inventory > Agentless Inventory.

2. In the Agentless Inventory Tasks Web Part, on the Available Tasks tab, on the toolbar, click New.

3. In the New Agentless Inventory Task dialog box, give the task a descriptive name, and then do the following:
   - Select Group of Devices, and then, in the drop-down list, click the group of devices that you want to gather inventory from.
   - Under Group of Devices, check the types of devices that you want to gather inventory from.
   - (Optional) To gather inventory from an individual device, select Individual device, and then, in the drop-down list, click the device that you want to gather inventory from.
     This list includes all SNMP-enabled devices that have been previously discovered and have resources in the Configuration Management Database (CMDB).
   - (Optional) Click Advanced, specify the maximum number of threads per inventory task, and then click OK.
     During the inventory process, a separate thread is used for each device. The maximum number of threads is based on the amount of traffic that you want this task to generate and on the capacity of your Notification Server computer.

4. Click OK.

To schedule agentless inventory tasks

1. In the Symantec Management Console, on the Home menu, click Discovery and Inventory > Agentless Inventory.

2. In the Agentless Inventory Tasks Web Part, on the Available Tasks tab, click the task that you want to schedule, and then click Schedule.

3. In the New Schedule dialog box, configure the task schedule according to your needs, and then click Schedule.

To configure or stop agentless inventory tasks

1. In the Symantec Management Console, on the Home menu, click Discovery and Inventory > Agentless Inventory.

2. In the Agentless Inventory Tasks Web Part, on the Available Tasks tab, click the task that you want to schedule, and then do one of the following:
To configure the task run schedule, on the toolbar, click **Schedule**. In the **New Schedule** dialog box, configure the task according to your needs, and then click **Schedule**.

To configure the task settings, on the toolbar, click the **Edit** symbol. In the **New Agentless Inventory Task** dialog box, configure the task according to your needs, and then click **OK**.

To stop the task, click the **Tasks Run** tab, click the task that you want to stop, and then, on the toolbar, click **Stop**.

The next step is to view the agentless inventory data.

See “Viewing agentless inventory results” on page 62.

### Viewing agentless inventory results

The data collected by the inventory tasks is stored in the CMDB.

You can view the collected data and the additional details about the devices in the **Resource Manager** or on the **Agentless Inventory Home** page.

The **Agentless Inventory Home** page presents a data summary of inventoried network devices. On this page you can also see the status of agentless inventory tasks.

This task is a step in the process for gathering agentless inventory.

**To view agentless inventory data in the Resource Manager**

1. In the Symantec Management Console, on the **Manage** menu, click **Resource**.
2. In the **Select Resource** dialog box, click the resource that you want to view, and then click **OK**.

**To view agentless inventory data on the Agentless Inventory Home page**

1. In the Symantec Management Console, on the **Home** menu, click **Discovery and Inventory > Agentless Inventory**.
2. On the **Agentless Inventory Home** page, view the **Devices Inventoried By Type (Last 30 Days)** and **Agentless Inventory Tasks** Web Parts.
3. On the **Resource Manager** page, on the toolbar, click **View > Inventory**, and then, in the navigation pane, under **Data Classes**, navigate to **Network Device Data** to view the inventory data.
Configuration Management

- Chapter 6. Installing the Symantec Management Agent for UNIX, Linux, and Mac
- Chapter 7. Patch Management for Linux
- Chapter 8. Software Management for Linux
- Chapter 9. Virtualization Management
Installing the Symantec Management Agent for UNIX, Linux, and Mac

This chapter includes the following topics:

- About the Symantec Management Agent for UNIX, Linux, and Mac
- About agent registration
- Methods of installing the Symantec Management Agent for UNIX, Linux, and Mac
- Installing the Symantec Management Agent manually on UNIX, Linux, and Mac computers
- Configuring the Symantec Management Agent using the configuration policies

About the Symantec Management Agent for UNIX, Linux, and Mac

The Symantec Management Agent is the software that establishes communication between the Notification Server computer and the computers in your network. Computers with the Symantec Management Agent installed on them are called managed computers. The Notification Server computer interacts with the Symantec Management Agent to monitor and manage each computer from the Symantec Management Console.

The Notification Server computer and the Symantec Management Agent work together to provide the following types of functionality for managed computers:
- Monitoring hardware and software
- Scheduling software installations and file updates
- Collecting basic inventory information
- Managing policies and packages

You can install the Symantec Management Agent on Windows, Linux, UNIX, and Mac computers. The Symantec Management Agent also lets you install and manage solution agent plug-ins that add additional functionality to the agent. For example, installing the Inventory plug-in lets you gather detailed hardware and software information from all of your managed computers.

See “Methods of installing the Symantec Management Agent for UNIX, Linux, and Mac” on page 66.

### About agent registration

The agent registration feature allows the Symantec Management Agent to communicate with Notification Server. Notification Server must approve the agent registration to allow the agent to communicate with Notification Server. The agent registration feature requires a client computer to be allowed to communicate with a Notification Server before it can be managed by this Notification Server.

Different agent installation scenarios handle the agent registration as follows:

**Push install**

The agent receives the push install token that allows the agent to automatically bypass the registration on Notification Server.

**Pull install**

When the token is not available or it has expired during the push install, the agent bypasses the registration based on the agent registration policy.

**CEM offline package**

If you install the agent using the CEM offline package, the agent is automatically registered on Notification Server. In this case, the process of the agent registration includes receiving the certificates that let the agent to identify Notification Server and receiving the certificates that prove the agent’s identity to Notification Server.

You can perform the agent registration in following ways:

- Enable the **Cloud-enabled Management Settings** policy and target it to required computers.
- Generate an offline package to install the Symantec Management Agent on a remote computer in the external network.

## Methods of installing the Symantec Management Agent for UNIX, Linux, and Mac

You can install the Symantec Management Agent for UNIX, Linux, and Mac in different ways.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Push installation from the Symantec Management Console</td>
<td>A push installation can be accomplished from the Symantec Management Console without touching individual client computers. You must enter root or administrator user credentials at the console.</td>
</tr>
<tr>
<td>Pull installation from a browser on a client computer.</td>
<td>If SSH is not available, or if you want to install the Symantec Management Agent for UNIX, Linux, and Mac on the remote computers that have limited network access, or the target computers are behind a firewall, you can pull the Symantec Management Agent to each computer. You can download Symantec Management Agent installer from the Pull install page and follow a standard installation procedure on a target computer. See “Installing the Symantec Management Agent for UNIX, Linux, and Mac with a manual pull” on page 73.</td>
</tr>
<tr>
<td>Manually, using the aex-bootstrap file.</td>
<td>A manual installation is a more controlled process typically performed by UNIX/Linux administrators, with a high degree of control over the client computers or systems. On the other hand, manual installations require that you manually create scripts or touch each server computer individually to complete the installation. See “Manually installing the Symantec Management Agent for UNIX, Linux, and Mac using the aex-bootstrap file” on page 74.</td>
</tr>
<tr>
<td>Manually, using native packages.</td>
<td>See “Manually installing the Symantec Management Agent for UNIX, Linux, and Mac using native packages” on page 76.</td>
</tr>
</tbody>
</table>
Installing the Symantec Management Agent manually on UNIX, Linux, and Mac computers

You can install the Symantec Management Agent with a manual push or a manual pull. It is recommended to install the Symantec Management Agent by manually pushing to selected computers. However, to install on the remote computers that have limited network access or are behind a firewall, you may need to perform a manual pull.

Table 6-2 Process for installing the Symantec Management Agent manually on UNIX, Linux, and Mac computers

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Select the computers to which you want to install the agent and plug-ins. | You have the following options for selecting computers:  
- Network Discovery  
- Manual selection by adding client host names or IP addresses  
- Active Directory Import  
- Import using a comma-separated values file. |
| Step 2 | Verify that the computers meet the installation prerequisites. | Each computer must meet the hardware prerequisites and the software prerequisites before you can install the Symantec Management Agent on it.  
See “Symantec Management Agent for UNIX, Linux, and Mac installation prerequisites” on page 69. |
| Step 3 | (Optional) Define the agent registration policies. | After you install the Symantec Management Agent, it sends out a registration request to Notification Server to establish trust between the server and the client.  
The default agent registration policy allows automatic registration of all agents. You can modify the default policy or create custom policies to specify more restrictive rules.  
See “Creating an agent registration policy” on page 70. |
| Step 4 | Specify the installation settings. | The UNIX, Linux, and Mac installation settings let you configure the communication and the authentication settings for the Symantec Management Agent for UNIX, Linux, and Mac. If you import computer names from a CSV file, you can specify these settings in the CSV file. You can also set or change these settings from the Symantec Management Console.  
See “Specifying the Symantec Management Agent for UNIX, Linux, and Mac installation settings” on page 72. |
Table 6-2  Process for installing the Symantec Management Agent manually on UNIX, Linux, and Mac computers (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 5 | Install the Symantec Management Agent using the appropriate method.     | The preferred method is to push the Symantec Management Agent to the selected computers. However, if any of the computers are behind a firewall or are difficult for Notification Server to access, you can pull the Symantec Management Agent to them.  
See “Installing the Symantec Management Agent for UNIX, Linux, and Mac with a manual pull” on page 73.  
See “Manually installing the Symantec Management Agent for UNIX, Linux, and Mac using the aex-bootstrap file” on page 74.  
See “Manually installing the Symantec Management Agent for UNIX, Linux, and Mac using native packages” on page 76. |
| Step 6 | View and manage the agent registration status to verify successful registration. | The Agent Registration Status report lets you view and manage all registration requests and completed registrations from Symantec Management Agents.  
See “Viewing and managing the agent registration status” on page 76. |

Creating a CSV file for importing UNIX, Linux, and Mac computers

If you want to install the Symantec Management Agent for UNIX, Linux, and Mac on a large number of computers that require different connection and configuration settings, we recommend that you use a CSV file to import the computers and configure the installation settings. The CSV file is a comma-delimited text file that includes the DNS names or the IP addresses of the client computers on which you want to install the Symantec Management Agent. Each line in the CSV file represents a computer entry that is imported into the Symantec Management Agent Install page. The CSV file can also contain the installation settings for each computer.

A CSV template file for importing UNIX, Linux, and Mac computers (CSVTemplate.csv) is provided with the Symantec Management Platform. The column header of the CSV template indicates the data that is required and the valid values that you can use.

Warning: The CSV file format (list separator) must meet the regional settings of the server. For example, the sample CSVTemplate.csv file uses the "English (United States)" regional settings with a comma "," as a list separator. You can view the Symantec Management Platform’s regional settings in the Windows Control Panel.
This task is a step in the process for installing the Symantec Management Agent manually.

To create a CSV file for importing UNIX, Linux, and Mac computers

1. In the Symantec Management Console, on the Actions menu, click Agents/Plug-ins > Push Symantec Management Agent.

2. On the Symantec Management Agent Install page, on the Install Agent for UNIX, Linux and Mac tab, under Rollout Agent for UNIX, Linux and Mac to Computers, right-click CSV file template, and then click Save Target As.

3. In the Save As dialog box, type a suitable file name for the CSVTemplate.csv file, browse to the appropriate location, and then click Save.

4. Open the saved CSV file in a text editor and enter the information for each computer on which you want to install the Symantec Management Agent for UNIX, Linux, and Mac.

   You do not have to use all of the fields. You can use only the fields that you need, such as computer name, root name, root password, and so on.

   The settings that you can specify in the CSV file are identical to the settings that you can set from the Install Settings window in the Symantec Management Console.

5. When you have finished, save the CSV file.

Symantec Management Agent for UNIX, Linux, and Mac installation prerequisites

Your computer must meet the hardware and software prerequisites before you can install the Symantec Management Agent for UNIX, Linux, and Mac.

This topic is a step in the process for installing the Symantec Management Agent manually.
Table 6-3  Symantec Management Agent for UNIX, Linux, and Mac installation prerequisites

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Any of the following operating systems:</td>
</tr>
<tr>
<td></td>
<td>• Solaris 10 (x86, x86_64 and SPARC)</td>
</tr>
<tr>
<td></td>
<td>• Solaris 11 (x86, x86_64 and SPARC)</td>
</tr>
<tr>
<td></td>
<td>• Red Hat Enterprise Linux 5.10, 5.11 (x86 and x86_64)</td>
</tr>
<tr>
<td></td>
<td>• Red Hat Enterprise Linux 6.0, 6.1, 6.2, 6.3, 6.4, 6.5 (x86 and x86_64)</td>
</tr>
<tr>
<td></td>
<td>• Red Hat Enterprise Linux 7.0</td>
</tr>
<tr>
<td></td>
<td>• SUSE Linux Enterprise Server 10, 11 SP1, 11 SP2, 11 SP3 (x86 and x86_64)</td>
</tr>
<tr>
<td></td>
<td>• SUSE Linux Enterprise Desktop 10, 11 SP1, 11 SP2, 11 SP3 (x86 and x86_64)</td>
</tr>
<tr>
<td></td>
<td>• Mac OS X 10.8.x, 10.9.x, 10.10.x</td>
</tr>
<tr>
<td></td>
<td>• Mac OS X Server 10.8.x, 10.9.x, 10.10.x</td>
</tr>
<tr>
<td></td>
<td>• HP-UX 11.11 (PA-RISC), 11.31 (PA-RISC/IA64)</td>
</tr>
<tr>
<td></td>
<td>• AIX 6.1 PPC, 7.1 Standard</td>
</tr>
<tr>
<td>Hard disk space</td>
<td>60 MB minimum</td>
</tr>
<tr>
<td>RAM</td>
<td>25 MB minimum</td>
</tr>
<tr>
<td>Access rights</td>
<td>Root user or a user with administrative privileges is required on UNIX/Linux and Mac platform.</td>
</tr>
<tr>
<td>Remote SSH connections enabled</td>
<td>Remote SSH connections must be enabled. There must be an SSH server running on the client computer and the firewall must be configured to allow an incoming SSH connection.</td>
</tr>
<tr>
<td>Outgoing connection to Notification Server enabled</td>
<td>The firewall must be configured to allow an outgoing connection to a WEB port on Notification Server.</td>
</tr>
</tbody>
</table>

Creating an agent registration policy

Agent registration policies let you automate the agent registration process. An agent registration policy is a set of rules that determine how the incoming registration requests are processed. In the registration request content, Symantec Management Agent sends its host name, MAC address, IP address, FQDN, and logged on user data. The agent registration policy uses the registration request data and the rules that you define within the policy to decide if the request is allowed or blocked.
Warning: The default agent registration policy automatically allows all agents to communicate with Notification Server. You can modify the default policy or create custom policies to restrict the agents that can communicate with Notification Server. If no active policies are available, the status of each incoming registration request is set to pending.

You can view the registration requests in the Agent Registration Status report. You can access this report in the Symantec Management Console, under Reports > Notification Server Management > Registration.

See “Viewing and managing the agent registration status” on page 76.

To create an agent registration policy

1. In the Symantec Management Console, on the Settings menu, click All Settings.
2. In the left pane, under Settings, expand Agents/Plug-ins > Symantec Management Agent > Settings.
3. Right-click Registration Policies, and then click New > Registration Policy.
4. On the right pane, specify the settings of the agent registration policy as follows:

   **Rules**

   Lets you define different types of masks for agent identification using the request data. For example, you can define a host name mask, an IP address mask, and a logged on user name mask.

   A single policy can contain unlimited number of masks of any type. During the mask matching process, Notification Server treats different mask types as logical AND operation and similar mask types as logical OR operation.

   For example, a policy with the following masks allows registration of all agents that have the name that matches mask “*test” and their IP address is either 10.31.12.1, 10.31.12.2, or any from 255 IP addresses from the 10.31.15.0 subnet:

   - Host = *test
   - IP=10.31.12.1
   - IP=10.31.12.2
   - IP=10.31.15.0/24

   **Note:** Asterisk is accepted for all rules except for IP address. If you want to specify an IP range in a rule, you must define it with the subnet mask. For example, instead of typing 10.31.15.*, you enter 10.31.15.0/24.
Actions  Lets you define the rule for complied agent processing with the following options:

■ Allow
   The agents are automatically registered and you do not need to accept them manually.

■ Block
   Requests from these agents are declined.

Note that if two policies are applicable to a registration request, and one of them allows registration and the other blocks it, the blocking policy is applied to the request.

5  Turn on the policy.
   At the upper right of the page, click the colored circle, and then click **On**.

6  Click **Save changes**.

Specifying the Symantec Management Agent for UNIX, Linux, and Mac installation settings

The Symantec Management Agent installation settings are the communication and the authentication settings for the Symantec Management Agent for UNIX, Linux, and Mac. You must specify the appropriate privileged account login name and password for each target computer.

When you import computers from a CSV file, you can specify the appropriate installation settings for each computer in the CSV file. If you do not specify any settings in the CSV file, or if you added computers manually, you need to specify the appropriate settings for each target computer before you install the Symantec Management Agent for UNIX, Linux, and Mac.

You can specify installation settings for a particular computer or for multiple computers. If you select multiple computers, the same installation settings are applied to each computer. You can also clone the current installation settings from a computer and apply it to other computers.

See “Creating a CSV file for importing UNIX, Linux, and Mac computers” on page 68.

This task is a step in the process for installing the Symantec Management Agent manually.
To specify the Symantec Management Agent for UNIX, Linux, and Mac installation settings

1. In the Symantec Management Console, on the Actions menu, click Agents/Plug-ins > Push Symantec Management Agent.

2. On the Symantec Management Agent Install page, on the Install Agent for UNIX, Linux and Mac tab, under Rollout Agent for UNIX, Linux, and Mac to Computers, in the computer list, click the computer for which you want to change the Symantec Management Agent installation settings, and then click Installation settings.

   If you want to specify identical installation settings for multiple computers, or if you want to clone the current installation settings from another computer, select the appropriate computers.

3. (Optional) If you want to clone the current installation settings from a particular computer, in the Installation Settings dialog box, in the Load settings drop-down list, select the appropriate computer.

   The option Load settings of appears at the upper right of the Installation Settings dialog box if you have selected multiple computers.

4. Specify the appropriate installation settings for the selected computers.

5. In the Installation Settings dialog box, click OK.

Installing the Symantec Management Agent for UNIX, Linux, and Mac with a manual pull

If SSH is not available, or if you want to install the Symantec Management Agent for UNIX, Linux, and Mac on remote the computers that have limited network access, or the target computers are behind a firewall, you can pull the Symantec Management Agent to each computer. You, or anybody else with administrator rights, can log on to each computer, access Symantec Management Platform through a URL, and download the install bootstrap program that performs the Symantec Management Agent for UNIX, Linux, and Mac installation.

The URL of the Download Symantec Management Agent for UNIX, Linux and Mac page is shown on the Symantec Management Agent Install page, under Download Page URL for UNIX, Linux and Mac. You can view the page, but you cannot change this setting.

This task is a step in the process for installing the Symantec Management Agent manually.
To preview the Download Symantec Management Agent for UNIX, Linux and Mac page

1. In the Symantec Management Console, on the Actions menu, click Agents/Plug-ins > Push Symantec Management Agent.

2. On the Symantec Management Agent Install page, on the Install Symantec Management Agent for UNIX, Linux and Mac tab, under Download Page URL for UNIX, Linux and Mac users, in the Select platform drop-down list, click the appropriate platform, and then click View page.

To pull the Symantec Management Agent for UNIX, Linux and Mac to a remote computer

1. Log on to the remote computer as an administrator.

2. On the remote computer, open a Web browser, and then go to the following URL:

   http://SMPName/Altiris/UnixAgent/AltirisUnixAgentDownload.aspx?ID=Platform

   where SMPName is the name of your Symantec Management Platform computer and Platform is the appropriate platform.

3. Follow the instructions that are displayed on the Download Symantec Management Agent for UNIX, Linux and Mac page for downloading and running the install bootstrap program on the remote computer.

Manually installing the Symantec Management Agent for UNIX, Linux, and Mac using the aex-bootstrap file

This procedure uses the aex-bootstrap-linux file as an example. To obtain file names for other UNIX or Linux platform bootstrap files, see the article Installation Files and Command Lines for the Unix, Linux and Mac Agent and Solutions Using Native Packages at:


The use of the configuration file .aex-agent-install-config.xml is optional. If the bootstrap file does not find this file, it uses default installation settings.

To manually install the Symantec Management Agent for UNIX, Linux, and Mac using the aex-bootstrap file

1. Make sure that you are logged in to the UNIX or Linux server as root.

2. Set up name resolution via DNS or by adding Notification Server’s host name and IP address to the UNIX or Linux server's /etc/hosts file.

3. In the Symantec Management Console, on the Settings menu, click Agents/Plug-ins > Symantec Management Agent.
4 In the left pane, expand Settings and click Symantec Management Agent install.

5 On the Symantec Management Agent Install page, on the Install Agent for UNIX, Linux and Mac tab, under Download Page URL for UNIX, Linux, and Mac Users, in the Select platform drop-down list, select the appropriate platform.

6 Click View page.

7 Click install bootstrap program to download the program to the Linux server.

8 On the Linux server, save the file as aex-bootstrap-linux file in the same directory as the .aex-agent-install-config.xml file.

9 Go to the directory where you saved aex-bootstrap-linux file.

10 Enter the following command:

```bash
chmod u+x aex-bootstrap-linux && ./aex-bootstrap-linux http://<NS Server hostname>
```

**Note:** If you want to install the agent to a custom directory or your Notification Server is accessible only through a specific port, you must use additional parameters with aex-bootstrap-linux command.

The aex-bootstrap-linux --help displays the full list of parameters.

The install bootstrap program connects to the specified Notification Server and downloads the full Symantec Management Agent package. It then passes execution to the agent-upgrade script inside that package. The agent-upgrade script installs, configures, and starts the agent. If the aex-bootstrap program cannot contact Notification Server, it schedules itself to run again in a few minutes, using the at command.

The agent is installed to the /opt/Altiris/notification/nsagent directory on the UNIX or Linux server. After the resource membership update runs on Notification Server, the agent reports basic inventory. It also appears in the All platforms filters and targets. At that point, you can enable inventory policies or other solutions you are working with.

See “Methods of installing the Symantec Management Agent for UNIX, Linux, and Mac” on page 66.
Manually installing the Symantec Management Agent for UNIX, Linux, and Mac using native packages

This method is the most direct command-line-based installation of the Symantec Management Agent. However, it does require configuration either before or after installation. All other installation methods have a default configuration, but this one does not.

**Note:** When you install the Symantec Management Agent using the a native package, you also need to install additional packages: Client Task Agent, Base Task Handlers, Inventory Rule Agent, and Software Management Framework Agent.

To manually install the Symantec Management Agent for UNIX, Linux, and Mac using a native packages

1. Copy the platform-specific `aex-nsclt` file from the following location the on Notification Server computer:

   ```
   %installdir%\Notification Server\NSCap\bin\UNIX\Agent
   ```

2. Set up appropriate environment variables, if desired.

3. Log in to the UNIX or Linux server as root.

4. On the Linux or UNIX server, run the installer for the desired platform by entering the following command line:

   ```
   rpm -i aex-nsclt<version number>.rpm
   ```

5. Repeat the steps for remaining `aex-basetasks`, `aex-ctagent`, `aex-iragent` and `aex-smfagent` packages.

See “Methods of installing the Symantec Management Agent for UNIX, Linux, and Mac” on page 66.

Viewing and managing the agent registration status

The **Agent Registration Status** report lets you view all registration requests and completed registrations from Symantec Management Agents.

In this report, you can see the computers that the **Agent Registration Policy** has automatically allowed or blocked. Note that for direct Symantec Management Agent push installation, the registration is bypassed. However, the computers are still displayed in the report and their status is set to **Allowed**. If no **Agent Registration Policy** applies to the computer, its status is set to **Pending** and the right-click menu lets you manually allow or block it. The right-click menu also lets you revoke the trust of the agents that you have previously allowed.
See “Creating an agent registration policy” on page 70.

Incoming registration requests are distinguished by the resource keys and they are merged based on the resource keys lookup.

In some situations, duplicate registration requests may appear. For example, if you reinstall the agent on a computer that is already registered on Notification Server, its public key changes. In this case, Symantec recommends that you approve the registration request to let this computer continue communicating with Notification Server. Also, the duplicate registration requests may appear if you have computers with identical resource keys in your network. In this case, Symantec recommends not to approve the duplicate registration request because it may cause connectivity issues for the resource that previously existed.

If you have duplicate registration requests in your report, the requests are handled as follows:

- If the initial request is allowed and the duplicate request is also allowed, the duplicate request is merged with the existing resource and the report is updated to display a single entry.

- If the initial request is allowed but the duplicate request is blocked, both requests remain in the list. The allowed request represents the actual resource and the duplicate request in blocked or pending state represents the registration attempt from a potentially duplicated resource.

The Agent Registration Status report keeps all requests for audit purposes and lets you continuously observe them.
To view and manage the agent registration status

1. In the Symantec Management Console, on the Reports menu, click All Reports.

2. In the left pane, under Reports, expand Notification Server Management > Registration, and then click Agent Registration Status.
3 (Optional) On the Agent Registration Status page, use the right-click menu options to modify the status of the agent. Note that depending on the status of the agent, the right-click options vary.

**Allow**

You can allow the agents that are in the Pending, Blocked, or Revoked state.

If you allow a blocked agent, the trust is granted next time when the agent sends a registration request to Notification Server.

**Block**

You can block the agents that are in the Pending or Revoked state.

If you block a revoked computer, its functional status does not change. However, changing the status lets you differentiate the revoked computers that should never again connect to Notification Server from the revoked computers that may still require your attention.

Note that computers with the Blocked status are removed from the list after a predefined period of time if no new registration requests were sent from the same computer during this time. The default period is three months, but you can change it on the Purging Maintenance page.

**Revoke**

You can revoke the registration of the agents that you have previously allowed. For example, you can revoke the registration for the client computer that is reported missing or stolen. After you revoke the agent, it stops receiving policies from Notification Server. Also, a revoked computer cannot be used as a site server.

During the revocation of internal agent trust, the agent encryption key registration gets marked as revoked on Notification Server. Revoked agents do not receive policies and do not run tasks. Also, the revoked agent clears locally stored policies to minimize its activity. After the revocation, Symantec Management Agent is forced to reinitiate the registration process.

The agent receives information about its revoked status next time when it tries to access secured data. Notification Server does not notify the agent about the revocation event when it occurs.

Note that the revoked agent remains in the Revoked state even if the agent registration policy allows it. You must manually manage the revoked computers, if you want to change their state.
The default Symantec Management Agent configuration settings are suitable for a small Symantec Management Platform environment. As your environment grows, or if your organization has particular requirements, you need to make the appropriate configuration changes.

The agent configuration settings are applied to the appropriate managed computers using agent configuration policies. You can modify these policies to change the settings at any time. The new configuration settings are applied to the agents when the managed computers get their next policy updates (which is typically once a day).

**Table 6-4 Types of agent configuration policies**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global settings</td>
<td>The global configuration settings apply to all Symantec Management Agents on all managed computers. These settings are applied as a single policy that automatically targets every managed computer. See “Configuring the global agent settings” on page 81.</td>
</tr>
<tr>
<td>Targeted settings</td>
<td>The targeted agent settings are the general parameters that control the Symantec Management Agent, including how the agent communicates with Notification Server. You can modify the default policies that are supplied with the Symantec Management Platform. You can create your own targeted agent settings policies and apply them to the appropriate managed computers. See “Configuring the targeted agent settings” on page 81.</td>
</tr>
<tr>
<td>Maintenance windows</td>
<td>A maintenance window is a scheduled time and duration when maintenance operations may be performed on a managed computer. A maintenance window policy defines one or more maintenance windows. You can modify the default policy that is supplied with the Symantec Management Platform. You can create your own maintenance window policies and apply them to the appropriate managed computers. See “Configuring maintenance window policies” on page 83.</td>
</tr>
</tbody>
</table>

The targeted settings policies and maintenance window policies are applied to the managed computers that are included in the specified policy targets. These targets...
may not be mutually exclusive. Two or more policies of the same type may apply to the same managed computer.

Configuring the global agent settings

The global configuration settings are those that you would not need to set differently on different computers, so they apply to all Symantec Management Agents on all managed computers. These settings are applied as a global agent settings policy, so they are updated in the same way as any other policy. By default, the global agent settings policy is refreshed hourly. You cannot delete or disable the global agent settings policy, or create alternative versions of it.

If you want to specify agent settings for particular groups of managed computers, you need to configure the appropriate targeted agent settings policies.

To configure the global agent settings

1. In the Symantec Management Console, on the Settings menu, click Agents/Plug-ins > Global Settings.
2. Make the appropriate configuration settings on the following tabs:
   - General: Specify the Tickle/Power Management and Package Multicast settings.
   - Authentication: Specify the user name and password that the Symantec Management Agent uses when it connects to Notification Server or to a package server.
   - Events: Specify Notification Server events that you want to capture.
3. Click Save changes.

See “Configuring the Symantec Management Agent using the configuration policies” on page 80.

Configuring the targeted agent settings

The targeted agent settings policy lets you configure the general parameters that control the Symantec Management Agent, including how the agent communicates with Notification Server. You can apply these settings to particular groups of computers. For example, some groups of computers may have different purposes, or you may want to treat servers differently from other managed computers. You can modify the default policies that are supplied with Notification Server or create your own targeted agent settings policies.
If you want to specify some configuration settings that apply to all Symantec Management Agents on all managed computers, you need to configure the global agent settings policy.

To configure the targeted agent settings

1. In the Symantec Management Console, on the Settings menu, click Agents/Plug-ins > Targeted Agent Settings.

2. In the left pane, do one of the following:
   - To create a new targeted agent settings policy, click Create new.
   - To set or change the policy name, click the appropriate policy, and then click Rename.
     In the Rename Item dialog box, type the new name, and then click OK.

3. In the right pane, make the appropriate configuration settings on the following tabs:
   - **General**: General settings include the policy download and inventory collection frequencies, and the computers, users, or resource targets to which the policy applies.
   - **UNIX/Linux/Mac**: Provides general settings for UNIX, Linux, and Mac managed computers.
   - **Downloads**: Download settings control how each agent downloads packages during software deliveries. You can enable multicast downloads and configure multicast for both master and client sessions. You can override these settings for individual software delivery policies and tasks.
   - **Blockouts**: Blockout periods are times when all communication between the agent and Notification Server is disabled. You can set up any number of blockout periods.
   - **User Control**: The user control settings are the options that affect what the user of the managed computer can see.
   - **Advanced**: Lets you specify an alternate URL that the Symantec Management Agent can use to access Notification Server, install SSL certificates on managed computers, and turn on the power management feature.

4. (Optional) To restore the policy to its default settings, click Restore Defaults.

5. Click Save changes.
See “Configuring the Symantec Management Agent using the configuration policies” on page 80.

Configuring maintenance window policies

A maintenance window is a scheduled time and duration when maintenance operations may be performed on a managed computer. A maintenance operation is one that changes the state of a computer, causes it to restart, or interferes with a user's ability to operate the computer. For example, installing software and operating system patches, or running a virus scan.

A maintenance window policy defines one or more maintenance windows and is applied to a resource target in the same way as any other policy. These policies provide the maximum flexibility for assigning maintenance windows to computers, without complicating the management of agent settings. If multiple maintenance window policies apply to a single computer, changes to the computer are permitted during any of the maintenance windows.

Using maintenance windows lets you schedule maintenance work on managed computers with minimal effect on workflow and productivity. Also, you can schedule maintenance work on critical servers at different times so no two servers are ever restarted at the same time. A maintenance window may be scheduled for certain times, such as daily, weekly, or monthly. The maintenance window may be available indefinitely or restricted to a particular date range.

When you apply a maintenance window to a managed computer, maintenance tasks, such as patches and software deliveries, can only be carried out on them in the scheduled time period. Symantec Management Agents can download software delivery packages any time, but associated programs can be run only during the maintenance windows.

The Symantec Management Agent processes the policy and provides the functionality that solutions use to determine whether a maintenance window is currently open. Functionality is also provided to allow solutions to inform Notification Server that a maintenance task has been performed.

If the Symantec Management Agent is performing a task as part of a job when the maintenance window expires, the maintenance window is automatically extended until all tasks that are contained in the job are completed.

You can create and modify the maintenance window policies that you need and apply them to the appropriate targets. The default maintenance window policy is applied to all managed computers.
To configure maintenance window policies

1. In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > Maintenance Windows**.

2. In the left pane, do one of the following:
   - To create a new maintenance window policy, right-click the **Maintenance Windows** folder, and then click **New > Maintenance Window**.
   - To modify an existing maintenance window policy, click the appropriate policy.

3. In the right pane, in the **Time zone** drop-down list, click the appropriate option:
   - **Use agent time**: The times are specified without time zone information and are applied at the local time at each managed computer. Maintenance windows open and close at different times depending on the time zones of the managed computers.

   **Use server time**: The times are specified with time zone information, where the time zone offset is that of the server’s time zone where the policy is defined. The maintenance windows open simultaneously irrespective of time zones and are compensated for daylight saving.

      This option ensures that maintenance windows are always coordinated with the specified local time on the server where the policy is created.

   **Coordinate using UTC**: The times are specified with time zone information, where the time zone offset is 0. The maintenance windows open simultaneously irrespective of time zones and are not affected by daylight saving.

   The time zone applies to all of the maintenance windows that are specified in this policy.
4 If you want the policy to take effect on a particular date, rather than as soon as it is enabled, in the upper right corner, click Advanced, then in the Advanced Options dialog box, set the start date and end date, and click OK.

Start

The date that the policy takes effect. The policy must be enabled in the same way as any other policy. You can enable the policy at any time before or after the start date.

End

If you want the policy to be available for a limited period of time, set the appropriate end date. The policy is unavailable after this date, whether or not it is enabled.

This setting is optional. If no end date is specified, the policy is available indefinitely.

5 To create the maintenance windows that you want to include in the policy, click Add Maintenance Window.

6 In each maintenance window, do the following:
   - Under Daily Times, specify the start time of the maintenance window and either the end time or the duration in the corresponding boxes. Alternatively, you can drag the green (start time) and red (end time) arrows to the appropriate places on the time line.
   - Under Repeat Schedule, in the Repeat every drop-down list, select a schedule and then specify the appropriate schedule filters.

7 Under Applied to, specify the maintenance window policy target.

   You can select an existing organizational group, filter, or resource target. You can also select individual resources.

   Details of the selected items are displayed in the grid. You can view the list by targets, resources, computers, or users, and make any necessary additions and deletions.

8 Click Save changes.

See “Configuring the Symantec Management Agent using the configuration policies” on page 80.
Patch Management for Linux

This chapter includes the following topics:

- About Patch Management Solution for Linux
- Differences in patching Red Hat Linux and SUSE Linux
- Patching Linux with Patch Management Solution
- Advanced configuration
- About Linux kernel patching

About Patch Management Solution for Linux

Patch Management Solution for Linux ensures that your Red Hat Linux and SUSE Linux computers have the most up-to-date patches applied and protected against security threats. The solution lets you inventory the managed Linux computers for security vulnerabilities and then reports on the findings. It provides you with the tools that let you download and distribute the needed software updates. Patch Management Solution for Linux lets you set up an automatic update schedule to ensure that managed computers are up-to-date and protected on an on-going basis.

The Patch Management Solution for Linux component of Patch Management Solution supports the following operating systems:

- Red Hat Enterprise Linux: 5.10-5.11, 6.0-6.5, 7
- Novell SUSE Linux Server: 10, 11 SP1, 11 SP2, 11 SP3

See "Differences in patching Red Hat Linux and SUSE Linux" on page 87.
Differences in patching Red Hat Linux and SUSE Linux

Patch Management Solution for Linux supports Red Hat Enterprise Linux and SUSE Linux from Novell.

See “About Patch Management Solution for Linux” on page 86.

While the processes of patching Red Hat Linux and SUSE Linux with Patch Management Suite is very similar, you have to mind the following differences:

- Patch bulletins for Red Hat are called Errata. For SUSE Linux those are called Announcements.
- Credentials that are used to download software updates for Red Hat are called Red Hat Network credentials. For SUSE Linux those are called Novell Customer Center credentials.
- SUSE Linux and Red Hat Linux have separate Import Tasks, Configuration Policy Settings, and Reports in Symantec Management Console.

Patching Linux with Patch Management Solution

Symantec recommends you to use the following workflow:

Table 7-1

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Install or upgrade the Software Update Plug-in</td>
<td>Install the plug-in that manages all of the Patch Management for Linux functionality on a client computer. See &quot;Installing the software update plug-in&quot; on page 88.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure the system assessment scan interval</td>
<td>Specify how often Symantec Management Agent scans Linux software for compliance with patch data. See &quot;Configuring the system assessment scan interval&quot; on page 89.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select software channels for the update</td>
<td>Select the products that you want to import patch metadata for. See “Selecting software channels for Linux” on page 90.</td>
</tr>
</tbody>
</table>
Table 7-1 (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>Schedule the import of patch metadata</td>
<td>Schedule and run the task to download patch metadata. See “Scheduling the import of patch metadata for Linux” on page 90.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Install selected software updates</td>
<td>Select and install software updates from the list. See “Installing software updates for Linux” on page 91.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Review the software delivery reports</td>
<td>Evaluate the results of software update to see the following data:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Computers with successfully updated software</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Computers with software update in progress</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Computers where software update was not successful</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Viewing the software update delivery report” on page 92.</td>
</tr>
</tbody>
</table>

**Installing the software update plug-in**

The software update plug-in manages patch management functionality on a client computer. When a client computer requires a certain software update, the update is sent from the Notification Server computer to the software update plug-in. The software update plug-in ensures that the update is applicable and not already installed, and then installs it.

See “Installing the software update plug-in” on page 88.

The software update plug-in manages all of the Patch Management Solution functionality on a client computer.

**Note:** If you have a large number of computers to which you want to install the software update plug-in, consider deploying it during off-peak hours to minimize network traffic. Deploying the software update plug-in can take some time, depending on the number of managed computers and the Symantec Management Agent settings.
To install the software update plug-in

1 In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**.

2 In the left pane, expand **Software > Patch Management > Software Update Plug-in Install**.

3 (Optional) In the right pane, make any necessary changes. For help, press **F1** or, on the **Help** menu, click **Context**.

4 In the upper right corner of the page, click the colored circle, and then click **On**.

5 Click **Save changes**.

The next step is to configure the Patch Management Solution core settings. See “Configuring software updates download location” on page 94.

Configuring the system assessment scan interval

The system assessment scan lets you periodically inventory operating systems, applications, and installed patches on managed computers with the software update plug-in installed. System assessment information is then used to determine which software updates the managed computer requires. Based on this information, filters are automatically created to assist with the targeting of software update policies.

You can configure how often you want to run the system assessment scan.

Before you perform this step, make sure that you have configured the software updates installation settings.

To configure the system assessment scan interval

1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.

2 In the left pane, click **Software > Patch Management > Linux System Assessment Scan**.

3 In the right pane, under **Schedule**, configure how often to perform the system assessment scan on the managed computers and report it back to Notification Server.

4 Do not change the targeted filter from **Linux Computers with Software Update Plug-in Installed Target** unless you have a specific reason to do so.

5 Click **Save changes**.

The next step is to download the software updates.
Selecting software channels for Linux

Patch Management Solution for Linux lets you choose the software channels for which you want to import patch metadata. Symantec recommends that you select only those channels that are applicable to your managed computers.

The metadata import tasks and software channels are not connected between operating systems. You have to run them separately for SUSE Linux and Red Hat Linux.

To select software channels for Linux

1. In the Symantec Management Console, on the Home menu, click Patch Management.
2. In the left pane, under Patch Management, expand Red Hat Linux or SUSE Linux, depending on the Linux distribution that you want to patch. Then, under Settings, click Remediation.
3. In the right pane, under Red Hat Patch Remediation Settings or Novell Patch Remediation Settings, click either Red Hat Network or Novell Customer Center, depending on the Linux distribution that you want to patch. Then, enter your subscription details and click Save Changes.
4. In the left pane, under Settings, click MetaData Import Task.
5. In the right pane, under Select software channels for import, click Import channels.
6. Under Select software channels for import, check the channels that you want to import patch data from.
7. Click Save changes.

Scheduling the import of patch metadata for Linux

Patch metadata contain package files and the hashes of those files. You can schedule the import of patch metadata to your Notification Server, so you can install packages to managed computers.

The same procedure is applicable for both Red Hat Linux and SUSE Linux, but you have to configure separate schedules for those operating systems.

To schedule the import of patch metadata for Linux

1. In the Symantec Management Console, on the Home menu, click Patch Management.
2. In the left pane, under Patch Management, expand Red Hat Linux or SUSE Linux, depending on the Linux distribution that you want to patch. Then, under Settings, click MetaData Import Task.
3 In the right pane, under Task Status, click New Schedule.

4 In the New Schedule dialog box, select Schedule, and then configure the schedule.

---

**Note:** To reduce the load on Notification Server, Symantec recommends you to use recurrence time longer than one week.

---

**Installing software updates for Linux**

You can install patches that you have imported to Notification Server. You can apply patches one by one or you can choose multiple patches to be applied together.

To apply patches to a managed computer, you have to make sure that a given computer reports system assessment scan data to Notification Server.

To view the list of Linux Computers Not Reporting System Assessment Scan Data

1 In the Symantec Management Console, on the Home menu, click Patch Management.

2 In the left pane, under Patch Management, expand Red Hat Linux or SUSE Linux, depending on the Linux distribution you want to patch.

3 Under Exception Handling, click No Scan Data Reported.

In the Symantec Management Console, you can view the compliance according to the following criteria:

- Compliance by Errata
- Compliance by Announcement
- Compliance by Update
- Compliance by Computer

To install software updates for Linux

1 In the Symantec Management Console, on the Home menu, click Patch Management.

2 In the left pane, under Patch Management, expand Red Hat Linux or SUSE Linux, depending on the Linux distribution that you want to patch. Then, under Compliance and Remediation, click either Compliance by Errata or Compliance by Announcement.

3 In the right pane, under Red Hat Compliance by Erratum or SUSE Compliance by Announcement, click the items that you want to distribute.

4 Right-click the selected items, and then click Distribute Packages.
5  In the **Distribute Software Updates** wizard, in the first step, do the following:
   - In the right pane, under **Software Update Policy Options**, edit the policy name and description.
   - Under **Package Options**, check **Run** to configure a custom schedule.
   - Under **Apply to computers**, click **Apply to > Computers** to specify different targets than **Linux Computer with Software Update Plug-In Installed Target**.
   - Click **Next**.

6  In the second step, in the right pane, at the upper right of the page, click the colored circle, and then click **On**.

7  Click **Distribute software updates**.

---

**Warning:** Symantec does recommend you not to use Patch Management Solution to update Linux kernel packages.

See “**About Linux kernel patching**” on page 94.

Red Hat and Novell assign severity information to each patch. However, a patch deemed non-critical can be critical for your environment. You can create your custom severity levels, and then assign them to errata and patches. You cannot change the severity level that is assigned to an update by the software vendor.

See “**Creating and assigning custom severity levels**” on page 93.

---

**Viewing the software update delivery report**

The **Linux Software Update Delivery Summary** report summarizes the results of all scheduled software update policies. It gives you information about which computers the software update tasks target, and if the updates have been successfully installed. The report also displays if any software update tasks failed, or if they have not yet completed.

Patch Management Solution for Linux also provides other reports that you can view.

**To view the software update delivery summary report**

1  In the Symantec Management Console, on the **Reports** menu, click **All Reports**.

2  In the left pane, expand **Software > Patch Management > Remediation Status**, and then click **Linux Software Update Delivery Summary**.

3  In the right pane, leave the default settings, and then click **Refresh**.
Advanced configuration

Patch Management Solution lets you customize its settings according to your needs. For example, you can use the following workflow:

Table 7-2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create and assign custom severity levels</td>
<td>You can create and assign custom severity levels to patch metadata.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating and assigning custom severity levels” on page 93.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure software updates download location.</td>
<td>You can configure software updates download location.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Configuring software updates download location” on page 94.</td>
</tr>
</tbody>
</table>

Creating and assigning custom severity levels

Errata or announcements deemed critical may not necessarily be critical in your environment. You can create your own custom severity levels and assign them to errata and patches.

You first create custom severity levels, and then assign them to bulletins. You can alter custom severity levels. You cannot alter the vendor-specified severity levels.

The settings that you configure apply to Windows and Linux components of Patch Management Solution.

To create a custom severity level

1. In the Symantec Management Console, on the Settings menu, click All Settings.
2. In the left pane, expand Software > Patch Management > Core Services.
3. In the right pane, click the Custom Severity tab.
4. On the Custom Severity tab, in the Severity Level box, type the name that you want to give the custom severity level. For example, "Install right away!"
5. Click Add.
6. Click Move Up or Move Down to position the custom severity levels in the list.
7. Click Save Changes.
To assign a custom severity level to a software bulletin

1. In the Symantec Management Console, on the Actions menu, click Software > Patch Remediation Center.
2. On the Patch Remediation Center page, in the software bulletin list, right-click a software bulletin, and then click Custom Severity.
3. Click a severity level.
4. Click Refresh to view the new data in the Custom Severity column.

Configuring software updates download location

You can configure to which location the software updates should be downloaded.

The settings that you configure apply to Windows and Linux components of Patch Management Solution.

Before you perform this step, ensure that you have installed or upgraded the software update plug-in.

See “Installing the software update plug-in” on page 88.

To configure software updates download location

1. In the Symantec Management Console, on the Settings menu, click All Settings.
2. In the left pane, expand Software > Patch Management > Core Services.
3. In the right pane, on the Locations tab, specify the software updates download location.
4. Click Save Changes.

If you change the location and you want to relocate existing software update packages, use the Check Software Update Package Integrity task.

The next step is to configure the software updates installation settings.

About Linux kernel patching

The procedure of patching Linux kernel is different from updating any other package. After the installation of files, it also requires a restart into a new kernel to be successful. Most system administrators prefer to install the new kernel without removing the previous version, instead of overwriting the current package.

The Patch Management Solution for Linux can upgrade the version of packages present on managed computers. That removes the option to revert to previous version of the package. Due to this fact, a new kernel can be installed with Software...
Management Solution. Symantec does not recommend you to use Patch Management Solution to update Linux kernel packages. In rare cases it can put managed computer into an unrecoverable state.
Software Management for Linux

This chapter includes the following topics:

- About Software Management Solution
- What you can do with Software Management Solution
- Implementing Software Management Solution
- About the agents and plug-ins that Software Management Solution uses
- Installing or upgrading the Software Management Solution plug-in
- Performing a quick delivery of a single software resource
- About advanced software deliveries
- Delivering multiple software resources and tasks sequentially

About Software Management Solution

Software Management Solution provides intelligent and bandwidth-sensitive distribution and management of software from a central Web console. It significantly reduces desktop visits and lets you easily support your mobile work force.

Software Management Solution also lets 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 part of the Symantec Management Platform. By leveraging this information, Software Management Solution ensures that the correct software gets installed, remains installed, and runs without interference from other software.
This integration lets your administrators focus on delivering the correct software instead of redefining the packages, command lines, and so on for each delivery.

Software Management Solution combines the functionality of earlier versions of Software Delivery Solution and Application Management Solution. It also supports the software virtualization technology that was available in Altiris Software Virtualization Solution.

Software Management Solution data is stored in the Configuration Management Database on the Notification Server computer. The data is grouped in resource data classes. A resource data class defines one or more fields, and the properties of the fields, that a resource of that class may have.

Settings in the Symantec Management Platform determine how long the data is retained in the database before it is purged. You can specify the retention period for specific data classes. These settings are on the Purging Maintenance page, Resource Event Data Purge Settings tab, that appears in the Symantec Management Console.

For UNIX and Linux client computers, the data classes that represent Software Management Solution data are as follows:

- **Computer Events:**
  - AeX SWD Execution
  - AeX SWD Package
  - AeX SWD Status

Software Management Solution supports hierarchy and replication. These features let you create tasks and policies at the top-level Notification Server computer and replicate them to child-level Notification Server computers.

Hierarchy defines the information flows across multiple Notification Server computers in an enterprise. Hierarchy uses replication to copy and synchronize shared objects and data between multiple Notification Server computers within the same hierarchical structure.

Software Management Solution supports full and differential replication. Differential replication replicates only those items that changed since the last replication.

Hierarchy replicates each object or piece of data in one direction only.

Software Management Solution supports hierarchy editable properties (HEP). This feature lets you configure which of the policies' properties can the administrators can change down the hierarchy. By default, all of the hierarchy editable properties (Schedule, Resource targets, and Enabled) are turned off and cannot be modified down the hierarchy. One exception is the Resource targets property in the managed software delivery policies, which is turned on by default. This exception is required for the managed software delivery policies to be published correctly to the Software Portal down the hierarchy.
Software Management Solution supports packages for the Windows, UNIX, Linux, and Mac operating systems. With few exceptions, all the functions in Software Management Solution work the same for all platforms. For example, you use the same method to create a delivery task for a Windows, UNIX, Linux, or Mac OS package.

For a complete list of the platforms that Software Management Solution supports, see the *Server Management Suite Release Notes*.

### What you can do with Software Management Solution

Software Management Solution lets you distribute and manage the software that is used in your organization.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure the default settings</strong> for Managed Software Delivery policies.</td>
<td>Configuration settings control the behavior of Managed Software Delivery policies. Rather than configuring these settings individually for each policy, you can configure the default settings that apply to all new Managed Software Delivery policies. Then you can change the settings for a specific policy only when needed. For more information about configuring the default settings, see the <em>Software Management Solution User Guide</em>.</td>
<td></td>
</tr>
<tr>
<td><strong>Perform an advanced software delivery.</strong></td>
<td>Managed Software Delivery simplifies your advanced software deliveries by letting you deliver software as a unit, which can include multiple software resources and their dependencies. For example, you can create a single Managed Software Delivery policy that installs an application and its associated patches and service packs. Managed Software Delivery can also run any task at any stage of the delivery. For more information about advanced software deliveries and performing an advanced software delivery, see the <em>Software Management Solution User Guide</em>.</td>
<td></td>
</tr>
<tr>
<td><strong>Perform a Quick Delivery of a single software resource.</strong></td>
<td>You can perform a Quick Delivery of a single software resource that runs with minimum configuration. You can use the task-based Quick Delivery method to specify the software to deliver, the action to perform, and the computers to which to deliver. Because the software resources and the delivery settings are predefined, Quick Delivery makes it easy for administrators and non-administrators to deliver software. For more information about Quick Deliveries of a single software resource and about performing a Quick Delivery of a single software resource, see the <em>Software Management Solution User Guide</em>.</td>
<td></td>
</tr>
</tbody>
</table>
Table 8-1  What you can do with Software Management Solution (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliver a package without defining a software resource.</td>
<td>Package Delivery lets you quickly push out any package regardless of whether it is associated with a software resource. For more information about package deliveries and delivering a package without defining a software resource, see the Software Management Solution User Guide.</td>
</tr>
<tr>
<td>Deliver software to fulfill user requests.</td>
<td>By using the Software Portal, users can request and install software through a Web-based interface with little or no administrator involvement. For more information on the Software Portal, see the Software Management Solution User Guide.</td>
</tr>
</tbody>
</table>

Implementing Software Management Solution

Before you use Software Management Solution, you must set it up and prepare it for use.

The prerequisites for implementing Software Management Solution are as follows:

- Symantec Management Platform and Software Management Solution must be installed on the Notification Server computer. For details, see the IT Management Suite Planning for Implementation Guide.
- The Symantec Management Agent must be installed or upgraded on the computers that you plan to manage. Software Management Solution requires that target computers be managed. A managed computer is one on which the Symantec Management Agent is installed. The Symantec Management Agent for UNIX, Linux, and Mac must be installed or upgraded on the non-Windows computers that you plan to manage.
### Table 8-2 Process for implementing Software Management Solution

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1| Install or upgrade the Software Management Solution plug-in on managed computers. | The Software Management Solution plug-in is required for you to deliver and manage software on client computers.  
Perform this step every time that you need to install the Software Management Solution plug-in on the client computers that do not have it.  
The unified *Software Management Solution Plug-in Install* policy lets you install the solution plug-in on all supported operating systems.  
You may have performed this step when you installed the Symantec Management Platform or when you added new computers to the network.  
See “Installing or upgrading the Software Management Solution plug-in” on page 101.  |
| Step 2| Configure security privileges for Software Management Solution.         | Administrators need the appropriate privileges to deliver and manage the software in your organization.  
You or another administrator may have already performed this step when you configured security for the Symantec Management Platform.  
For more information about security privileges, recommended security privileges, and system privileges, see the *Software Management Solution User Guide*.  |
| Step 3| Configure default settings for Managed Software Delivery.               | You can configure the settings that control the behavior of Managed Software Delivery policies. Rather than configuring these settings individually for each policy, you can configure the default settings that apply to all new Managed Software Delivery policies.  
For more information about configuring the default settings for managed software delivery, see the *Software Management Solution User Guide*.  |

### About the agents and plug-ins that Software Management Solution uses

Certain agents and plug-ins must be installed on the client computers to manage and run the Software Management Solution functions.  
Predefined tasks are provided to install these agents and plug-ins.
Table 8-3  Agents and plug-ins that Software Management Solution uses

<table>
<thead>
<tr>
<th>Agent or plug-in</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Management Framework agent</td>
<td>Manages all the software delivery functions in Software Management Solution. Software deliveries are closely integrated with the software resources in the Software Catalog. The Software Management Framework agent manages the package downloads and other aspects of software delivery. The Software Management Framework agent is installed on the client computers when the Symantec Management Agent is installed. For more information, see the topics about the Software Management Framework agent in the <em>Symantec Management Platform Help</em>.</td>
</tr>
</tbody>
</table>
| Software Management Solution Plug-ins   | Although Software Management Solution plug-ins for Mac, UNIX, and Linux-based platforms differ from plug-ins for Windows clients, the policies that manage client-side installation, upgrade, and uninstallation are unified on the console side for all platforms. A unified plug-in means that you enable the same installation, upgrade, or uninstallation policy for managing the Software Management plug-in on all clients. You use the same plug-in for Mac, UNIX, and Linux clients that you use for Windows clients. The software resources that comprise this plug-in are as follows, in alphabetical order:  
  ■ Software Management Plug-in for AIX  
  ■ Software Management Plug-in for HP UX  
  ■ Software Management Plug-in for Linux  
  ■ Software Management Plug-in for Mac  
  ■ Software Management Plug-in for Solaris  
  See “Installing or upgrading the Software Management Solution plug-in” on page 101. |

Installing or upgrading the Software Management Solution plug-in

Before you use Software Management Solution to deliver or manage software on managed computers, you must install the Software Management Solution plug-in on those computers.

If you upgraded from a 7.x version of Software Management Solution, you must upgrade the Software Management Solution plug-in that is installed on the managed computers.

Upgrade from a 6.x version of Software Management Solution plug-in is not supported. You must upgrade the Symantec Management Agent first, and then use the *Software Management Solution Plug-in Install* policy to install the plug-in.
You install the Software Management Solution plug-in to Windows and non-Windows computers using the same installation policy: **Software Management Solution Plug-in Install.**

**To install or upgrade the Software Management Solution plug-in**

1. In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > All Agents/Plug-ins.**
2. In the left pane, expand **Software > Software Management.**
3. Click one of the following policies:
   - **Software Management Solution Plug-in Install**
     - Click if it is a new installation or if you upgraded from the 6.x version of the product.
   - **Software Management Solution Plug-in Upgrade**
     - Click if you upgraded from the 7.x version of the product.
4. Check or uncheck **Enable Verbose Reporting of Status Events** as appropriate.
   - This option records the detailed events that are related to the installation and posts them to the Notification Server computer.
5. Under **Applied to**, select where to install the agent or you can keep the default settings.
6. Under **Schedule**, set the schedule for the policy or you can use the default **Run once ASAP** option to run the policy as soon as possible.
   - Note that if you turn off and then turn on the policy, it cannot run on the same computer again. To run a policy on the same computer again, you must configure it to run on a schedule.
7. (Optional) Under **Extra schedule options**, configure other options.
8. Turn on the policy.
   - At the upper right of the page, click the colored circle and then click On.
9. Click **Save changes**.

See “Implementing Software Management Solution” on page 99.
Performing a quick delivery of a single software resource

You can perform a quick delivery of a single software resource that runs with minimum configuration. You can use the task-based Quick Delivery method to specify the software to deliver, the action to perform, and the computers to deliver to.

Because the software resources and the delivery settings are predefined, Quick Delivery makes it easy for administrators and non-administrators to deliver software. For example, help desk personnel can easily deliver hotfixes because all they have to do is select the correct hotfix from the Software Catalog. They do not need to know which package to select or how to create the command line.

Most organizations can use Quick Delivery for the majority of their software delivery needs. Quick Delivery helps you reduce the amount of time that you spend on routine deliveries so that you can devote more time to advanced activities.

The software that you deliver in this way must be defined as a deliverable software resource in the Software Catalog. It must also have at least one command line.

After the initial instance of a Quick Delivery task runs, you can edit and rerun it. For example, you can deliver the software to different computers or run a different command line on the same computers. You can also edit the delivery settings for the task. For example, you can change the user credentials under which the task runs.

If you need to perform compliance checks or other advanced delivery activities, use Managed Software Delivery instead of Quick Delivery.

See “About advanced software deliveries” on page 110.
Table 8-4  Process for performing a quick delivery of a single software resource

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Create a Quick Delivery task. | The options for creating a Quick Delivery task are as follows:  
  ■ Use the **Quick Delivery** wizard.  
    The **Quick Delivery** wizard let you create and run a Quick Delivery task with minimum configuration.  
    See "Creating a Quick Delivery task with the Quick Delivery wizard" on page 105.  
  ■ Create and configure the task manually.  
    Use this method when you need to configure the default settings of the task or run the task on a specific schedule. You can also configure the task that you created with a wizard.  
    See "Creating a task in Software Management Solution" on page 106. |
| Step 2 | (Optional) Configure the task settings. | Every task inherits the default run settings. You can override the default settings for a particular task.  
  For example, if you want to deliver a large package over slow network, you may want to increase the **End task after** value. |
| Step 3 | Schedule the task and choose the delivery destinations. | When you use the **Quick Delivery** wizard to create the task, you choose the destinations in the wizard. Those destinations apply to that instance of the task only. You do not have to schedule the task because it runs as soon as possible.  
  When you edit the task or create it without the wizard, you define the schedule and the delivery destinations every time you run the task.  
  The options for scheduling the task are as follows:  
  ■ Run the task now.  
    This option runs the task as soon as possible, unless it must wait for a maintenance window.  
  ■ Schedule the task to run at a specific time.  
    See "Scheduling a task and selecting computers in Software Management Solution" on page 107. |
| Step 4 | After the task runs, view the reports. | The Software Management reports let you monitor the software deliveries.  
  The delivery reports provide information about the status of the software downloads and executions. For example, the software downloads for each computer, including the status and the download date.  
  See "Running a Software Management Solution report" on page 108. |
Creating a Quick Delivery task with the Quick Delivery wizard

A Quick Delivery task lets you deliver software without the need to know which package to select or how to create the command line. Creating a Quick Delivery task is the first step in performing a Quick Delivery of a single software resource.

The **Quick Delivery** wizard is the fastest and easiest way to create and run a Quick Delivery task with minimum configuration. During the wizard, you specify the software resource to deliver, the action to perform, and the destinations to deliver to. The resulting Quick Delivery task runs as soon as possible without further configuring or scheduling. We recommend that non-administrators use the **Quick Delivery** wizard because it provides the fewest options and therefore the fewest opportunities for errors.

---

**Warning:** When a Quick Delivery task runs automatically, you can recall, stop, or disable it only if the task needs to wait for a maintenance window.

---

The advantages of using the **Quick Delivery** wizard are as follows:

- It speeds the task creation.
- It does not let non-administrators change the delivery settings.
  - In most cases, it is important to prevent non-administrators from changing the delivery settings when they deliver software.
- It sets the task to run as soon as possible.

When you create a Quick Delivery task without the wizard, it does not run automatically. You must run it or schedule it.

The software that you deliver in this way must be defined as a deliverable software resource in the Software Catalog.

When you run the **Quick Delivery** wizard from the **Software Catalog** view, it populates the most default information. However, you can run the **Quick Delivery** wizard from other areas of the Symantec Management Console. Your point of entry into the **Quick Delivery** wizard determines the amount of default information that is populated.

If you need to change the task’s default settings or run the task on a specific schedule, create the task without the **Quick Delivery** wizard.

**To create a Quick Delivery task with the Quick Delivery wizard**

1. In the Symantec Management Console, on the **Manage** menu, click **Software**.
2. In the left pane, under **Deliverable Software**, click **Software Releases**.
3. In the **Software Releases** pane, right-click a deliverable software resource and then click **Actions > Quick Delivery Task**.
4 In the **Quick Delivery Task** dialog box, specify the following items:

- The software resource to deliver
- The command line to run
  The list contains the names of the command lines that are defined for the software resource.
- Whether to accept the maintenance windows
- The destinations you want to deliver the software resource to

5 Click **OK**.

**Creating a task in Software Management Solution**

Creating a task is typically the first step in performing the software-related actions in Software Management Solution. This procedure describes how to create any type of task in Software Management Solution.

Every task inherits the default settings that control how the task runs. You can override the default settings for a particular task.

Notification Server tasks let you download and run packages, programs, commands, and other items to client computers. You use tasks to perform most of the actions in Software Management Solution.

<table>
<thead>
<tr>
<th>Table 8-5</th>
<th>Types of tasks in Software Management Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of task</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Package Delivery</td>
<td>Lets you deliver any package regardless of whether it is associated with a software resource.</td>
</tr>
<tr>
<td>Quick Delivery</td>
<td>Lets you perform a Quick Delivery of a single software resource. Creating this task is the first step in the Quick Delivery process. The software that you deliver in this way must be defined as a deliverable software resource in the Software Catalog.</td>
</tr>
<tr>
<td>Source Path Update</td>
<td>Lets you update the source paths of Windows Installer applications with the resilient source paths that point to the package servers that you designate.</td>
</tr>
<tr>
<td>Software Virtualization</td>
<td>(Windows only) Lets you manage virtual software layers on managed computers or deliver a VSA or an XPF file to managed computers.</td>
</tr>
</tbody>
</table>
Table 8-5  Types of tasks in Software Management Solution *(continued)*

<table>
<thead>
<tr>
<th>Type of task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Installer Repair</td>
<td>Lets you proactively identify and repair broken Windows Installer applications on selected computers.</td>
</tr>
</tbody>
</table>

To create a task

1. In the Symantec Management Console, on the Manage menu, click Jobs and Tasks.
2. In the left pane, expand System Jobs and Tasks > Software.
3. Right-click the folder under which you want to create a task, and then click New > Task.
4. In the Create new task dialog box, in the left pane, under Software click the type of task that you want to create.

   The type of task that you selected determines the options that appear, as follows:
   - Package Delivery
   - Quick Delivery
   - Software Virtualization Command *(Windows only)*
   - Source Path Update *(Windows only)*
   - Windows Installer Repair

5. In the right pane, configure the task.
6. Click OK.

Scheduling a task and selecting computers in Software Management Solution

Software Management tasks use the task management component of Notification Server that provides flexibility in targeting computers and scheduling tasks. For example, when you schedule tasks, you can configure multiple schedules for an individual task, use maintenance windows, or use shared schedules. When you select computers, you can build and re-use predefined groups of computers.
To schedule a task and to select computers
1. In the Symantec Management Console, on the Manage menu, click Jobs and Tasks.
2. In the left pane, expand System Jobs and Tasks > Software > Quick Delivery.
3. Under the Quick Delivery folder, click on the task you want to schedule.
4. On the task page, click either of the following:
   - **Quick Run**
     Lets you run the task on a single destination as soon as possible, unless it must wait for a maintenance window. This option is not available for some tasks.
   - **New Schedule**
     Lets you schedule the task to run at a specific time. The name of the option depends on the type of task.
     
     To see these options, you might have to click a tab or expand a section on the task page.
5. Select the computers to run the task on.
6. (Optional) To create multiple schedules and computer lists for this task, repeat step 4 through step 5.

Running a Software Management Solution report

You can view reports to get information about the actions that you perform in Software Management Solution.

Predefined reports let you easily view and analyze your Software Management Solution data. The reports are grouped in folders by type in the Symantec Management Console.

You can also create your own custom reports.

By default, all the Software Management Solution reports support resource scoping, which limits the data that users can access based on their security roles.

The Software Management Solution reports use the scoping feature as follows:

- When a user runs a report, the report contains only the data that the user has permissions for.
- When a user saves a snapshot of a report, the snapshot is scoped according to that user's permissions. The users who have a lower security role than the original user cannot view the snapshot. The users who have a higher security role can view the snapshot.
role than the original user can see only the data that the original user was allowed to access.

- You can clone a report and edit the clone’s SQL query to customize how the data is scoped when it is extracted for that report. You can also include scoping information when you create an SQL query for a custom report.
- You can clone a report and edit the clone to select the fields that are scoped when data is extracted from that report’s snapshots.

### Table 8-6 Types of predefined reports in Software Management Solution

<table>
<thead>
<tr>
<th>Report type and folder</th>
<th>Description</th>
</tr>
</thead>
</table>
| **6.0 Legacy Reports** | Contains the reports that appeared in Software Delivery Solution 6.x. This folder does not contain any custom reports that were defined in 6.0.  
The Legacy Reports can contain data from Software Management Solution 7.x as appropriate. They can also contain any data that you might have migrated from Software Delivery Solution 6.x. |
| **Application Management** | Contains the reports that display information about the Windows Installer applications that are broken or that have inaccessible source paths. |
| **Compliance** | Contains the reports that display information about the compliance actions and the remediation actions that Managed Software Delivery performs. |
| **Delivery** | Contains the reports that display information about the status of the software downloads and executions.  
If you migrated software delivery data from Software Delivery Solution 6.x, the new delivery reports contain data from both 6.x and 7.x. |
| **Portal** | Contains the reports that display the status of software requests that are made through the Software Portal. |
| **Virtualized Software Resources** | Contains the reports that display information about the actions (events) that have been performed on the virtual layers that are installed on client computers. |
To run a Software Management Solution report

1. In the Symantec Management Console, on the Reports menu, click All Reports.

2. In the left pane, expand Software, and then expand the folder that contains the report that you want to run.

3. Under the folder that you expanded, click a report.

4. When the report appears in the right pane, you can print the report or save it in a variety of formats. Other actions might be available depending on the type of report.

About advanced software deliveries

Managed Software Delivery simplifies advanced software deliveries by letting you deliver software as a unit, which can include multiple software resources as well as dependencies. For example, you can create a single Managed Software Delivery policy that installs an application and its associated patches and service packs. Managed Software Delivery can also run any task at any stage of the delivery. For example, it can run a task that performs a restart or runs a script.

Managed Software Delivery is a policy-based delivery method that lets you configure advanced delivery settings.

Managed Software Delivery allows you to do the following:

- Intelligently perform the compliance checks and the remediation actions that let you deliver software and manage it.
- Leverage the software resource information and the logic that is in the Software Catalog such as dependencies, packages, and detection rules.
- Save bandwidth by downloading packages only when they are needed. If a client computer does not have the appropriate configuration for the software or if the software is already installed, the package is not downloaded.
- To perform multiple delivery actions with a single policy.

The software that you deliver in this way must be defined as a software resource in the Software Catalog.

If you need to perform a Quick Delivery of a single software resource, use Quick Delivery instead of Managed Software Delivery.
Delivering multiple software resources and tasks sequentially

You can deliver multiple software resources and tasks with a single Managed Software Delivery policy. When Managed Software Delivery evaluates compliance for a group of software, only the software that is out of compliance is downloaded and installed. You can add any client tasks to the execution queue to perform custom operations before, during, or after the software remediation process. A client task is one that is defined in Notification Server and is intended to run on a client computer.

For example, you can create a single Managed Software Delivery policy that performs the following actions:

- Run a task that uses a script to set a registry key on the managed computer.
- Determine whether the software resource or its dependencies are already installed.
- Install the software and any of its dependencies that are not already installed.
- Install an additional software resource into a virtual layer because it is known to conflict with other software that might be on the managed computer.
- Run every week to determine whether the registry key is still correct and the software is still installed.
- Reset the registry key to the correct value if necessary.
- Reinstall any software that the compliance check determines is broken or not present.

The default settings for Managed Software Delivery determine what happens if the policy fails. Initially, this setting is the same for each software resource and task that the policy contains. You can edit the policy to override this setting for each software resource and task. For example, if a critical execution in the sequence fails, you can abort the remaining items in the sequence. Conversely, if a less-critical execution fails, you might decide to run the subsequent tasks anyway.
### Table 8-7

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Create a Managed Software Delivery policy.  | The options for creating a Managed Software Delivery policy are as follows:  
- Use the Managed Software Delivery wizard.  
  The Managed Software Delivery wizard provides a quick way to create and schedule a policy for a single software resource and its dependency software. We recommend that you use the wizard because it can include any dependency software and warn you of software associations automatically.  
  See “Creating a Managed Software Delivery policy with the Managed Software Delivery wizard” on page 113.  
- Create the policy without the wizard.  
  Use this method to create a Managed Software Delivery policy when you need to add multiple software resources and tasks or override the default settings. You also can publish the policy to the Software Portal. However, you must add any dependency software or determine software associations yourself.  
  See “Creating a Managed Software Delivery policy” on page 114.                                                                                           |
| Step 2 | Select the delivery destinations.            | Select the managed computers to deliver to.  
  See “Selecting the delivery destinations for a Managed Software Delivery policy” on page 116.  
  When you use the Managed Software Delivery wizard to create the policy, you select the destinations during the wizard.                                                                                                             |
| Step 3 | Schedule the policy.                        | Define the schedule for the entire policy. You can schedule the compliance check and the remediation separately.  
  When you use the Managed Software Delivery wizard to create the policy, you can define the schedule during the wizard.                                                                                                  |
| Step 4 | Add the additional software resources and tasks to the policy. | You can add multiple software resources and tasks when you create the policy without the Managed Software Delivery wizard. When you use the Managed Software Delivery wizard to create the policy, you can select only one software resource. Edit the policy to add software and tasks. |
| Step 5 | Arrange the sequence in which the software resources and tasks are run. | Move the software resources and tasks up or down in the list to rearrange their order. Plan the sequence before you enable the policy.                                                                                                                                                  |
Table 8-7 Process for delivering multiple software resources and tasks

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>(Optional) Change the settings for individual software resources or tasks.</td>
<td>When you add software resources and tasks to a Managed Software Delivery policy, they inherit the settings from the policy. You can change the settings for any specific software resource or task that is in the policy. The settings that you can change for a specific software resource or task include the remediation schedule, the download settings, and the run settings.</td>
</tr>
</tbody>
</table>

Creating a Managed Software Delivery policy with the Managed Software Delivery wizard

You can perform one or more advanced software delivery actions with a single Managed Software Delivery policy. Creating a Managed Software Delivery policy is the first step in performing an advanced software delivery.

See “About advanced software deliveries” on page 110.

The Managed Software Delivery wizard provides a quick way to create and schedule a policy for a single software resource and its dependency software. We recommend that you use the wizard because it can include any dependency software and warn you of software associations.

When you create a Managed Software Delivery policy with the Managed Software Delivery wizard, the policy is enabled automatically. If you do not want the policy to be available to managed computers immediately, edit the policy, and disable it. You also might edit the policy to add information about what to deliver.

The software that you deliver in this way must be defined as a software resource in the Software Catalog. If the software resource is not defined, contact an administrator who can edit the Software Catalog.

You can run the Managed Software Delivery wizard from the Manage > Software view or from other areas of the Symantec Management Console. Your point of entry into the Managed Software Delivery wizard determines the amount of default information that is populated.

Create the policy without the wizard if you need to perform any of the following tasks:

- Add multiple software resources and tasks.
- Override the default settings.
(Windows and Mac OS only) Add the policy to the Software Portal.

See “Creating a Managed Software Delivery policy” on page 114.

To create a Managed Software Delivery policy with the Managed Software Delivery wizard

1. In the Symantec Management Console, on the Manage menu, click Software.
2. In the left pane, under Deliverable Software, click Software Releases.
3. Right-click a software resource and then click Actions > Managed Software Delivery.
   
   If the Managed Software Delivery option is not available, the software resource does not have a package associated with it and cannot be delivered. Click Actions > Edit Software Resource and configure the software resource.
4. In the Managed Software Delivery wizard, on the Select software page, specify the software to deliver and other delivery options and then click Next.
5. On the Select destinations page, specify the destinations to deliver the software to and then click Next.
   
   See “Selecting the delivery destinations for a Managed Software Delivery policy” on page 116.
6. On the Schedule delivery page, define the schedule for running the Managed Software Delivery and then click Next.
7. (Optional) On the Specify dependencies and updates page, select any dependencies, updates, or service packs that are defined for this software resource and then click Next.
   
   Dependencies: Check Verify dependencies and select the check box for each dependency to include.
   
   Updates or service packs: Select the check box for each update or each service pack to include.
8. To complete the wizard, click Deliver Software.

Creating a Managed Software Delivery policy

A single Managed Software Delivery policy lets you perform one or more advanced software delivery actions. Creating a Managed Software Delivery policy is the first step in performing an advanced software delivery.

See “About advanced software deliveries” on page 110.
When you create a Managed Software Delivery policy, you can add multiple software resources and tasks or override the default settings. You also can publish the policy to the Software Portal for Windows and Mac client computers.

The software that you deliver in this way must be defined as a software resource in the Software Catalog. If the software resource is not defined, contact an administrator who can edit the Software Catalog.

If you need to quickly create and schedule a Managed Software Delivery policy, use the Managed Software Delivery wizard instead.

See “Creating a Managed Software Delivery policy with the Managed Software Delivery wizard” on page 113.

To create a Managed Software Delivery policy

1. In the Symantec Management Console, on the Manage menu, click Policies.
2. In the left pane, under Policies, expand Software > Managed Software Delivery.
3. In the left pane, right-click the Managed Software Delivery folder, and then click New > Managed Software Delivery.
4. In the right pane, click and type over the following text:
   - New Managed Software Delivery: Type a name to identify this policy in any list of policies. Make the name descriptive enough for others to easily identify this policy and the software that it delivers or manages.
   - Add description: Type a description to provide further information about this policy. Do not include critical information in the description because it is not intended to appear in all the lists that contain the name.
5. Under Policy Rules/Actions, on the Software tab, click Add. On the Add menu, select one of the following options:
   - Software
     - Lets you select from the deliverable software resources that are defined in the Software Catalog.
   - Task
     - Lets you select from the client tasks that are defined in Notification Server.
6. Repeat step 5 for each software resource and task that you want to add.
7. (Optional) To change the default settings for this policy, under Policy Rules/Actions, enter additional settings on the Policy settings tab and the Software Publishing tab.
8 (Optional) To change the default settings for a specific software resource or task, under Policy Rules/Actions, click the software resource or task. At the right of the page, do any of the following:

- Change any of the options that are available on the page.
- In a software resource, click Advanced options to display and change additional settings.
- In a task, click Show Task to display and change additional settings.

9 Expand the Applied to section to add or change the delivery destinations. See “Selecting the delivery destinations for a Managed Software Delivery policy” on page 116.

10 Expand the Schedule section to define the delivery schedule.

11 Turn on the policy.

   At the upper right of the page, click the colored circle and then click On.

12 At the bottom of the page, click Save changes.

Selecting the delivery destinations for a Managed Software Delivery policy

You can apply a Managed Software Delivery policy to selected resource targets, computers, users, and resources. You can use any combination of these options to define the computers to which the policy applies.

Managed Software Delivery supports user-based policies by letting you specify users and user groups as policy targets. This feature lets you deliver software to any managed computer that a specific user logs on to. When the user logs on to a computer, the Symantec Management Agent refreshes any policy that targets that user. The policy runs on that computer according to the schedule that you defined for it.

See “Creating a Managed Software Delivery policy with the Managed Software Delivery wizard” on page 113.

See “Creating a Managed Software Delivery policy” on page 114.

To select the delivery destinations for a Managed Software Delivery policy

1 In the Symantec Management Console, on the Manage menu, click Policies.

2 In the left pane, under Policies, expand Software > Managed Software Delivery.

3 In the right pane, click a Managed Software Delivery policy.
4 On the policy page, expand the **Applied to** section to add or change the delivery destinations.

5 On the policy page, turn on the policy or turn off the policy as needed.
At the upper right of the page, click the colored circle and then click **On** or **Off**.

6 When you finish editing the Managed Software Delivery policy, click **Save changes**.
Virtualization Management

This chapter includes the following topics:

■ About Virtual Machine Management on UNIX and Linux systems
■ About server virtualization
■ Permissions that Virtual Machine Management requires
■ Getting started with the Virtual Machine Management component
■ Creating a virtual environment
■ Best practices to prevent protocol replacement
■ Deployment of ESX or ESXi servers
■ Tables populated during the Network Discovery and Run Inventory tasks
■ About Log Viewer

About Virtual Machine Management on UNIX and Linux systems

Virtual Machine Management is included in Altiris Server Management Suite from Symantec and should already be installed and deployed on your network. Virtual Machine Management lets you perform the virtualization process on your network. Virtualization is a technology that lets you make optimum use of the hardware resources of your organization. You can create various virtual server environments on a single physical server. Each virtual environment is isolated and functions independently from the physical server and from the other virtual environments.

Virtualization enhances the efficiency and productivity of the hardware resources and helps to reduce administrative costs.
The features of the Virtual Machine Management component let you get information from your virtualization infrastructure and bring it to your Server Management Suite environment. From there, this information can be consumed in the context of the broader systems management landscape. The pervasiveness of virtualization has made this a necessity as it becomes increasingly impractical to properly manage a server environment without intimate knowledge of the virtualization stack that is present and the ability to access key virtualization operations. The following three scenarios illustrate this critical need:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host/VM ratio</td>
<td>Performing a traditional management operation, such as patch and virus scans on highly dense VM environments, produces unacceptable performance degradation. Using the knowledge of host/guest relationship in systems management policies enables intelligent, no-impact maintenance to be performed on those environments.</td>
</tr>
<tr>
<td>VM cloning</td>
<td>The bare-metal portion of server builds has been replaced by VM provisioning. Administrators need access to VM creation and cloning capabilities from within their systems management console to preserve their fine-tuned and highly customized automated build processes. A complete set of VM management options enables them to find the right balance between VM template proliferation and server build customization needs.</td>
</tr>
<tr>
<td>Host/VM resource consumption</td>
<td>Overall system performance is exponentially more sensitive to resource utilization in virtual environments. To aggravate matters, the hosting of increasing numbers of VMs on a single physical server means that glitches to a single operating environment can disrupt thousands of users. Having access in the systems management console for information on key virtualization performance indicators enables systems administrators to take a holistic approach to preventing and remediating critical system conditions.</td>
</tr>
</tbody>
</table>

Virtual Machine Management supports several guest operating systems. The Hyper-V Integration Services and VMware Tools are available for many of these
guest operating systems. The **Shut Down** and **Restart** tasks are supported in the guest operating systems that support Hyper-V Integration Services and VMware Tools.

Virtual Machine Management does not have any UNIX/Linux-specific functionality. However, you can leverage the same tasks that you complete on Windows guest operating systems on UNIX and Linux systems. Creating and managing virtual machines (including inventory, discovery, and patching) functionality with Virtual Machine Management is the same, no matter what the operating system of the virtual machine.

### About server virtualization

Server virtualization lets you divide a single physical server into multiple virtual environments. The virtual machines share the hardware resources of the physical server. The physical server is called the host and the virtual machine is called the guest.

The virtual machines behave like physical computers. Virtual machine shares the hardware resources of the host server. Each virtual machine also is independent and unaware of the other virtual machines that run on the same physical server.

In Virtual Machine Management, Hypervisor serves as a platform for the operating system of the virtual server. Currently, Virtual Machine Management supports the following Hypervisors:

- Hyper-V
- VMware

These platforms support the virtualization features, which are provided in the Virtual Machine Management component.

Virtual Machine Management component currently supports the following Hyper-V Hypervisors:

- Hyper-V (Win 2K8 R2 enterprise)
- Hyper-V (Win 2K8 R2 SP1)
- Hyper-V (Windows Server 2012)
- Hyper-V (Windows Server 2012 R2)

Virtual Machine Management component also supports VMware vCenter to centrally administer multiple ESX or ESXi hosts and virtual machines in a complex virtual environment. vCenter lets you manage virtual machines on ESX servers, which are discovered using vCenter credentials or managed by vCenter. vCenter lets you
streamline all the virtual machine management tasks to have a better control over the virtual environment.

If ESX servers are managed and discovered through a vCenter then you can perform all the virtual machine management tasks except the **Create Virtual Disk** and **Delete Virtual Disk**. In case of the **Create Virtual Disk** and **Delete Virtual Disk** tasks, the credentials (user name and password) for vCenter and ESX server must be same for the successful execution of the task.

Virtual Machine Management component currently supports the following vCenter versions:

- vCenter 4.0
- vCenter 4.1
- vCenter 5.0
- vCenter 5.1
- vCenter 5.5

These vCenters can be used to manage ESX 4.0, ESX 4.1, ESXi 4.0, ESXi 4.1, ESXi 5.0, and ESXi 5.1, ESXi 5.5.

**Permissions that Virtual Machine Management requires**

For executing different VMM tasks an account or group needs to be given required permissions. You need to perform discovery tasks on a host or vCenter, and run inventory on hosts before you execute different VMM management tasks. Credentials used in the discovery tasks are used to execute various VMM tasks.

**Executing VMM tasks on VMware Hypervisor (ESX/ESXi Host)**

vCenter server or ESX/ESXi host gives access to the user based on the permissions given to him. When user discovers an ESX/ESXi host directly then permissions given on a host are used for VMM tasks execution, but if user discovers a host using vCenter then permissions given to him on vCenter are used for VMM task execution. Various permissions can be given to a user or group using the vSphere client. User permissions defined on an object take precedence over group permissions. If no user permissions are given then the user is given union of privileges given to the groups, to which user belongs for that object.

For detailed information about this please refer to Managing Users, Groups, Roles, and Permissions topic of the *vSphere Basic System Administration manual.*
You can directly discover a host using host credentials and execute different VMM tasks on it. Authorized users/groups on ESX/ESXi host are directly added to the list and given permissions when ESX/ESXi is installed. An administrator can add different users using User & Groups tab on vSphere client and give him required permission using the Permissions tab. By default, root user has administrative privileges. The vpxuser user is created with administrative privileges when a host is attached to a vCenter.

Table 9-1 Permissions required for executing VMM tasks on an ESX/ESXi host discovered directly

<table>
<thead>
<tr>
<th>VMM task</th>
<th>Read-only</th>
<th>Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Run Inventory</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Create/Delete VM</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Create/Delete Disk</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Create/Delete Network</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Deploy VM (from template)*</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Create/Revert/ Delete Snapshot</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Power Mgmt. (Start, Stop, Suspend, Resume, Shutdown, Restart)</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

**Note:** The Deploy VM task is supported only on those ESX hosts, which are discovered using vCenter credentials.

You can discover a vCenter and execute VMM tasks on the hosts managed by the vCenter. After discovery, only the hosts for which you have access rights are listed. vCenter uses Windows mechanism for authentication and authorization. An Administrator can give permissions to a domain user or local windows user/group on vCenter to access vCenter infrastructure. Permissions Tab in vSphere client can be used to give necessary permission to a user/group.
Table 9-2 Permissions required for Executing VMM tasks on an ESX/ESXi host discovered using vCenter credentials/managed by vCenter:

<table>
<thead>
<tr>
<th>VMM task</th>
<th>Read-only</th>
<th>Administrator</th>
<th>Power user</th>
<th>VM user</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Run Inventory</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Create/Delete VM</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create/Delete Disk</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create/Delete Network</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deploy VM (from template)</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create/Revert/ Delete Snapshot</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power Mgmt. (Start, Stop, Suspend, Resume, Shutdown, Restart)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

These are some default roles available to user. But user does have option to assign other default roles like Resource pool administrator, VMware consolidated backup user, Datastore consumer etc. Also user can create custom roles depending upon need.

**Note**: Because of current VMware API limitations, the Delete Disk and Create Disks tasks can only be executed using ESX server admin credentials. If your vCenter admin credentials are different than your ESX admin credentials, then you must discover your ESX server directly using its admin credentials to perform the Delete Disk and Create Disk tasks.

**Executing VMM tasks on Hyper-V**

Hyper-V uses Windows authentication mechanism. A domain user or a local user on windows with administrative privileges to the HyperV server is required to execute VMM tasks.
Table 9-3  Permissions required for Executing VMM tasks on Hyper-V permissions

<table>
<thead>
<tr>
<th>VMM task</th>
<th>Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery</td>
<td>x</td>
</tr>
<tr>
<td>Run Inventory</td>
<td>x</td>
</tr>
<tr>
<td>Create/Delete VM</td>
<td>x</td>
</tr>
<tr>
<td>Create/Delete Disk</td>
<td>x</td>
</tr>
<tr>
<td>Create/Delete Network</td>
<td>x</td>
</tr>
<tr>
<td>Deploy VM (from template)*</td>
<td>N/A</td>
</tr>
<tr>
<td>Create/Revert/ Delete Snapshot</td>
<td>x</td>
</tr>
<tr>
<td>Power Mgmt. (Start, Stop, Suspend, Resume, Shutdown, Restart)</td>
<td>x</td>
</tr>
</tbody>
</table>

Note: Hyper-V hypervisor does not support the Deploy VM task.

Getting started with the Virtual Machine Management component

The Virtual Machine Management component lets you manage your virtual environment. To start to use Virtual Machine Management features, Symantec recommends you to use the following workflow:

Table 9-4  Process for getting started with the Virtual Machine Management component

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Install the Virtual Machine Management Plug-in</td>
<td>You can install the Virtual Machine Management Plug-in on a separate task server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Installing the Virtual Machine Management Task Server Plug-in” on page 125.</td>
</tr>
</tbody>
</table>
### Table 9-4 Process for getting started with the Virtual Machine Management component (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Discover and add hosts</td>
<td>You can specify IP address of a single host and quickly add it to the network.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Discovering and adding a single vCenter or host” on page 126.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can discover all the hosts and their virtual machines that are available in the network. The discovery data is added into the Configuration Management Database (CMDB).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Discovering and adding multiple vCenter or hosts” on page 127.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Collect the inventory on the hosts</td>
<td>After you discover the Hyper-V and VMware servers on your network, you can gather inventory of these servers and their virtual environments.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Gathering inventory on the host” on page 128.</td>
</tr>
<tr>
<td>Step 4</td>
<td>View Virtual Machine Management reports</td>
<td>You can review the inventory reports gathered on the hosts.</td>
</tr>
</tbody>
</table>

For more information about managing your virtual environment, see the Virtual Machine Management User Guide.

See “About Virtual Machine Management on UNIX and Linux systems” on page 118.

### Installing the Virtual Machine Management Task Server Plug-in

To perform any Virtual Machine Management tasks, you must install the Virtual Machine Management Task Server Plug-in on your task server.

The Virtual Machine Management Task Server Plug-in install policy is enabled by default. The Virtual Machine Management Task Server Plug-in install policy is roll out automatically only on the Notification Server computer on which the task service installed; the plug-in policy does not automatically roll-out on all the task servers. If you want to roll out the VMM plug-in install policy on a remote task server then you need to select respective targets in install policy and run that. The policy installs the Virtual Machine Management Task Server Plug-in on your task server.
To install the Virtual Machine Management Task Server Plug-in

1. In the Symantec Management Console, on the Settings menu, click All Settings.

2. In the left pane, under Settings, click Agents/Plug-ins > Virtual Machine Management > Virtual Machine Management Task Server Plug-in - Install.


4. Under Schedule, specify a schedule for the policy.

5. Turn on the policy.
   At the upper right of the page, click the colored circle, and then click On.

6. Click Save changes.

Discovering and adding a single vCenter or host

The Add Host feature lets you find and add a specific host or vCenter to your network by only specifying its IP address. In this case, the network discovery task is run internally.

For better network discovery results, it is recommended to assign unique name and IP address to the virtual machines and templates, which are associated with the same Host.

The discovery task uses the default connection profile to discover the host or vCenter. So, before you discover and add a host or vCenter, ensure that the vCenter or Host credential is present and enabled for the respective protocol (WMI protocol for Hyper-V servers, and VMware protocol for ESX servers) in the default connection profile. When the host or vCenter is found, its data is added to the Configuration Management Database (CMDB). Discovery ensures the right protocol and credential associations are made for future inventory operations.

See “Best practices to prevent protocol replacement” on page 141.

After a host or vCenter is added, you can view its data on the Virtual Machine Management home page. You can also run the Virtual Machine Management tasks on the host.

To discover and add a single host

1. In the Symantec Management Console, on the Home menu, click Virtual Machine Management.

2. In the left pane, click Actions > Add Host.

3. In the dialog box, type the IP address of the host or vCenter and click OK.
Discovering and adding multiple vCenter or hosts

Before you can perform the Virtual Machine Management operations, you must discover the hosts or vCenters and associated virtual machines, and then gather inventory on each of the hosts.

For better network discovery results, it is recommended to assign unique names and IP addresses to the virtual machines and templates, which are associated with the same Host.

You can discover the virtual machines separately with the Network Discovery wizard on Home > Discovery and Inventory > Network Discovery or from Manage > Jobs and Tasks > Discovery and Inventory, but for VMM to work properly you must discover VMs using a host or vCenter credentials. Discovery ensures the right protocol and credential associations are made for future inventory operations.

For more information about discovering and adding multiple vCenter or hosts, see the following video in Symantec Connect:

Configuring VMM to Discover a vCenter or ESX Server Video

For more information about discovering and adding multiple Hyper-V hosts, see the following video in Symantec Connect:

Configuring VMM Solution to Discover a Hyper-V Server Video

After the hosts and their virtual machines are discovered, accordingly corresponding resources are created in the Configuration Management Database (CMDB). The Virtual Machine Management home page displays the hosts and their virtual machines that are available on your network.

Each time you add a host, vCenter or a virtual machine, you must launch the network discovery wizard to update the discovery data. You can also set up a recurring Network Discovery task by using a custom connection profile. You can choose Discover Virtual managers VMware and HyperV to target the new hosts, vCenters, and virtual machines in your environment.

See “About Network Discovery” on page 35.

To discover the hosts

1. In the Symantec Management Console, on the Home menu, click Virtual Machine Management.

2. In the left pane, click Actions > Getting Started.

3. In the Getting Started dialog box, click Launch Network Discovery Wizard.
4 In the network discovery wizard, on the **Choose method of device discovery** page, specify a discovery method and then click **Next**.

5 On the **Enter network IP Ranges** page, specify the portions of the network to discover and then click **Next**.

6 On the **Select device communication profile** page, select a connection profile.

7 To specify the VMware or WMI credentials, click the **Edit** symbol.

   The credentials that you specify, are automatically used for all other tasks that require credentials.

   Make sure that the VMware protocol is always turned on for vCenter and ESX servers, and WMI protocol is turned on for Hyper-V servers.

8 In the **Define Group Settings** dialog box, click **OK**.

9 Click **Next**.

10 On the **Enter task name** page, name the task and then click **Next**.

11 On the **Choose when to run the discovery** page, schedule the task and then click **Finish**.

   See “Best practices to prevent protocol replacement” on page 141.

   See “Permissions that Virtual Machine Management requires” on page 121.

### Gathering inventory on the host

After you discover the VMware vCenter, ESX server and Hyper-V servers on your network, you can gather inventory on these servers. Even though the discovery has been done on a vCenter, the inventory must be explicitly gathered on an ESX server.

To gather inventory on the hosts, you must run a Virtual Machine Management Inventory task. The inventory task lets you collect the data about a host and its virtual environment.

For example you can collect information about the host name, IP address, system type, and hardware utilization. You can also collect information about the virtual machines, virtual disks, and the virtual networks that are created on the host.

For more information about running VMM inventory, see the following video in Symantec Connect:

**Running Virtual Machine Management Inventory Video**

The **Run Inventory** task is a host level task and can only be executed against a host. On executing an inventory task on a host, all the information about the virtual machines that are associated with the host, is automatically collected. You do not
require to run the inventory tasks on the virtual machines as there is no separate inventory task for the virtual machines. If you have performed the Network Discovery task using vCenter credentials then you must execute separate inventory task on the host.

For example, if applying the Network Discovery task to a specific vCenter returns 10 associated ESX servers, then you must execute separate inventory task on each host to get the full information on the environments.

If the inventory is not gathered on a host then except the Run Inventory task, you are not allowed to perform any other host level or guest level tasks such as Create Virtual Machine, Create Virtual Disk, Start, Stop, etc. as these tasks are unaccessible from the Virtual Machine Management portal page and through all other access paths like Actions > Virtual Machine Management > Create VM (List of Hosts), Manage > Jobs and Tasks, or Manage > All Resources > Asset > Network Resource > Computer. In these scenarios, you must first execute the Run Inventory task on the host and then perform other host level and guest level tasks using the options available on different pages.

You can run the inventory task once or you can set it to run repeatedly and automatically update the inventory data. In Virtual Machine Management, there is a preconfigured inventory task called VMM inventory. It is scheduled by default to run at 6:30 P.M. daily on all hypervisors. You can edit or delete the preconfigured inventory task instance. If you want, you can create multiple new instances of the default inventory task through the New Schedule option that is provided on the inventory task page, and have different scheduled inventory run on single or multiple hypervisors.

To gather inventory on the host

1. In the Symantec Management Console, on the Home menu, click Virtual Machine Management.

2. In the left pane, do one of the following:
   - Click Actions > Getting Started and in the Getting Started window, click Run Inventory Task.
   - Click the host, go to the host page on the right pane, under Actions, click Run Inventory.
   - Right-click the host and click Run Inventory. All the discovered hosts are displayed in the left pane.

   The above option can also be accessed on right-click of the host from Manage > All Resources > Asset > Network Resource > Computer.

3. On the inventory task page, under Task Status, specify a schedule for the task.
To manually create a Virtual Machine Management Inventory task

1. In the Symantec Management Console page, on the Manage menu, click Jobs and Tasks.

2. In the left pane, under Jobs and Tasks, expand System Jobs and Tasks, and click Virtual Machine Management.

3. Right-click the Inventory folder and click New > Task.

4. In the tasks list, click Inventory.

5. On the inventory task page, give the task a name.

6. On the inventory task page, under Task Status, specify a schedule for the task.

7. If you make changes in the task after you have created it, click Save changes.

Creating a virtual environment

The virtualization process helps you optimally use the resources and application of your organization. Each virtual machine has its own virtual processor, memory, hard disk, and network interface card. You can use the Virtual Machine Management Solution to design and create your virtual environment. For that task, Symantec recommends that you use the following workflow:

Table 9-5 Process for creating a virtual environment

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create a virtual network</td>
<td>Create a virtual network that lets you connect the virtual machines to the host and the network for accessing other computers and the Internet. See “Creating a virtual network on a host” on page 139.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Create a virtual disk</td>
<td>Create a virtual hard disk that you can use to store data from virtual machine. See “Creating a virtual disk on a host” on page 138.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create a virtual machine</td>
<td>Create a virtual machine on a specific host. See “Creating a virtual machine on a host” on page 131.</td>
</tr>
</tbody>
</table>
Table 9-5 Process for creating a virtual environment (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>Start a virtual machine</td>
<td>Start a virtual machine and its operating system.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Create a snapshot</td>
<td>Create a snapshot of the virtual machine at any given time. You can later use the snapshot to restore the virtual machine to previous configuration. See “Creating a snapshot” on page 140.</td>
</tr>
</tbody>
</table>

For more information on both the host and the guest level tasks that you can perform with Virtual Machine Management Solution, see the [Virtual Machine Management User Guide](#).

Creating a virtual machine on a host

Virtual machines are created on a host. You can create the virtual machine with the **Create Virtual Machine** wizard. You can also manually create a task that creates a virtual machine. When you create a virtual machine using a task that is created manually from **Jobs and Tasks**, the virtual network that is associated with the virtual machine can only be of type internal.

You must configure the Deployment Solution job and enable the PXE service to send an automation image to all unknown computers before you provision a virtual machine. This step is optional and required only if you want to deploy an operating system on the virtual machine.

For more information about configuring a Deployment Solution job, setting up the PXE service and creating images, see the *Deployment Solution User Guide* or see the following video in Symantec Connect:

**Creating a Virtual Machine using Existing Deployment Solution Job in VMM Solution Video**

Things you should consider before you create a virtual machine and use the OS deployment functionality with the **Create Virtual Machine** wizard:

- Select only the Deployment Solution job that contains the Partition task and Scripted OS installation task.
- Initial Deployment task of the Deployment Solution should not be enabled.
- When you select a network, make sure that it is external only.
To create a virtual machine and use the OS deployment functionality with the Create Virtual Machine wizard

1. In the Symantec Management Console, do one of the following:
   - From the **Actions** menu, select **Virtual Machine Management > Create VM**, and execute steps 3 to 9.
   - From the **Home** menu, click **Virtual Machine Management**, and execute steps 2 to 9.

2. In the left pane, do one of the following:
   - Click the host, go to the host page on the right pane, under **Actions**, click **Create Virtual Machine**.
   - Right-click the host and click **Create VM**.
     The above option can also be accessed on right-click of the host from **All Resources > Asset > Network Resource > Computer**.

3. In the **Create Virtual Machine** wizard, on the **Select Host** page, select the host from the list and then click **Next**. The **Select Host** page is displayed only if you are accessing **Create Virtual Machine** wizard from the **Actions** menu.
4 On the **Virtual Machine Details** page, specify the following virtual machine details and then click **Next**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Lets you specify a name for the virtual machine.</td>
</tr>
<tr>
<td>Description</td>
<td>Lets you specify a description about the virtual machine.</td>
</tr>
<tr>
<td>Guest OS</td>
<td>Lets you select a guest operating system.</td>
</tr>
<tr>
<td>OS version</td>
<td>Lets you select the appropriate version of the guest operating system. Ensure that you have chosen a correct guest operating system from the available <strong>OS version</strong> list and your host supports the guest operating system that you have selected. You can refer to VMware and Microsoft Hyper-V guest OS list for more information about the supported guest OS.</td>
</tr>
<tr>
<td>CPUs</td>
<td>Lets you select or specify the number of CPUs for the virtual machine. The number of CPUs you select depends on the number of logical processors on the host server. The maximum number of logical processors for the ESX server is 8, for the Hyper-V 2008 is 4, and for the Hyper-V 2012 is 8.</td>
</tr>
<tr>
<td>ISO path</td>
<td>Lets you select or specify the ISO path. This path is used for installing the guest operating system on the virtual machine. While creating a VM with the Deployment Solution job, it is recommended to leave this field blank.</td>
</tr>
<tr>
<td>Memory</td>
<td>Lets you specify the memory for the virtual machine in GB or MB.</td>
</tr>
</tbody>
</table>

5 On the **Select Disk** page, create a new disk or select an existing virtual disk, and then click **Next**.

6 On the **Select Network** page, do one of the following:
Select **New** to create a new virtual network for the virtual machine. Now, you can enter a **Name** for the new virtual network and select an **Adapter** to which the network is connected.

Select **Existing network** to use an existing network for creating the virtual machine. In case of VMware hypervisor, the existing network list includes 'Standard' or 'Virtual' switches. It also includes the 'Distributed switch port groups' networks, which are created through vSphere client; not from VMM solution. Currently, only the existing ‘Distributed switch port groups’ is supported.

In case of ESX hypervisors, while creating an internal or external network, the network name must be unique, whereas if you are using Hyper-V hypervisors, the network name can be duplicate.

7 Click **Next**.

8 On the **Select Datastore and Deployment Job** page, select a datastore and a deployment solution job.

9 Click **Finish**.

After you finish the wizard, a job is created. This job contains a task that creates a virtual machine and one task that schedules an operating system deployment job on it.

To create a virtual machine with the Create Virtual Machine wizard

1 In the Symantec Management Console, do one of the following:

   - From the **Actions** menu, select **Virtual Machine Management > Create VM**, and execute steps 3 to 8.
   - From the **Home** menu, click **Virtual Machine Management**, and execute steps 2 to 8.

2 In the left pane, do one of the following:

   - Click the host, go to the host page on the right pane, under **Actions**, click **Create Virtual Machine**.
   - Right-click the host and click **Create VM**.
     The above option can also be accessed on right click of the host from **All Resources > Asset > Network Resource > Computer**.

3 In the **Create Virtual Machine** wizard, on the **Select Host** page, select the host from the list and then click **Next**. The **Select Host** page is displayed only if you are accessing **Create Virtual Machine** wizard from the **Actions** menu.

4 On the **Virtual Machine Details** page, specify the following virtual machine details and then click **Next**:
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Lets you specify a name for the virtual machine.</td>
</tr>
<tr>
<td>Description</td>
<td>Lets you specify a description about the virtual machine.</td>
</tr>
<tr>
<td>Guest OS</td>
<td>Lets you select a guest operating system.</td>
</tr>
<tr>
<td>OS version</td>
<td>Lets you select the appropriate version of the guest operating system. Ensure that you have chosen a correct guest operating system from the available OS version list and your host supports the guest operating system that you have selected. You can refer to VMware and Microsoft Hyper-V guest OS list for more information about the supported guest OS.</td>
</tr>
<tr>
<td>CPUs</td>
<td>Lets you select or specify the number of CPUs for the virtual machine. The number of CPUs you select depends on the number of logical processors on the host server. The maximum number of logical processors for the ESX server is 8, for the Hyper-V 2008 is 4, and for the Hyper-V 2012 is 8.</td>
</tr>
</tbody>
</table>
ISO path

Lets you select or specify the ISO path. This path is used for installing the guest operating system on the virtual machine. For a specific host, the ISO paths are available for selection only if they are under the parent folder or a root folder of the host. In case of Hyper-V ISO files, the ISO paths are available for selection only in following scenarios:

- ISO files are located under default Hyper-V disk path where .vhd files get saved.
- ISO files, which are referred or used by existing VMs irrespective of file path location.

If ISO files are not available for selection then you can specify the path manually.

Memory

Lets you specify the memory for the virtual machine in GB or MB.

5 On the Select Disk page, create a new disk or select a virtual disk and then click Next.

6 On the Select Network page, create or select a virtual network, and then click Next.

7 On the Select Datastore and Deployment Job page, select a datastore.

8 Click Finish.

After you finish the wizard, a task is created. This task creates a virtual machine with the specified configuration.

To manually create a task that creates a virtual machine

1 In the Symantec Management Console page, on the Manage menu, click Jobs and Tasks.

2 In the left pane, under Jobs and Tasks, expand System Jobs and Tasks, and click Virtual Machine Management.

3 Right-click the Create Virtual Machine folder and click New > Task.

4 In the tasks list, click Create Virtual Machine.

5 Give the task a name.
6 On the **VM Details** tab, specify the following virtual machine details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Lets you specify a name for the virtual machine.</td>
</tr>
<tr>
<td>Description</td>
<td>Lets you specify a description about the virtual machine.</td>
</tr>
<tr>
<td>Guest OS</td>
<td>Lets you select a guest operating system.</td>
</tr>
<tr>
<td>OS version</td>
<td>Lets you select the appropriate version of the guest operating system.</td>
</tr>
<tr>
<td>Memory</td>
<td>Lets you specify the memory for the virtual machine in MB.</td>
</tr>
<tr>
<td>CPUs</td>
<td>Lets you specify the number of CPUs for the virtual machine.</td>
</tr>
</tbody>
</table>

   - Ensure that you have chosen a correct guest operating system from the available OS version list and your host supports the guest operating system that you have selected.
   - You can refer to VMware and Microsoft Hyper-V guest OS list for more information about the supported guest OS.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>Lets you specify the memory for the virtual machine in MB.</td>
</tr>
<tr>
<td>CPUs</td>
<td>Lets you specify the number of CPUs for the virtual machine.</td>
</tr>
</tbody>
</table>

   - The number of CPUs depend on the number of logical processors on the host server.
   - The maximum number of logical processors for the ESX server is 8, for the Hyper-V 2008 is 4, and for the Hyper-V 2012 is 8.

7 On the **Disk Details** tab, specify the disk details.

8 On the **Network Details** tab, specify the network details.

   - Here, the virtual network is created of type internal.

9 Click **OK**.

10 On the create virtual machine task page, under **Task Status**, specify a schedule for the task.

11 If you make changes in the task after you have created it, click **Save changes**.
Creating a virtual disk on a host

While creating a virtual machine, you need to create or specify a virtual disk for it. The virtual disk is created on a host.

Note: VMware vCenter lets you manage and discover multiple hosts. In this case, for the successful creation of a virtual disk, the credentials for the host and the respective vCenter must be the same.

To create a virtual disk

1. In the Symantec Management Console, on the Home menu, click Virtual Machine Management.

2. In the left pane, do one of the following:
   - Click the host, go to the host page on the right pane, under Actions, click Create Virtual Disk.
   - Right-click the host, and click Create Disk.
   
   The above option can also be accessed on right-click of the host from All Resources > Asset > Network Resource > Computer.

3. In the Create Disk dialog box, specify the following disk settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>Lets you specify a name for the virtual disk.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Lets you specify a description about the Virtual disk.</td>
</tr>
<tr>
<td>Capacity</td>
<td>Lets you specify the size of the virtual disk in GB or MB.</td>
</tr>
<tr>
<td>Datastore</td>
<td>Lets you select a datastore on which you want to create the virtual disk.</td>
</tr>
</tbody>
</table>

   This field displays data store name, its total storage capacity and total free space in GB.

   While selecting the datastore, do check the values in the Capacity (GB) and Free Space(GB) columns. This helps you to choose a correct datastore.

4. Click OK.
To manually create a task that creates a virtual disk

1. In the Symantec Management Console page, on the Manage menu, click Jobs and Tasks.
2. In the left pane, under Jobs and Tasks, click Virtual Machine Management.
3. Right-click the Create Disk folder and click New > Task.
4. In the tasks list, click Create Disk.
5. Give the task a name.
6. In the right pane, under Software Setting, specify the disk settings, and click OK.
7. On the create disk task page, under Task Status, specify a schedule for the task.
8. If you make changes in the task after you have created it, click Save changes.

Creating a virtual network on a host

While creating a virtual machine, you need to create or specify a virtual network that lets you connect the virtual machine to the host and to the network for accessing Internet or other computers. The Create Virtual Network task lets you create both internal as well as external virtual network from the VMM portal page. Currently, you can create only Standard or Virtual Switches networks.

If you are manually creating a task from Jobs and Tasks that creates a virtual network then you can create only internal network.

To create a virtual network

1. In the Symantec Management Console, on the Home menu, click Virtual Machine Management.
2. In the left pane, do one of the following:
   - Click the host, go to the host page on the right pane, and under Actions, click Create Virtual Network.
   - Right-click the host and click Create Network.
     The above option can also be accessed on right-click of the host from All Resources > Asset > Network Resource > Computer.
3. On the Create Network page, enter the name of the new virtual network, select the adapter to use for the network, and then click OK.

In the Adapters drop-down list, you can see only those adapters (physical NICs), which are connected to the Standard or Virtual switches.
To manually create a task that creates a virtual network

1. In the Symantec Management Console, on the Manage menu, click Jobs and Tasks.
2. In the left pane, under Jobs and Tasks, expand System Jobs and Tasks, and click Virtual Machine Management.
3. Right-click the Create Network folder and click New > Task.
4. In the tasks list, click Create Network.
5. In the right pane, under Software settings, specify the network name, and click OK.
6. On the create network task page, under Task Status, specify a schedule for the task.
7. If you make changes in the task after you have created it, click Save changes.

Creating a snapshot

You can take the snapshot of a virtual machine any time. If you change the configurations of the virtual machines frequently, you can take the snapshots of individual configurations and return to them at any time.

To create a snapshot

1. In the Symantec Management Console, on the Home menu, click Virtual Machine Management.
2. In the left pane, do one of the following:
   - Click the virtual machine, go to the virtual machine page on the right pane, and click Actions > Create Snapshot.
   - Click the virtual machine, go to the Snapshot details section of the virtual machine page on the right pane, and click Actions > Create Snapshot.
   - Right-click the virtual machine, and click Create Snapshot.

The above option can also be accessed on right click of the All Resources > Asset > Network Resource > Computer > Virtual Machine.
3. In the Create Snapshot dialog box, do one of the following:
   - Select Use the default snapshot name option for creating a snapshot with default settings. By default, this option is selected.
     The name of the default snapshot is assigned in the following format: Virtual Machine Name Creation Date Creation Time.
     For example, TestVM 20-Aug-2011 20:30:20 PM.
Select Name to manually enter the Name and Description of the snapshot.

4 Click OK.

A task is created in the Manage > Jobs and Tasks menu. This task creates a snapshot with the specified configuration.

5 To make changes to the task, update the configuration and click Save changes.

To manually create a task that creates a snapshot

1 In the Symantec Management Console, on the Manage menu, click Jobs and Tasks

2 In the left pane, under Jobs and Tasks, expand System Jobs and Tasks, and click Virtual Machine Management.

3 Right-click the Create Snapshot folder and click New > Task.

4 In the tasks list, click Create Snapshot.

5 Give the task a name and do one of the following:

- Select Use the default snapshot name option for creating a snapshot with default settings. By default, this option is selected. The name of the default snapshot is assigned in the following format: Virtual Machine Name Creation Date Creation Time. For example, TestVM 20-Aug-2011 20:30:20 PM.

- Select Name to manually enter the Name and Description of the snapshot.

6 Click OK.

7 On the create snapshot task page, under Task Status, specify a schedule for the task.

8 To make changes to the task, update the configuration and click Save changes.

Best practices to prevent protocol replacement

The Virtual Machine Management protocol can be replaced by different protocols. Agent less communication uses the first protocol and credential combination that connect successfully to a server. Network Discovery can swap node-protocol and credential associations.

Virtual Machine Management requires the VMware protocol for it to perform at its full capacity. To prevent the Virtual Machine Management protocol from being replaced, you must ensure that any discovery tasks that include vCenter servers in their scan range need to use a connection profile where the VMware protocol is enabled and include the corresponding vCenter credential information. Users must
recognize that enabling the VMware protocol in tasks with large scan ranges can take considerably longer to execute. Users should consider excluding vCenter servers from these tasks so the VMware protocol does not need to be enabled for them, thus avoiding unsuccessful attempts to use the VMware protocol on a wide range of nodes. Instead, they can create vCenter-specific discovery tasks, where the individual vCenter servers are identified and the tasks use a connection profile where the VMware protocol as well as any other protocols needed to communicate to that server are enabled.

Deployment of ESX or ESXi servers

Several sources of information about ESX/ESXi servers are available, including information about deployment.

Videos, demos, and documentation from Dell and Symantec around ESX are available at the following URL:

https://dell.symantec.com/virtualization-resources

A guide on deploying and updating VMware vSphere 5.0 (which runs ESXi) on HP ProLiant Servers is available at the following URL:

Deploying and updating VMware vSphere 5.0 on HP ProLiant Servers

An article from Symantec about how to execute tasks on VMware Hypervisor (ESX/ESXi host) and what permissions are required to execute tasks is available at the following URL:

www.symantec.com/docs/TECH188201

Tables populated during the Network Discovery and Run Inventory tasks

Below are the tables, which get populated during execution of the Network Discovery and Run Inventory tasks. These tables can help you to resolve the issues such as failure of the Run Inventory task due to tasks getting queued up or tasks timed out.

<table>
<thead>
<tr>
<th>Table 9-6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Table Name</strong></td>
</tr>
<tr>
<td>Inv_VM_Host</td>
</tr>
</tbody>
</table>
### Table 9-6 (continued)

<table>
<thead>
<tr>
<th>Table Name</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inv_VM_Guest</td>
<td>This table is populated only if you have successfully run the Network Discovery task. It contains data related to the guest servers of all the discovered ESX and HyperV hosts servers.</td>
</tr>
</tbody>
</table>
| Inv_Symantec_VMM_VirtualMachine | This table is populated only if you have successfully run the Inventory task. It contains data related to all the virtual machines for the discovered host servers. This includes following information:  
  - Virtual machine name  
  - Associated virtual disk  
  - Associated virtual network  
  - Host server guid  
  - Memory  
  - State such as Running, Stopped, Suspended, etc. |
| Inv_Symantec_VMM_Disk | Contains data related to all the virtual disks for the discovered host servers. This includes following information:  
  - Disk name  
  - Device type  
  - Capacity  
  - Host server resource guid |
| Inv_Symantec_VMM_Network | Contains data related to all the virtual networks for the discovered host servers. This includes following information:  
  - Network ID  
  - Network name  
  - Network description  
  - Host server resource guid |
About Log Viewer

The Log Viewer is a complete record of what happens when you perform a particular action in Virtual Machine Management. Administrators can use this information to debug issues that occur during the execution of Virtual Machine Management specific tasks. Quality assurance personnel can also use the Log Viewer to check the accuracy of task execution.

As you execute any Virtual Machine Management task, every action is logged in the Log Viewer. This information includes failures of actions to execute, areas to debug, and the changes that are made in your computer. You can use the Log Viewer to determine the problems and their cause. In case of any problem, the Log Viewer helps you to understand the problem and raise the issue to the technical support team.

For example, you can use the Log Viewer to check whether the Virtual Machine Management solution has been successful in establishing a connection with vCenter. The Log Viewer provides details such as the IP address of the vCenter.

You can launch the Log Viewer from the Start > All Programs > Symantec > Diagnostics > Altiris Log Viewer executable file.
Server health

- Chapter 10. Monitor Solution and Monitor Packs
- Chapter 11. Event Console
- Chapter 12. Historical and Real-Time Monitoring
Monitor Solution and Monitor Packs

This chapter includes the following topics:

- About Monitor Solution
- Introducing Monitor Solution in UNIX/Linux environments
- About core components of Monitor Solution
- About Monitor Packs, policies, rules, metrics, and tasks
- About Monitor Pack for Servers
- What you can do with monitor pack for servers
- About monitor server configuration
- Importing monitor packs
- Downloading custom Monitor packs from the Symantec Connect Community
- About agentless monitoring
- About agent-based versus agentless monitoring
- About monitor service
- Setting up a remote monitoring site server
- Setting up credentials for agentless monitoring
- About scalability best practices for Monitor Solution
About Monitor Solution

Monitor Solution lets you monitor various aspects of computer operating systems, applications, and device, such as events, processes, and performance. It helps you ensure that your servers and your devices function properly, and reduces the costs of server and network monitoring.

Monitor Solution continuously collects and analyzes data that is captured from computers and other devices on your network. When data is captured that meets the specified criteria, alerts can be raised to notify you and actions can be taken.

Monitor Solution lets you do the following:

- Collect detailed data from servers, applications, and network devices to diagnose the health of your environment.
- Collect comprehensive real-time and historical performance data to analyze trends and isolate recurring issues.
- Pinpoint problems, define their cause, and take automated actions to resolve them.

Monitor Solution supports both agent-based and agentless monitoring methods. It runs on the Symantec Management Platform and is a key component of Server Management Suite.

See “About core components of Monitor Solution” on page 148.

Monitor Plug-in or the Remote Monitoring Server gather the data that you want to monitor. The data is remotely managed from the Symantec Management Console. The Monitor Plug-in and the Remote Monitoring Server receive policies from the Notification Server computer. Monitor policies instruct the plug-in and Remote Monitoring Server of what actions to perform.

Introducing Monitor Solution in UNIX/Linux environments

Monitor Solution lets you monitor various aspects of UNIX/Linux operating systems, applications, and devices. These aspects can include events, processes, and performance. This ability helps you ensure that your servers and your devices work and reduces the costs of server and network monitoring.

See “About Monitor Packs, policies, rules, metrics, and tasks” on page 151.

Monitor Solution lets you complete the following tasks:

- Identify the health of your environment by collecting detailed data from servers, applications, and network devices.
■ Analyze trends and isolate recurring issues by collecting comprehensive real-time and historical performance data.

■ Pinpoint problems, define their cause, and take automated actions to resolve them.

Monitor Solution supports both agent-based and agentless monitoring methods. It runs on the Symantec Management Platform and is a key component of Server Management Suite.

For more information, see the Monitor Solution User Guide.

Although most Monitor Solution functions work across all platforms, the following differences exist between Windows support and support for UNIX/Linux:

■ Not all of the Application Detection Rules are cross-platform. Some work with Windows only.

■ Several metric types are only applicable to Windows (for example, Windows Processes, Windows Services, and Performance Counters). The most commonly used metric type on UNIX/Linux is the Command Line metric type.

■ Monitor packs differ between Windows and UNIX/Linux; they collect most of the same information but they use different methods.

■ The Agentless Monitor Pack applies only to Windows. However, you can manually create policies for UNIX and Linux servers and include cross-platform rules.

■ Symantec offers a Server Health Pack for Windows and Linux, but not for UNIX.

### About core components of Monitor Solution

Monitor Solution lets you monitor different aspects of servers and applications. This is done through multiple monitoring solutions that work together using a common set of Monitor Solution components that are called the core components. Each monitoring solution uses the core components and includes a set of monitoring components specific to the purpose of the solution.

<table>
<thead>
<tr>
<th>Table 10-1</th>
<th>Core components of Monitor Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Component</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Monitor Plug-in</td>
<td>Monitor Plug-in performs monitoring on client computers. Monitor Plug-in receives policies from the Notification Server computer specifying what aspects of the computer are to be monitored.</td>
</tr>
</tbody>
</table>
### Table 10-1 Core components of Monitor Solution (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agentless monitoring</td>
<td>A monitor service on a site server acts in place of Monitor Plug-in. It lets you monitor the computers that don't have Agent Plug-in installed on them. See “About agentless monitoring” on page 155.</td>
</tr>
<tr>
<td>Real-time and historical performance viewers</td>
<td>Performance viewers let you view the performance of a computer in real time or historically. Performance monitoring data makes it easy to analyze performance and identify problems. See “Viewing real-time performance data” on page 176. See “Viewing historical performance data” on page 175.</td>
</tr>
<tr>
<td>Reports</td>
<td>You can view the predefined reports, or create custom reports to meet your needs. See “About viewing the monitor data” on page 173.</td>
</tr>
<tr>
<td>Monitor packs</td>
<td>Monitor packs include the monitor policies, metrics, rules, and tasks for monitoring an operating system or application. Monitor packs also contain preconfigured monitor policies with preset thresholds and severities.</td>
</tr>
</tbody>
</table>
### Table 10-1  
Core components of Monitor Solution *(continued)*

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor policies</td>
<td>A monitor policy is group of monitoring rules. You apply monitor policies to the groups of computers and devices that you want to monitor. Monitor policies inform the Monitor Plug-in or the Remote Monitoring Server of what data you want monitored and how that data should be analyzed. The data is evaluated against the conditions of rules. Based on these rules, Monitor Plug-in can run automated actions in response to data that reaches an undesired state or range. Monitor Plug-in returns the monitored data to the Notification Server computer. The Notification Server computer uses monitored data to run Task Server tasks for real-time performance monitoring and historical performance reporting. Monitor policies are built from metrics and rules.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Metrics define how Monitor Plug-in or the Remote Monitoring Server collects data from supported data sources, called metric sources. Each plug-in can use numerous metrics to define all of the data that you want to collect.</td>
</tr>
<tr>
<td>Rules</td>
<td>Rules specify how to analyze the metric data or the event data that Monitor Plug-in and the Remote Monitoring Server collect. Rules also define the conditions that trigger them, and the actions taken.</td>
</tr>
</tbody>
</table>
### Table 10-1  Core components of Monitor Solution (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions and Tasks</td>
<td>You can add actions and tasks to a rule or a policy. Rules are triggered when monitored metric data reaches a determined value or goes beyond an acceptable value range. The triggered rule sends an alert, and any actions or tasks that are specified for that rule or policy are executed. You configure a schedule for monitor actions and tasks, or run them on demand. You can run tasks from a task server or you can choose from several Monitor Plug-in-specific task types.</td>
</tr>
</tbody>
</table>

See “About Monitor Solution” on page 147.

### About Monitor Packs, policies, rules, metrics, and tasks

Each monitor pack contains policies, which contain rules and metrics used for collecting data, and which can trigger tasks. The data collected can be used either for trending (historical) or for alerting purposes.

See “About Monitor Pack for Servers” on page 152.

- A policy is a category that describes the area you are monitoring. For example, one of your policies might be a system health and tuning policy.

- A policy is made up of a number of rules. A rule is a threshold definition that determines what conditions must occur in order for the rule to trigger. For example, a policy might contain a rule that measures excessive disk activity.

- Metrics within the rule constantly make values available to the rule evaluator mechanism. They answer the question: Does this value exceed the threshold mechanism defined in the rule?

- If yes, an alert is generated and subsequent tasks are triggered. Tasks let you define what should be done if a particular condition is met. There are two types of tasks: task server-based tasks (server side tasks), and Monitor agent tasks.
About Monitor Pack for Servers

Monitor Pack for Servers works with the Monitor Solution core components of the Symantec Management Platform. It lets you monitor operating system performance, services, and events of your Windows, Linux, or UNIX server environment.

This pack includes several reports to help you evaluate and tune the performance of your server components.

What you can do with monitor pack for servers

You can use monitor pack for servers to monitor several Windows-specific, and Linux and UNIX-specific elements.

You can monitor the following Windows elements:

- Active Directory
You can monitor the following Linux and UNIX elements:

- Disk
- Memory
- Ports
- Printers
- Processor
- Security
- DNS
- DHCP
- MSMQ

**About monitor server configuration**

You can configure the monitor server settings to meet your specific needs.
Table 10-2  Process for configuring the monitor server

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Import a monitor pack.</td>
<td>Monitor packs include monitor policies, metrics, rules, and tasks for monitoring an operating system or application. Monitor packs also contain preconfigured monitor policies with preset thresholds and severities. You can import a monitor pack to monitor computers and devices. See “Importing monitor packs” on page 154.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Set up database maintenance.</td>
<td>Monitor Solution collects data from monitor computers and stores it in the database. You can configure the database maintenance settings to define when data is summarized and purged.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure heartbeat monitoring settings.</td>
<td>Monitor Solution collects heartbeat signals from Monitor Plug-ins. You can configure the server-side heartbeat settings to define how often Monitor Solution checks for heartbeats. Specify the number of failures that are allowed to occur before Monitor Solution sends an alert to the Event Console.</td>
</tr>
</tbody>
</table>

Importing monitor packs

You use monitor packs to monitor different aspects of your computer resources and network to ensure their availability. Monitor packs include monitor policies, metrics, rules, and tasks for monitoring an operating system or application. Monitor packs also contain preconfigured monitor policies with preset thresholds and severities.

You can import monitor packs after the installation of Monitor Solution. Importing monitor packs lets you choose what functionality you want to install on your monitoring server, and when you want to install it.

See “About monitor server configuration” on page 153.

To import monitor packs

1. In the Symantec Management Console, on the Home menu, click Monitoring and Alerting.
2. In the left pane, under Monitoring and Alerting, expand Monitor > Policies, and then click Import Monitor Pack.
3 On the Import Monitor Pack page, click the monitor pack that you want to import.

4 On the toolbar, click Schedule.

5 In the Schedule Monitor Pack dialog box, configure the schedule settings, and then click OK.

Downloading custom Monitor packs from the Symantec Connect Community

Symantec Connect is a source for both Symantec monitor packs and custom monitor packs provided by users and third parties. Customers can submit any type of Monitor pack that other customers may find useful. Monitor packs can vary from a single custom rule and metric to complex rules and metrics. You can also submit requests for Monitor packs on Symantec Connect. The product manager usually responds with information on whether this particular pack is in development or planned.

See “About Monitor Pack for Servers” on page 152.

To download custom monitor packs


2 Do a search on "Monitor pack."

3 For community guidelines and disclaimers on creating custom Monitor packs, go to http://www.symantec.com/connect/articles/monitor-packs-community-guidelines-creating-custom-monitor-packs

About agentless monitoring

Agentless monitoring lets you monitor the computers that do not have Monitor Plug-in installed. You monitor these computers with agentless monitoring policies. Because Monitor Plug-in is not available on the computer, fewer aspects of the computer are available to be monitored. You use monitor service on a site server to perform agentless monitoring.

All agentless monitoring policies have a list of resource targets that are monitored. Each monitor service monitors the resources assigned to its server if an agentless monitoring policy targets those resources. Multiple site servers can monitor the same resource that is targeted by an agentless monitor policy. Also, different site
servers can monitor different resources that are targeted by the same agentless monitor policy.

You can use agentless monitoring in the following situations:

■ You cannot install Symantec Management Agent on the device that you want to monitor.
   For example, devices that have an embedded system.

■ You want to monitor the availability of a server.
   In most cases, you need to use agentless monitoring to perform an availability (ping) monitor.

About agent-based versus agentless monitoring

Monitor Solution supports the following methods for monitoring servers:

■ Agent-based monitoring, using a plug-in that extends the Symantec Management Agent

■ Agentless monitoring, using standard protocols like WMI, SNMP and WSMan, and so forth. Monitor Solution Agentless is integrated into site servers and is referred to as the Remote Monitoring Server (RMS). Agentless monitoring is dependent on the credentials that are used during the Network Discovery phase.

See “Setting up a remote monitoring site server” on page 157.

The general best practice is to use the plug-in where possible as it provides more monitoring capabilities and auto remediation and is less intrusive on the network bandwidth. The following table highlights some of the advantages and disadvantages of each approach.

Table 10-3  Comparison of agent-based and agentless monitoring

<table>
<thead>
<tr>
<th>Agent-based monitoring</th>
<th>Agentless monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gathers much more information</td>
<td>Provides more limited monitoring capabilities (those available through the standard protocols).</td>
</tr>
<tr>
<td>Provides auto remediation</td>
<td>Is limited to the remediation capabilities through those protocols.</td>
</tr>
</tbody>
</table>
Table 10-3  Comparison of agent-based and agentless monitoring (continued)

<table>
<thead>
<tr>
<th>Agent-based monitoring</th>
<th>Agentless monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is less intrusive on the network bandwidth.</td>
<td>Is dependent on the network; the metric values must be sent to the site server to be</td>
</tr>
<tr>
<td>For example, the agent will send events to the central event console only when the</td>
<td>evaluated to determine if a threshold has been triggered.</td>
</tr>
<tr>
<td>threshold has been triggered. The auto remediation occurs even before the event has</td>
<td></td>
</tr>
<tr>
<td>reached the central event console and is not dependent on the network.</td>
<td></td>
</tr>
</tbody>
</table>

About monitor service

Monitor service on a site server lets you perform agentless monitoring. Monitor service is installed on the Notification Server computer by default.

See “About agentless monitoring” on page 155.

Because monitoring can be resource-intensive, you can distribute the monitoring load to other site servers to reduce the load on Notification Server. You can also remove monitor service from the Notification Server computer to further reduce the load on this server.

See “Setting up a remote monitoring site server” on page 157.

Monitor service is integrated with the site server infrastructure. This integration lets the user specify the resources that each site server monitors.

Setting up a remote monitoring site server

You use monitor service on a site server to perform agentless monitoring. By default, monitor service is installed on the Notification Server computer. You can distribute the monitoring load to other site servers to reduce the load on Notification Server. You can also remove monitor service from the Notification Server computer to further reduce the load on this server.

You can set up as many monitoring site servers as you need.

Monitor service is integrated with the site server infrastructure. This integration lets you specify the resources that each site server monitors.

See “About agentless monitoring” on page 155.

See “About monitor service” on page 157.

To install monitor service on a remote site server, the server must be running one of the following operating systems:
- Microsoft Windows Server 2008 R2 x64
- Microsoft Windows Server 2012 R2 x64

The **Potential Monitor Servers** filter automatically determines possible site servers. This filter is available on the Manage menu, under Filters. Agentless monitor policies do not require any special configuration to work with a monitor service on one or more site servers.

**Warning:** Symantec recommends that you only install monitor service on a computer that is secure and trusted. The security settings of the Notification Server computer must also apply to the site server computer.

Monitor service requires that you install the following on the site server:

- Symantec Management Agent.
- The Pluggable Protocols Architecture (PPA) client computer component.
- The credential manager client computer component.

**Table 10-4 Process for setting up a remote monitoring site server**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Install Symantec Management Agent on the site server.</td>
<td>A remote monitoring server requires Symantec Management Agent to be installed on the site server.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure connection profiles on Notification Server.</td>
<td>Connection profiles must be configured on Notification Server computer for remote monitoring to work. Configure your connection profiles before you install the Pluggable Protocols Architecture (PPA) client computer component on the site server.</td>
</tr>
</tbody>
</table>
### Table 10-4  
**Process for setting up a remote monitoring site server (continued)**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Install the Pluggable Protocols Architecture (PPA) client computer component on the site server.</td>
<td>A remote monitoring server depends on the Pluggable Protocols Architecture (PPA) client computer component to communicate with network devices and computers. When the Pluggable Protocols Architecture (PPA) client computer component is installed, the credential manager client computer component is also installed. See “Installing the Pluggable Protocols Architecture (PPA) client computer component on a site server” on page 159.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Add monitor service to one or more site servers.</td>
<td>You can add monitor service to a site server on the site management page. See &quot;Adding monitor service to a site server&quot; on page 160.</td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) Remove monitor service from Notification Server.</td>
<td>You can remove monitor service from Notification Server to reduce the load on this server.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Configure the remote monitoring server settings.</td>
<td>You can configure the remote monitoring server settings. These settings apply to all monitor site servers. See “Configuring remote monitoring server settings” on page 162.</td>
</tr>
<tr>
<td>Step 7</td>
<td>(Optional) View the monitor site server reports.</td>
<td>The monitor site server reports let you determine which site servers monitor the resources that your agentless monitor policies target. See “Viewing monitor site server reports” on page 162.</td>
</tr>
</tbody>
</table>

### Installing the Pluggable Protocols Architecture (PPA) client computer component on a site server

Pluggable Protocols Architecture (PPA) includes a policy that can remotely install the Pluggable Protocols Architecture (PPA) client computer component on a site server. You must install this component on a site server before you can add monitor...
service to the site server. When the Pluggable Protocols Architecture (PPA) client computer component is installed, the credential manager client computer component is also installed. The policy that installs the credential manager client computer component configures the agent to automatically import credentials from Notification Server.

See “Setting up a remote monitoring site server” on page 157.

**Warning:** Symantec recommends that you only install monitor service on a computer that is secure and trusted. The security settings of the Notification Server computer must also apply to the site server computer.

---

To install the Pluggable Protocols Architecture (PPA) client computer component on a site server

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.

2. In the left pane, under **Settings**, expand **Monitoring and Alerting > Protocol Management**, and then click **Install x86 Pluggable Protocols Agent Package** or **Install x64 Pluggable Protocols Agent Package**.

3. In the right pane, do the following:
   - Under **Applied to**, on the toolbar, click **Apply to**, and then configure the policy application.
   - Under **Schedule**, on the toolbar, click **Add schedule**, and then configure the policy run settings.
   - Turn on the policy.
     At the upper right of the page, click the colored circle, and then click **On**.

4. Click **Save changes**.

After Pluggable Protocols Architecture (PPA) and credential manager are installed, wait until Symantec Management Agent sends inventory information before adding a monitor service. You can confirm that the inventory information was sent on the site server, on the **Symantec Management Agent Settings** tab of the Symantec Management Agent user interface.

---

Adding monitor service to a site server

You use monitor service on a site server to perform agentless monitoring. Monitor service is installed on the Notification Server computer by default. You can also add monitor service to one or more site servers.

See “About agentless monitoring” on page 155.
Before you can add monitor service to a site server, you need to install the following components on that server:

- Symantec Management Agent.
- Pluggable Protocols Architecture (PPA) client computer component.
- Credential manager client computer component.
  Credential manager client computer component is installed when you install Pluggable Protocols Architecture (PPA) client computer component. After Pluggable Protocols Architecture (PPA) and credential manager are installed, wait until the Symantec Management Agent sends inventory information before adding a monitor service.

See “Setting up a remote monitoring site server” on page 157.

**Warning:** Symantec recommends that you only install monitor service on a computer that is secure and trusted. The security settings of the Notification Server computer must also apply to the site server computer.

When you add monitor service to a site server, it is installed according to the schedule of the installation policy. Monitor service has installation policies for 64-bit and 32-bit computers. To access these installation policies, in the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**, and then, in the right pane, expand the **Monitor Service** section.

**To add monitor service to a site server**

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.

2. In the right pane, under **Detailed Information**, on the toolbar, in the **View** drop-down list, click **Site Servers**.

3. Under **Detailed Information**, in the server list, click the site server, and then, on the toolbar, click the **Edit** symbol.

4. In the **Add/Remove Services** dialog box, check **Monitor Service**, and then click **Next**.

   You cannot check **Monitor Service**, if Pluggable Protocols Architecture (PPA) and credential manager are not installed on the site server.

5. In the **Add/Remove Services** dialog box, click **OK**.

6. To check the status of the installation, on the **Site Management** page, expand **Site Services > Monitor Service**.

   A pie chart displays the site servers that are installed, pending installation, or not installed.
Configuring remote monitoring server settings

You can configure the settings for the remote monitoring servers. You use a remote monitoring server and a monitor service to perform agentless monitoring.

See “About agentless monitoring” on page 155.

The remote monitoring server settings are the global settings that apply to all monitor site servers.

See “Setting up a remote monitoring site server” on page 157.

See “Adding monitor service to a site server” on page 160.

To configure remote monitoring server settings

1. In the Symantec Management Console, on the Home menu, click Monitoring and Alerting.
2. In the left pane, under Monitoring and Alerting, expand Monitor > Settings, and then click Remote Monitoring Server Settings.
3. In the right pane, under Plug-in Config Settings, click the following tabs to configure policy settings:
   - General
   - Performance Tuning
   - Data Collection
4. Turn on the policy.
   At the upper right of the page, click the colored circle, and then click On.
5. In the right pane, click Save changes.

Viewing monitor site server reports

Monitor service on a site server lets you run agentless monitoring policies to monitor the resources that do not have Symantec Management Agent installed. The monitor site server reports let you determine which site servers monitor the resources that your agentless monitor policies target.

See “About agentless monitoring” on page 155.

The monitor site server reports are as follows:

- Monitored resources by RMS
- Resources not monitored by RMS

This report lists the resources that the specified site server monitors.

This report lists the resources that no site server monitors.
This report lists the site servers that monitor the specified resource.

To view monitor site server reports

1. In the Symantec Management Console, on the Reports menu, click All Reports.
2. In the left pane, under Reports, expand Monitoring and Alerting > Monitor > Configuration > Monitor site server.

Setting up credentials for agentless monitoring

You must set up credentials so that the Remote Monitoring Server (RMS) agent can connect to the computers to be monitored. To set up credentials, use Credential Manager, which is a component of the Symantec Management Platform.

See “Setting up a remote monitoring site server” on page 157.

Credential Manager provides a secure storage location for user names and passwords. The types of credentials that are stored are defined by the installed management solutions. Access to credentials is controlled using the built-in role-based security of the Symantec Management Platform. When a credential is created, only the creator is granted access. If other users need to perform management operations requiring a credential, they must be assigned rights.

The credential manager agent package installs on a Notification Server as part of the Symantec Management Platform. This enables the Notification Server computer to access the credential store.

Connection Profiles and the Pluggable Protocols Architecture store the information that is required to communicate with computers and other network devices using standard network monitoring protocols. The Pluggable Protocols Architecture unifies the configuration of protocols across the Symantec Management Platform. Connection Profiles is a feature of the Symantec Management Platform that other solutions and components in the Symantec Management Platform leverage. It provides the ability to update and add protocols without requiring a wholesale upgrade of all dependent solutions. These protocols include SNMP, WMI, WSMAN, as well as several others.
### Table 10-5

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create protocol-specific credentials.</td>
<td>You use Credential Manager to add credentials specific to the protocol that is used for monitoring. See “Creating protocol-specific credentials” on page 164.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Associate the credential with a connection profile.</td>
<td>You store the credential with the associated protocol in a connection profile. See “Associating credentials with a connection profile” on page 164.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Discover resources to bind the connection profiles to them.</td>
<td>Connection profiles are associated with devices during network discovery. See “Discovering resources to which to bind connection profiles” on page 165.</td>
</tr>
</tbody>
</table>

### Creating protocol-specific credentials

You use Credential Manager to add credentials specific to the protocol that is used for monitoring.

See “Setting up credentials for agentless monitoring” on page 163.

**To create credentials**

1. In the Symantec Management Console, navigate to **Settings > Monitoring and Alerting > Credentials Settings > Credential Management**

2. Click **Add Credentials**.

3. Select the type of credential from the list.

   The credential type must correspond to the protocol that is monitored in the agentless policy rules. For example, a policy containing rules that use HTTP would need HTTP credentials for monitoring.

4. Add a user name, password, and domain (if applicable.)

5. Click **Save**.

### Associating credentials with a connection profile

See “Setting up credentials for agentless monitoring” on page 163.
Connection profiles store the information that is required to communicate with computers and other network devices using standard network monitoring protocols. These protocols include SNMP, WMI, WSMan, and several others.

The credentials that are provided are stored securely by the credential manager. If additional administrators need access to use a connection profile, they must be granted rights to the credentials and to the connection profile. You can grant the rights by editing the credential and the connection profile.

Typically, you should create a new connection profile for each segment of your network that uses different network monitoring credentials. You can copy and make changes to already existing connection profiles. This process is called cloning.

To associate credentials with a connection profile

1. In the Symantec Management Console, navigate to Settings > Monitoring and Alerting > Protocol Management > Connection Profiles > Manage connection profiles.

2. Click Add settings, and provide a name for the new profile.

3. Click the arrow next to any protocols that you want enabled and provide the required protocol details.

4. At the upper right, next to the protocols you want enabled, click the colored circle, and then click On.

5. Click OK to save your changes.

Discovering resources to which to bind connection profiles

See “Setting up credentials for agentless monitoring” on page 163.

In order for the RMS Agent to connect to a resource using a specific protocol, you must have the connection profile binding to that resource. Running a network discovery task achieves that goal. It binds the computers that are specified in the IP range to the connection profile that is used in that network discovery task. It establishes the association between a resource and the connection profile to be used. This “resource-to-connection-profile association” is needed for a resource to be monitored in an agentless manner, using any of the following agentless metric sources:

- HTTP
- SNMP
- WMI
- WS-MAN
Connection profiles are associated with devices during network discovery. During discovery, a connection profile is selected to define the protocols and credentials to use. When discovery completes, this connection profile is then associated with each discovered resource. When information is required, the associated connection profile is used to connect.

To discover resources to which to bind connection profiles

1. In the Symantec Management Console, navigate to **Home > Discovery and Inventory > Network Discovery**.
2. Click **Launch Discovery Wizard**.
3. Specify an IP address range of resources you want to monitor in an agentless manner and click **OK**.
4. Select a connection profile and click **Finish**.

The resources are now discovered, based on the connection profiles. The associated protocols and credentials are bound to the resources.

The PPA Agent (as leveraged by the RMS) uses a stored procedure (dbo.sp_PPA_GetResourceIPAddressList) to obtain a list of IP addresses by resource GUID. Depending on the protocol, either the “primary” (best IP available) is used, or all IP addresses are used. IP addresses in the Network Discovery tables take precedence, but basic inventory tables are also called to obtain IP address information.

If Network Discovery has not been run against the resource, the “default connection profile” is used. In that case, basic inventory that is gathered by the Symantec Management Agent is referenced for available IP address information.

### About scalability best practices for Monitor Solution

When implementing Monitoring and Alerting as part of Server Management Solution, the following items should be reviewed:

- Number of managed/monitored nodes or resources.
- All Agent versions are up-to-date.
- Number of enabled monitor packs/policies.
- Metric polling interval
- Configuration settings and data performance
- Purging settings
- CMDB database growth and Monitor table size
For more information about recommended settings for these items, see the article at the following URL:

Suggested scalability configuration and values for Monitoring and Alerting:

- Number of Monitored Resources: 1500 per Symantec Management Platform
- Agent Based: 1500 resources
- Agent Less: 500 resources per Remote Monitoring Server RMS
- Number of metrics: 40 total per server
- Polling Interval: default
- Data Collection: Record Process Value: default
- Turn Off most machines: suggest separating them into classes/different configuration policies
- Server Settings: Purging Detailed Data Numeric: default
Event Console

This chapter includes the following topics:

- About alerts
- About alert management
- About Event Console alert filters
- Filtering alerts

About alerts

Alerts are the status messages that contain information about device or network health. Status messages are generated using standard monitoring protocols, such as SNMP.

Each status message that is received is converted into a common format that is called an alert. During conversion, alerts are associated with the affected resource in the CMDB and are assigned a severity and a status. Severity ranges from normal to critical, and alert status can be new, acknowledged, or resolved.

Alerts from multiple protocols are displayed using common severity and status. All received alerts are displayed in the Event Console.

See “About Event Console alert filters” on page 169.

About alert management

Alert management shows a consolidated view of device health across your network. You can view health by network layout, organizational group, or by directly monitoring the list of received alerts in the Event Console.

The Event Console reduces the need to maintain separate tools to monitor different devices. The Event Console collects SNMP traps and other status messages and
displays them in a single location. All status messages are converted to a common format that links each received message to the affected resource in the Configuration Management Database (CMDB). These formatted messages are called alerts. See “About alerts” on page 168.

Advanced search features let you quickly find specific alerts or groups of alerts. The Event Console also provides a rule-based triggering system that lets you create alert matching rules to process alerts in the following ways:

- Discard specific alerts from the database.
- Forward alerts to another management system.
- Execute task server tasks in response to specific alerts.
- Initiate a workflow in response to specific alerts.

**Note:** If the Notification Server computers and the SQL Server computers are not set to the same time and the same time zone, then any alerts that have occurred in the past few hours are not displayed in the Event Console.

### About Event Console alert filters

The Event Console in Symantec Management Platform displays alerts in a grid layout. Alert filters let you sort the alerts so that you can analyze and manage them.

To view the alerts, in the Symantec Management Console, on the **Manage** menu, click **Events and Alerts**.

The Event Console contains several rule types that represent automated, event-based actions. The rule types include discarding, forwarding, task, and workflow rules. Discarding rules filter and discard matching alerts. Forwarding rules forward a Simple Network Management Protocol (SNMP) trap to a downstream listener. Task rules initiate Symantec Management Platform task server tasks. An event can automatically start a workflow process. This workflow process can pass along valuable event data.

See “About alerts” on page 168.

The advanced filter function lets you use advanced filters to manage alerts.

To filter the alerts, on the **Event Console** page, in the **Select a filter** drop-down list, click an alert type.

The color-coded status bar lets you see the number of alerts by severity level, as follows:
To view the information about a specific alert type, on the Event Console page, click the colour section of the status bar, and the grid view below changes. It shows only those alerts that match the severity level of the color that you clicked. For example, if you click yellow on the status bar, then the grid shows alerts with severity Warning. After you filter by severity level, in the Select a filter drop-down list, you can clear the selection to see the complete list of alerts again.

See “Filtering alerts” on page 171.

The toolbar on the Event Console page displays the following symbols:

- **Details**
  
  Opens the Alert Details dialog box for the chosen alert.

- **Acknowledge**
  
  Lets you acknowledge a chosen alert. In the State column, a blue flag indicates an acknowledged alert.

- **Resolve**
  
  Flags the chosen alert with a check mark in the State column.

  When you right-click a resolved alert, you can view alert details. You can also view the available rules for discarding the alert or open the Resource Manager in a new window.

  If you click Discarding Rules with a resolved alert selected, you can create a global discard filter rule or create a resource discard filter rule.

- **Actions**
  
  When you click an alert, and then on the toolbar, click the Actions symbol, you see the options that you see when you right-click a resolved alert.
When you click an alert, you can manage it by changing its severity to any of the following:

- Undetermined
- Informational
- Warning
- Major
- Critical
- Normal

On the Alert Filter Settings page, you can create and configure filters. To access this page, on the toolbar, click the symbol.

You can type the custom search criteria in the Search box, on the toolbar.

When you click a different filter in the drop-down list, the grid view displays the alerts that pertain to the selected filter. You can click any other control on the page, except Refresh, and the filter that you chose remains active.

Filtering alerts

The Event Console grid can contain thousands of alerts, which you can filter. If the alerts that you expect to see are not displayed, they may be hidden, or a filtering rule has blocked them. For example, some administrators prefer to hide warning alerts.

See “About Event Console alert filters” on page 169.

In the Event Console, the default filter is Exclude information alerts. When you open the alert grid, this default filter is applied. Anytime you click the Refresh icon in the browser window, the selected filter is reset. You can also clear filters and select new ones.
To filter alerts

1  In the Symantec Management Console, on the Manage menu, click Events and Alerts.

   If the filter you see in the filter drop-down box is not the one you want to use, perform the next step.

2  (Optional) In Event Console click the X icon to the right of the filter drop-down box, or delete the filter text from the box.

   The alerts are cleared from the grid, and Select a filter appears in the drop-down box.

3  Click the down-arrow next to the drop-down box to select a different filter.

   As soon as you select a different filter from the drop-down list, the grid view changes. It shows only the alerts that pertain to the selected filter. You can click any other control on the page, except Refresh, and the filter that you chose remains active. If you need to view alerts for more than one filter, you can open multiple instances of Event Console. You then select a different filter in each window.
Historical and Real-Time Monitoring

This chapter includes the following topics:

- About viewing the monitor data
- Viewing historical performance data
- Viewing real-time performance data
- Viewing the Monitor Alerts dashboard
- Generate a report on Monitor Solution metrics, trends, alerts, and actions
- Generating ad-hoc reports with the IT Analytics Monitor Metrics cube

About viewing the monitor data

Monitor Solution lets you view data about your monitored computers in different reports to ensure that all monitored computers and applications function properly.

You can view the data on the **Monitoring and Alerting** page or on the **Reports** page.

To view monitor data on the **Monitoring and Alerting** page, in the Symantec Management Console, on the **Home** menu, click **Monitoring and Alerting**.

The **Monitoring and Alerting** page includes the following Web parts:
### Table 12-1 Monitoring and Alerting page Web parts

<table>
<thead>
<tr>
<th>Web part</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Launch Performance Viewer</strong></td>
<td>You use this Web part to enter the name of a computer and run the performance viewer.</td>
</tr>
<tr>
<td></td>
<td>See &quot;Viewing real-time performance data&quot; on page 176.</td>
</tr>
<tr>
<td><strong>Monitored Resources by Status</strong></td>
<td>This Web part shows the monitored resources. The resources are organized according to severity status. The state of a computer is the most severe state of any triggered rule on the computer.</td>
</tr>
<tr>
<td></td>
<td>For example, if one rule state is warning and another is critical, the overall state of the computer is critical. If all rule states are normal, and then one rule state changes to warning, the computer state is set to warning.</td>
</tr>
<tr>
<td></td>
<td>This Web part also shows computers with Monitor Plug-in installed. You can click a computer, and then, on the toolbar, launch the Performance Viewer, the Resource Manager, or the Event console.</td>
</tr>
<tr>
<td><strong>Monitor Site Servers Status</strong></td>
<td>This Web part shows a list of Monitor Site Servers and their status.</td>
</tr>
<tr>
<td><strong>Group View - Aggregate health by resource</strong></td>
<td>This Web part shows the aggregate health of the devices and computers in your organizational groups.</td>
</tr>
<tr>
<td><strong>Event Console</strong></td>
<td>This Web part shows a consolidated view of all alerts that are raised.</td>
</tr>
</tbody>
</table>

### To view the data on the Monitoring and Alerting page

1. In the Symantec Management Console, on the **Home** menu, click **Monitoring and Alerting**.

2. In the left pane, under **Monitoring and Alerting**, expand **Monitor > Reports**, and then navigate to the report that you want to view.

### To view monitor data on the Reports page

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.

2. In the left pane, under **Reports**, click **Monitoring and Alerting**, and then navigate to the report that you want to view.
Viewing historical performance data

The historical performance viewer is a component of Monitor Solution that lets you view historical performance data. Historical data is available from both Monitor Plug-in and Remote Monitor Server.

To view historical performance data

1. In the Symantec Management Console, on the Actions menu, click Monitor > Historical.

2. On the Historical Performance Viewer page, on the toolbar, in the Device box, type the name of the device, or click the Select resource with historical data symbol, and then choose a device from the resource list.

3. Specify the time period for which you want to view the data.

   The time period that you specified in From and To boxes, may contain no data in the beginning or at the end of the period. In this case, Summarized View shows only the actual time when the data is available. The empty timeline with no data in the beginning or at the end of the chart is not displayed.

4. On the toolbar, click Metrics.

5. In the Available Metrics dialog box, specify the metric data that you want to view, and then click OK.

6. In the Summarized View diagram, drag the mouse across the graph to specify the range that you want to view.

7. In the Detailed View box, choose a point on the graph.

   If available, the data that was last gathered for the selected point is displayed in Processes, Events, Ports, and Text Data Web parts.

   The Metrics Web part displays the average, minimum, and maximum values for the whole range of data that is displayed in the Detailed View. However, the Last Value and Last Time columns in the Metrics Web part display the value for the selected point. If the selected point has no value, these columns display the value that precedes this point. If no value is available for the metric in the Detailed View, the Last Value and Last Time columns are left blank in the Metrics Web part.

See “Viewing real-time performance data” on page 176.
Viewing real-time performance data

The Performance Viewer is a component of Monitor Solution that lets you view real-time performance data. Performance data is available from both Monitor Plug-in and Remote Monitor Server.

To view real-time performance data

1. In the Symantec Management Console, on the Actions menu, click Monitor > Real-time.

2. On the Real-time Performance Viewer page, on the toolbar, in the Device box, type the name of the device, or click the Select resource with historical data symbol, and then choose a device from the resource list.

3. In the Registered Metrics dialog box, check the metric data that you want to monitor, and then click OK.

The performance viewer begins monitoring the computer and displays the following information:

- **Graph**: This section displays graphical performance data. The data is scaled to fit within the limits of the graph. If you place the mouse pointer over a point on a graph line, the monitored metric data is displayed next to the mouse pointer. If you monitor multiple instance metrics, each instance has a separate graph line. You can use the Select Metrics option to monitor different metrics.

- **Metrics**: This section displays all numeric metric data that is monitored.

- **Processes**: This section displays the processes that are currently running on a monitored computer.

- **Events**: This section displays all Windows NT event data.

- **Ports**: This section displays the status of the monitored ports on the computer.

- **Text Data**: This section displays the retrieved text data for command, custom DLL, custom COM object, WS-MAN, SNMP, SQL, and string-type Windows Management Instrumentation (WMI) metrics. The predefined WMI metrics are the only metrics that collect this type of data. If you create or use a custom DLL, COM object, SNMP, or command metric that retrieves this data, it is also displayed in this section.

See “Viewing historical performance data” on page 175.
Viewing the Monitor Alerts dashboard

After IT Analytics Solution is installed and configured, you can view any dashboards in Symantec Management Platform. For more information, see the IT Analytics User Guide at the following URL:

See “Generate a report on Monitor Solution metrics, trends, alerts, and actions” on page 178.

See “Generating ad-hoc reports with the IT Analytics Monitor Metrics cube” on page 180.

The dashboard displays the following information:

- Alerts by category (such as memory, heartbeat, network, processor)
- Alerts by severity level (critical, major, normal, warning)
- The most active rules that generate alerts (lists the rules that cause the most problems)

To view the Monitor Alerts dashboard

1. In the Symantec Management Console, navigate to Home > Monitoring and Alerting > Monitor.

2. Click IT Analytics Monitor Alerts Dashboard.

3. View the output, similar to the following screenshot:
After IT Analytics Solution is installed and configured, you can create IT Analytics reports in Symantec Management Platform. For more information, see the *IT Analytics User Guide*.

See “Generating ad-hoc reports with the IT Analytics Monitor Metrics cube” on page 180.

See “Viewing the Monitor Alerts dashboard” on page 177.

IT Analytics reports combine metrics, trends, alerts, and actions. They let you see what occurs with a particular metric over a period of time. The report shows the following information:

- How the metric trends over time
- Any alerts that were triggered
- Any remediation tasks that resolved the alert
- Notifications that were generated
Details on individual timestamps

To generate the Monitor Metrics Trend report

1. In the Symantec Management Console, navigate to Home > Monitoring and Alerting > Monitor.
2. Select IT Analytics reports, then select the Monitor Metrics Trend report.
3. Select a date.
4. Select a computer resource.
5. Select a metric value, such as Available memory in MB.
6. Run the report.
7. View the output, similar to the following screenshot:

Monitor Metrics Trend

![Graph showing historical and real-time memory usage]

Hourly Details for Memory - Available MB

<table>
<thead>
<tr>
<th>Hour</th>
<th>Min</th>
<th>Avg</th>
<th>Max</th>
<th>Alerts</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 AM</td>
<td>980.00</td>
<td>980.00</td>
<td>980.00</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 AM</td>
<td>1,209.00</td>
<td>1,209.00</td>
<td>1,209.00</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 AM</td>
<td>404.00</td>
<td>404.00</td>
<td>404.00</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 AM</td>
<td>1,208.00</td>
<td>1,208.00</td>
<td>1,208.00</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4 AM</td>
<td>1,186.00</td>
<td>1,186.00</td>
<td>1,186.00</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5 AM</td>
<td>1,139.00</td>
<td>1,139.00</td>
<td>1,139.00</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6 AM</td>
<td>219.00</td>
<td>219.00</td>
<td>219.00</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7 AM</td>
<td>234.00</td>
<td>234.00</td>
<td>234.00</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8 AM</td>
<td>1,119.00</td>
<td>1,119.00</td>
<td>1,119.00</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>9 AM</td>
<td>1,119.00</td>
<td>1,119.00</td>
<td>1,119.00</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10 AM</td>
<td>1,119.00</td>
<td>1,119.00</td>
<td>1,119.00</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>11 AM</td>
<td>104.00</td>
<td>104.00</td>
<td>104.00</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>12 PM</td>
<td>1,123.00</td>
<td>1,123.00</td>
<td>1,123.00</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>1 PM</td>
<td>161.00</td>
<td>161.00</td>
<td>161.00</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2 PM</td>
<td>161.00</td>
<td>161.00</td>
<td>161.00</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 PM</td>
<td>161.00</td>
<td>161.00</td>
<td>161.00</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Generating ad-hoc reports with the IT Analytics Monitor Metrics cube

After IT Analytics solution is installed and configured, you can create IT Analytics reports in Symantec Management Platform. For more information, see the IT Analytics User Guide at the following URL:

See “Generate a report on Monitor Solution metrics, trends, alerts, and actions” on page 178.

See “Viewing the Monitor Alerts dashboard” on page 177.

IT Analytics Monitor cubes allow for quick ad-hoc reporting and data mining from the data that is collected by Monitor Solution. IT Analytics currently ships with one Monitor Solution-related cube that supports UNIX/Linux environments, the Monitor Metrics cube.

The cube lets you do the following:

■ Build a report by selecting tables and attributes, such as computer count, alert count, and action count, computer name, OS, event category, severity level, event message.

■ Drill down into the computer, the OS, and see all the categories of alerts.

■ Drill down on the alert categories, such as memory alerts and their severity.

■ Turn this report into a chart for a graphical presentation.

■ Drag and drop different report elements and refine the report ad hoc.

The following screenshot is an example of what this report might look like.

![Monitor Metrics screenshot](image-url)
Process Automation

- Chapter 13. Built-in Workflow capabilities
Built-in Workflow capabilities

This chapter includes the following topics:

- About Symantec Workflow integration with UNIX and Linux clients
- Pieces of Symantec Workflow
- What you can do with Symantec Workflow
- Executing scripts on UNIX and Linux systems through SSH
- About Process Manager reporting

About Symantec Workflow integration with UNIX and Linux clients

Symantec Workflow is a security process development framework that you can use to create both automated business processes and security processes. These processes provide for increased repeatability, control, and accountability. At the same time, Workflow lets you reduce your overall workload.

The Symantec Workflow framework also lets you create Workflow processes that integrate Symantec tools into your organization's unique business processes. After Workflow is deployed, Workflow processes can respond automatically to environmental variables. Workflow processes can also allow for human interface points when a process calls for someone to make a decision with accountability. The applications that you design can create human interaction through a variety of user interfaces. You can create human interaction through email, Web forms, handheld devices, or a task list.

See “What you can do with Symantec Workflow” on page 187.
Workflow is included as part of Server Management Suite. The Workflow Installer is available as a download from Symantec Management Console on the Manage > Workflows menu.

Symantec Workflow runs natively on Windows Server. The best practice is to install Workflow onto a separate server computer that runs Windows Server software rather than installing it on the platform server. For more information on where and how to install Workflow, see the Symantec Workflow User Guide.

Although Workflow does not run natively on UNIX or Linux platforms, it can integrate with UNIX/Linux client computers on your network through the following methods:

- Symantec recommends that you use an intermediary platform such as Symantec Management Platform to run the tasks that are part of a Workflow project. This method is the best practice.
  
  Through the platform Administrator Software Developer Kit (ASDK), you can design Workflow projects to coordinate platform activities and tasks. This coordination lets you perform actions on UNIX and Linux client computers as part of the Workflow project. Such actions can include but are not limited to running scripts, collecting data, or deploying patches and software. In this way, Workflow orchestrates activities on UNIX and Linux clients as well as Windows clients.
  
  For information about using the ASDK to integrate with Symantec Management Platform, see the ASDK documentation. This documentation was installed on your computer when you installed the ASDK. The documentation is a stand-alone CHM file. Double-click the file to open and browse it.

- Workflow can communicate through the applications that are hosted on UNIX and Linux systems if those applications include the necessary integration points. Integration points include an API, a Web services layer, or an ODBC layer. The applications must follow the protocols with which Workflow can communicate, including XML and flat files.
  
  For more information on communication layer options, see the Symantec Workflow User Guide.

- If a Workflow project requires that actions be performed on a computer on which the Symantec Management Agent cannot be installed, you have one option. You can use a non-secure integration method.

  Warning: This method is not secure and is not a best practice. However, you may find it necessary to execute scripts if no agent is available to do so.

  Ideally, you use the Symantec Management Agent to run scripts and commands because the agent method is secure. However, Workflow can execute commands without the agent. Workflow can execute scripts on a UNIX or Linux client through
Secure Shell (SSH) if that client does not have Symantec Management Agent installed.

If a Workflow project requires that actions be performed on a computer where an agent cannot be installed, the script method provides a workaround. One scenario in which you might need this workaround is if actions need to be performed on a server. To use this method, you must pass the credentials to run the command at the same time that you run the command.

See “Executing scripts on UNIX and Linux systems through SSH” on page 189.

See “Pieces of Symantec Workflow” on page 184.

**Pieces of Symantec Workflow**

When you install Symantec Management Platform in your environment, the Symantec Workflow Installer is installed on the platform server. You find the installer in the console under Manage > Workflows.

Workflow comprises the following pieces of software that you install as you run the Workflow Installer:

- Workflow Manager and Workflow Designer
- Workflow Server
- Process Manager
- Client tools
Table 13-1  Pieces of Workflow

<table>
<thead>
<tr>
<th>Piece</th>
<th>Description</th>
</tr>
</thead>
</table>
| Symantec Workflow  | The Symantec Workflow installer is installed with the Symantec Management Platform server.  
The best practice is to download the installer and run it on a separate server computer that has Windows Server installed on it. The installer is an executable file that you run on the computer on which you want to install Workflow.  
In Symantec Management Console, you can view Workflow reports. Workflow integrates Workflow Designer and Workflow Server with the platform. This integration lets Workflow interact with Notification Server, the central piece of the platform. Integration also lets Workflow interact with the suites that run on the platform. In this example, a Workflow process can cause Notification Server to create the tasks that the installed suites can use.  
| Workflow Manager   | Workflow Manager is the repository of Workflow projects and the starting point for creating and modifying projects.  
Workflow Manager lets you create, edit, open, and manage projects. Workflow Manager also lets you configure certain project settings; for example, you can manage tool preferences and computer information. These settings are available in the **Tools** menu. |
| Workflow Designer  | Any time you open or create a project, that project opens automatically in the Workflow Designer piece of Symantec Workflow. Workflow Designer is the tool that you use to design Workflow projects, which are typically a series of connected processes. The Designer contains pieces of the code that are called components. You use these components to build processes and connect them into a single project that you publish to Workflow Server.  
You should install Workflow Designer on a computer other than the Symantec Management Platform host. |
Table 13-1  Pieces of Workflow (continued)

<table>
<thead>
<tr>
<th>Piece</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Workflow Server</strong></td>
<td>Workflow Server is not a standalone server computer; rather, it is a process that runs in the background of each Workflow piece that you install. Workflow Server manages published workflow projects. It is the execution engine (or runtime engine) for all published processes. Workflow Server is automatically installed on any computer with Workflow Designer. A common installation scenario is to install Process Manager, Workflow Manager, and Workflow Designer on a designated server computer. You should install Workflow on any server to which you want to publish workflow projects. You can install on a designated server, on your local server, or both.</td>
</tr>
</tbody>
</table>
| **Process Manager** | The Process Manager piece of Workflow is a Web portal for managing the various parts of a workflow process. These parts include tasks, documents, data, and so on. You use Process Manager to interact with and manage the published processes that include human interaction. Process Manager can be integrated with Active Directory for user authentication, proper access control, and user management. The following list describes some of the functions of Process Manager:  
  - Lets you view and manage tasks.  
  - Lets you view reports on the processes that are running.  
  - Lets you store documents, articles, and schedules to share.  
  - Lets you change pages, symbols, Web parts, and so on to create an interface that works for you.  
  - Lets you add new pages to Process Manager that embed Process Manager content or content from the Web or other servers. Process Manager should be installed on a central Process Manager server. |


Table 13-1  Pieces of Workflow (continued)

<table>
<thead>
<tr>
<th>Piece</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client tools</td>
<td>Workflow client tools are support applications for Workflow.</td>
</tr>
<tr>
<td></td>
<td>The following client tools are available:</td>
</tr>
<tr>
<td>■ Business TimeSpan Editor</td>
<td>Manages the information about the work hours and holidays for your organization.</td>
</tr>
<tr>
<td>■ Credentials Manager</td>
<td></td>
</tr>
<tr>
<td>■ Critical Errors Viewer</td>
<td></td>
</tr>
<tr>
<td>■ License Status Manager</td>
<td></td>
</tr>
<tr>
<td>■ Local Machine Info Editor</td>
<td></td>
</tr>
<tr>
<td>■ Log Viewer</td>
<td></td>
</tr>
<tr>
<td>■ Messaging Console</td>
<td></td>
</tr>
<tr>
<td>■ Screen Capture Utility</td>
<td></td>
</tr>
<tr>
<td>■ Server Extensions Configurator</td>
<td></td>
</tr>
<tr>
<td>■ Task Tray Tool</td>
<td></td>
</tr>
<tr>
<td>■ Tool Preferences Editor</td>
<td></td>
</tr>
<tr>
<td>■ Web Forms Theme Editor</td>
<td>Lets you create new themes for the Web forms that you can use in form components (for example, Form Builder).</td>
</tr>
<tr>
<td>■ Workflow Explorer</td>
<td></td>
</tr>
</tbody>
</table>

You do not need to install all of the pieces of Workflow on the same computer. For information about installation configuration in your organization, see the Symantec Workflow User Guide.

See “About Symantec Workflow integration with UNIX and Linux clients” on page 182.

**What you can do with Symantec Workflow**

You can use Workflow to create and implement an endless number of workflows to automate business processes. You can create applications for a variety of purposes. You can monitor hardware or software systems, manage communication, and manage data analysis and delivery from databases or other sources. You can also execute complex logic and use the functions of other tools (including any Web service).

In many cases, business processes may be specific to UNIX or Linux systems. In other cases, processes are OS-agnostic. You can use the same Workflow project to run UNIX and Linux devices that you use to run Windows devices. You use the
same workflow by making decisions in a Workflow process to call the agents to run a Workflow task.

The ability to manage human interactions in a business process is one of the most useful functions of Workflow. You can insert human interaction points in key places while you leverage the data and existing solutions that are available through the Symantec Management Platform. A component in the Workflow process controls each point of interaction with a person or a technology. This interaction can include communicating with a database or creating a task in Process Manager or SharePoint. It can also include almost any supporting or third-party technology necessary to accomplish the goal.

You can create the applications that work with Process Manager. Your applications can work with many of the parts of Process Manager. For example, you can use task management, knowledge base, document management, scheduling, reporting, workflow tracking, and user management with Process Manager. You can create a Workflow project and publish it to Process Manager so you can invoke it and manage it in Process Manager. You can set up Workflow projects to create tasks in Process Manager that users see in their task lists. You can also manage servers.

### Table 13-2  What you can do with Symantec Workflow

<table>
<thead>
<tr>
<th>Use case</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make data actionable.</td>
<td>Almost every enterprise-level application creates thousands of records of data. Use Workflow to manage that data by exception within a defined process.</td>
</tr>
<tr>
<td>Automate manual tasks.</td>
<td>Use Workflow as a run book to automatically execute scripts, procedures, Web services, or tasks to reduce manual effort.</td>
</tr>
<tr>
<td>Extend an existing application</td>
<td>Use Workflow to create and manage specific access to an existing application beyond the application's intended uses.</td>
</tr>
<tr>
<td>Integrate disparate user groups and applications.</td>
<td>User groups include administrators and end users. Use Workflow to integrate several disparate user groups and applications to transform a series of discrete products into a single, comprehensive business solution.</td>
</tr>
<tr>
<td>Control processes.</td>
<td>Use the Workflow auditing and reporting framework to integrate control and accountability into your IT security and business processes.</td>
</tr>
</tbody>
</table>

See “About Symantec Workflow integration with UNIX and Linux clients” on page 182.
Executing scripts on UNIX and Linux systems through SSH

You can execute scripts on a UNIX or Linux system by using a Secure Shell (SSH) rather than Symantec Management Platform. Running scripts through SSH is not secure like executing tasks through an agent is. For this reason it is not a best practice; however, in some cases you may need to use this method.

See “About Symantec Workflow integration with UNIX and Linux clients” on page 182.

**Warning:** Use this method with caution. Use it only if you must execute scripts and no agent is available to do so.

The following options let you run scripts:

- Execute Symantec Management Platform tasks from within Workflow.
  In a Workflow project, you call a task. That task can run on client computers on any platform, including UNIX and Linux.
  See "Working with tasks" in the *Symantec Workflow User Guide*.

- Run scripts directly through SSH.
  You can run dynamic commands against a UNIX or Linux server from a Workflow process. The commands are run using the SSH protocol by the command-line plink.exe from Quest. This method secures all communications between the Workflow and UNIX servers.
  The following procedure describes how to run a UNIX command on the target server, illustrating the flexibility of Workflow to interact with non-Windows environments.

**To run scripts through SSH**

1. On the Workflow Server computer, download the Putty 0.60_q1.129 MSI file from the following location:
   
   [http://rc.quest.com/downloads.php?release=Quest-PuTTY-0.60_q1](http://rc.quest.com/downloads.php?release=Quest-PuTTY-0.60_q1)

   This installer lays down plink.exe and starts the installation wizard automatically. The plink executable file is a command-line SSH tool through which you can run SSH commands from Workflow.

2. Complete the installation wizard.

3. Browse to `C:\Program Files\Quest Software\PuTTY` and check that the version of the plink.exe file is correct. To check the file, right-click it and then click **Properties**. On the **Details** tab, next to **Product version** you see the product version listed.
4 Copy the location of the plink file, open a command prompt, and change the
directory to the location of the plink file. Enter `plink <user name of the unix
computer that I want to have a trusted connection with>@<IP address>`
into the command line to register the computer as a trusted connection.

5 After the command prompt, enter `y`. Entering the `y` command stores the key
in the cache and adds the computer as a permanent trusted connection. If you
initiate a non-interactive session, enter this command for any server with which
you want to create a trusted connection.

6 In Workflow Manager, click **File > New** to create an empty Web forms project
and build your workflow.

7 After you build the workflow, add a **Merge Text** component. This component
lets you merge all of the information that your workflow collects into a plink
command line.

8 Name the component, and next to **Merge Data** click the ellipses (…). In the
**String Formatter**, enter the following text and click **OK**:

```
-plink <Server IP variable> -l <User Name variable> -pw <Server Password
variable> -no_in <Command variable>
```

You enter `-no_in` so that the workflow does not pass in any standard input. If
you use this command and have the wrong version of plink, you receive an
error message when you attempt to run this workflow.

9 Continue building the workflow. Then debug it and publish it.

When you use this method, ensure that each app pool user is given rights to
run plink.exe from its location on the Workflow Server.

---

**About Process Manager reporting**

Symantec Workflow includes a built-in auditing and reporting framework. The
reporting feature in Process Manager lets users access Process Manager data in
the form of predefined reports. Users can also create custom reports.

**Note:** If you want to report about something in the Symantec Management Platform
infrastructure, use the platform reporting capability that is found in Symantec
Management Console. The Workflow reporting framework that is built in to Process
Manager reports about the state and status of Workflow projects.

The main Process Manager reporting features are as follows:

- The predefined reports that are installed with Process Manager meet the ITIL
  needs of many users.
■ Predefined reports can be easily customized by copying a report and changing a few items so that the new report meets your exact needs.

■ A wizard interface is used to create new reports. The wizard eliminates the need to use SQL for report creation. All reports can be included on portal pages and dashboards, and the size and placement of the report is customizable by the administrator.

■ During report creation, you can add run-time filters to the report definition. Run-time filters allow users to scope the reports based on the data that they want to see.

■ All reports can be configured to represent Process Manager data in a graphical format.

Reports are easily customizable and can contain any Process Manager data.

For information about using the reporting feature, see the chapter titled "Reporting in Process Manager" in the *Symantec Workflow User Guide*
Centralized management

- Chapter 14. Topology View
- Chapter 15. Remote Management
- Chapter 16. Package server for Linux
This chapter includes the following topics:

- About Product Name Portal page
- Viewing the Server Management Suite Portal page
- About Topology View Web Part
- Topology View Web part options
- Viewing network topology
- Topology View Web part options

About Product Name Portal page

Product Name Portal page consolidates the key information about your network resources into a single view. The Web parts on the Product Name Portal page let you monitor the state of your computers and view the inventory data. You can check the status of the recent software deliveries and find out the number of software patches that need to be addressed. The network topology diagram provides you with an overview of the physical structure of your network.


You can customize the Product Name Portal page according to your preferences. You can edit and remove the predefined Web parts, or you can create new Web parts.

Viewing the Server Management Suite Portal page

Server Management Suite Portal page consolidates the key information about your network resources into a single view. It contains different predefined Web parts.
The Web parts on the Portal page let you monitor the state of your computers and view the inventory data. For example, you can check the status of the recent software deliveries and find out the number of the Microsoft patches that need to be addressed. The network topology diagram provides you with an overview of the physical structure of your network.

### Table 14-1  Default Web parts on the Server Management Suite Portal page

<table>
<thead>
<tr>
<th>Web part</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Event Console</strong></td>
<td>Event Console provides a consolidated view of all alerts that are raised. Event Console is part of the Server Management Suite, Client Management Suite, and IT Management Suite.</td>
</tr>
<tr>
<td><strong>Monitored Resources by Status</strong></td>
<td>The chart on this Monitor Solution Web part shows the severity status of all monitored resources. In the devices list you can select a computer and launch the Performance Viewer, the Resource Manager, or the Event console.</td>
</tr>
<tr>
<td><strong>Topology View</strong></td>
<td>This Web part provides a network topology diagram of the SNMP-enabled devices that are found in your network. Topology View Web part displays the data that you collect using Network Discovery tasks. See “Viewing network topology” on page 196.</td>
</tr>
<tr>
<td><strong>Group View - Aggregate health by resource</strong></td>
<td>This Web part shows the aggregate health of the devices and computers in your organizational groups. The Group View is installed as a part of the Monitor Solutions.</td>
</tr>
<tr>
<td><strong>How current is my computer inventory?</strong></td>
<td>This Web part of the Inventory Solution displays a graph that shows how many computers have reported inventory in a specified period of time. You can edit the period of the time that you want reported.</td>
</tr>
<tr>
<td><strong>Recent Software Delivery Status</strong></td>
<td>This Web part of the Software Management Solution lists all software deliveries and their status. Following delivery types are displayed: Managed Software Delivery, Quick Delivery, Package Delivery, and Legacy Software Delivery.</td>
</tr>
<tr>
<td><strong>Microsoft Vulnerabilities</strong></td>
<td>This graph reports the number and the severity of the Microsoft patches that need to be addressed. The Microsoft Vulnerabilities graph is a Web part of the Patch Management Solution.</td>
</tr>
</tbody>
</table>
To view the Server Management Suite Portal page

1. In the Symantec Management Console, on the Home menu, click Server Management Suite Portal.

2. View the Web parts.

3. (Optional) To customize the Server Management Suite Portal page, click Edit.
   You can edit or remove the predefined Web parts, or you can create new Web parts.

About Topology View Web Part

The Topology View Web Part provides a view of the SNMP-enabled network devices and the physical organization of your network. You see the status of all the network devices that are connected to your network and you can access the reports of each device.

Icons on the topology diagram let you identify the different SNMP-enabled network devices that are found. Labels on the icon indicate the status of each device. You can double-click the icon of the device to open the Event Console. When you right-click the icon, you can access other reports of the device and run different tasks.

In the Topology View Web Part you can create groups and maps to document the network, troubleshoot the subnets, or plan infrastructure expansions.

To view the topology diagram in the Topology View Web Part, select the root device for the network topology. Before you can select a device, you must collect the data about the SNMP-enabled devices on your network. Use the Network Discovery task to discover your network resources. Make sure that the connection profile of the Network Discovery task has the SNMP turned on.

Network Discovery lets you find routers, switches, hubs, network printers, Novell NetWare servers, and the computers that are running Windows, UNIX, Linux, and Mac. The collected data is saved in the Configuration Management Database (CMDB).

**Note:** The Topology View Web Part does not display the SNMP-enabled devices that are discovered with the single device discovery task. When you create a Network Discovery task to collect the data for the Topology View Web Part, you must set the range of the IP addresses that you want to discover.

The Topology View Web Part is installed as a part of the Product Name.

See “Viewing network topology” on page 196.
Topology View Web part options

The Topology View Web part provides you with a quick overview of your network. On the topology diagram you see all the SNMP-enabled devices that are discovered on your network and the status of each device.

Table 14-2 Options on the Topology View Web part

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root device</td>
<td>Lets you set any device of infrastructure type that is found in your network, as a root device for the topology view.</td>
</tr>
<tr>
<td></td>
<td>When you click Select root device, the list of network devices available for selection as a root device is displayed. You can filter and search</td>
</tr>
<tr>
<td></td>
<td>devices and set any of them as a root device. The layout of the network is rearranged according to the selection.</td>
</tr>
<tr>
<td>Open</td>
<td>Lets you select and display previously saved views.</td>
</tr>
<tr>
<td>Save</td>
<td>Lets you save the settings and topology layout of the current view. Type a descriptive name that helps you easily identify the view in the future.</td>
</tr>
<tr>
<td>Levels</td>
<td>Lets you select the depth of levels to display. The drop-down list gets filled dynamically, according to the number of levels of the actual network.</td>
</tr>
<tr>
<td>Display</td>
<td>Lets you hide or show different types of network devices.</td>
</tr>
<tr>
<td>Screen</td>
<td>Lets you display the Topology View Web part in the full screen mode.</td>
</tr>
<tr>
<td>Search device</td>
<td>Lets you search devices by name or IP address. After you type the item to search for in the Search device box, the view is refreshed automatically.</td>
</tr>
</tbody>
</table>

See “Viewing network topology” on page 196.


Viewing network topology

The Topology View Web part provides a view of the SNMP-enabled network devices and the physical organization of your network. You see the status of all the
network devices that are connected to your network and you can access the reports of each device.

Icons on the topology diagram let you identify the different SNMP-enabled network devices that are found. Labels on the icon indicate the status of each device. You can double-click the icon of the device to open the Event Console. When you right-click the icon, you can access other reports of the device and run different tasks.

In the Topology View Web part you can create groups and maps to document the network, troubleshoot the subnets, or plan infrastructure expansions.

Before you can view the topology diagram, you must collect the data about the SNMP-enabled devices on your network. Use the Network Discovery task to discover your network resources. Network Discovery lets you find routers, switches, hubs, network printers, Novell NetWare servers, and the computers that are running Windows, UNIX, Linux, and Mac OS X. The collected data is saved in the Configuration Management Database (CMDB). Make sure that the connection profile of the Network Discovery task has the SNMP turned on.

**Note:** The Topology View Web part does not display the SNMP-enabled devices that are discovered with the single device discovery task. When you create a Network Discovery task to collect the data for the Topology View Web part, you must set the range of the IP addresses that you want to discover.

The Topology View Web part is installed as a part of the .

To view network topology

1. In the Symantec Management Console, on the Home menu, click Portal.
2. On the Topology View Web part, click Select device and select the root device for the network topology.
3. (Optional) Edit the settings of the network topology view. After you make the changes, you can save the network topology view for further use.

   See “Topology View Web part options” on page 197.


**Topology View Web part options**

The Topology View Web part provides you with a quick overview of your network. On the topology diagram you see all the SNMP-enabled devices that are discovered on your network and the status of each device.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root device</td>
<td>Lets you set any device of infrastructure type that is found in your network, as a root device for the topology view. When you click <strong>Select root device</strong>, the list of network devices available for selection as a root device is displayed. You can filter and search devices and set any of them as a root device. The layout of the network is rearranged according to the selection.</td>
</tr>
<tr>
<td>Open</td>
<td>Lets you select and display previously saved views.</td>
</tr>
<tr>
<td>Save</td>
<td>Lets you save the settings and topology layout of the current view. Type a descriptive name that helps you easily identify the view in the future.</td>
</tr>
<tr>
<td>Levels</td>
<td>Lets you select the depth of levels to display. The drop-down list gets filled dynamically, according to the number of levels of the actual network.</td>
</tr>
<tr>
<td>Display</td>
<td>Lets you hide or show different types of network devices.</td>
</tr>
<tr>
<td>Screen</td>
<td>Lets you display the <strong>Topology View</strong> Web part in the full screen mode.</td>
</tr>
<tr>
<td>Search device</td>
<td>Lets you search devices by name or IP address. After you type the item to search for in the <strong>Search device</strong> box, the view is refreshed automatically.</td>
</tr>
</tbody>
</table>

See “Viewing network topology” on page 196.

Remote Management

This chapter includes the following topics:

- Methods for remotely managing UNIX/Linux servers
- About Server Resource Manager Home page
- Accessing the Server Resource Manager Home page

Methods for remotely managing UNIX/Linux servers

You can remotely manage UNIX and Linux servers using a variety of tools and methods.

<table>
<thead>
<tr>
<th>Remote management method</th>
<th>Description</th>
<th>Integrated with Symantec Management Platform?</th>
</tr>
</thead>
<tbody>
<tr>
<td>VNC (Virtual Network Computing)</td>
<td>You can install VNC on your remote computer and then use it to connect to a host computer. In the console, go to Actions &gt; Remote Management &gt; Remote Control. From the Connect using drop-down list, select VNC server.</td>
<td>Yes</td>
</tr>
<tr>
<td>DRAC (DELL remote access controller) card</td>
<td><a href="http://www.symantec.com/docs/HOWTO63438">http://www.symantec.com/docs/HOWTO63438</a></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.symantec.com/docs/HOWTO63437">http://www.symantec.com/docs/HOWTO63437</a></td>
<td></td>
</tr>
</tbody>
</table>
### Table 15-1 Remote management methods (continued)

<table>
<thead>
<tr>
<th>Remote management method</th>
<th>Description</th>
<th>Integrated with Symantec Management Platform?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HP iLO</strong></td>
<td>iLO stands for 'integrated Lights-Out' and is a hardware interface available in HP systems to remote control servers.</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>xwindows, telnet, ssh</strong></td>
<td>You can add these and other remote control options to the console through user-defined right-click actions. For more information, see the knowledge base article <em>Adding user-defined actions to the context menu</em> at the following URL: <a href="http://www.symantec.com/docs/HOWTO62815">http://www.symantec.com/docs/HOWTO62815</a></td>
<td>Possible</td>
</tr>
<tr>
<td><strong>vPro</strong></td>
<td>Covered by Altiris Real-Time System Management. For more information, see the <em>Altiris™ Real-Time System Management User Guide</em></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Symantec pcAnywhere Solution</strong></td>
<td>Requires the installation of an agent on the UNIX/Linux server. For more information, see the <em>Symantec pcAnywhere Solution User Guide</em> at the following URL: <a href="http://www.symantec.com/docs/DOC5394">http://www.symantec.com/docs/DOC5394</a></td>
<td>Yes</td>
</tr>
</tbody>
</table>

### About Server Resource Manager Home page

The **Server Resource Manager Home** page consolidates the most relevant inventory and monitoring data of a server resource into a single view.

On the **Server Resource Manager Home** page you see the attributes of the server, and current disk utilization for all attached disks. You can view the different health and performance reports of your server. For example you can view the reports of processor, physical memory, disk I/O, network bandwidth, and disk space utilization.

The Web parts display the data in real time or for the last 24 hours. The real-time data is received directly from the managed computer. The historical data is taken from the Configuration Management Database (CMDB). When you want to see the report for longer than 24-hour period, click the historical diagram.
The Server Resource Manager Home page lets you also access all the functions that are available in the Resource Manager.

You can access the Server Resource Manager Home page from the Resource Manager.

See “Accessing the Server Resource Manager Home page” on page 201.

The Server Resource Manager Home page is installed as a part of the Product Name.

To gather the data for the Web parts that are displayed on the Server Resource Manager Home page, you must install the following agent and plug-ins on the target computers:

- Symantec Management Agent
- Inventory Plug-in
- Monitor Plug-in

You need to enable an Inventory policy and the Windows Server Performance Health Monitor Policy and assign them to a resource before the Server Resource Manager Home page is populated.

Accessing the Server Resource Manager Home page

The Server Resource Manager Home page consolidates the most relevant inventory and monitoring data of a server resource into a single view.

Different reports let you easily check and ensure that any of your Windows, UNIX, or Linux servers functions properly. On the Server Resource Manager Home page you see the attributes of the server, and current disk utilization for all attached disks. You can view the different health and performance reports of your server. For example you can view the reports of processor, physical memory, disk I/O, network bandwidth, and disk space utilization.

The Web parts display the data in real time or for the last 24 hours. The real-time data is received directly from the managed computer. The historical data is taken from the Configuration Management Database (CMDB). When you want to see the report for longer than 24-hour period, click the historical diagram.

To gather the data for the Web parts that are displayed on the Server Resource Manager Home page, you must install the following agent and plug-ins on the target computers:

- Symantec Management Agent
- Inventory Plug-in
Monitor Plug-in

You need to enable an Inventory policy and the **Windows Server Performance Health Monitor Policy** and assign them to a resource before the Server Resource Manager Home page is populated.

The **Server Resource Manager Home** page lets you also access all the functions that are available in the Resource Manager.

When you have selected the **Server Resource Manager View** for a resource, this view is the default view for all resources.

The **Server Resource Manager Home** page is installed as a part of the .

To access the Server Resource Manager Home page

1. In the Symantec Management Console, on the **Manage** menu, click **Resource**.
2. In the **Select Resource** dialog box, select the server resource that you want to manage, and then click **OK**.
3. In **Resource Manager**, in the **Custom View** drop-down list, click **Server Resource Manager View**.
Package server for Linux

This chapter includes the following topics:

■ About package server for Linux
■ About integrating Apache Web Server with package server for Linux
■ About detecting the Apache Web Server
■ Requirements to configure package server and the Apache Web Server
■ Requirements to configure HTTPS and HTTP
■ Package server configuration example that uses main web directory for package server links
■ Package server configuration example using an alias for package server links

About package server for Linux

To designate a Linux computer as a package server, ensure that the computer is running the following software:

■ Symantec Management Agent for UNIX, Linux, and Mac
  Symantec Management Agent for UNIX, Linux, and Mac runs on a managed computer. That agent must match the version of the agent that is installed on the Notification Server computer in Symantec Management Platform. If the agent on the managed computer is older than the agent on Notification Server, upgrade it. After the agent is upgraded, the managed computer can become a package server.

■ Apache Web Server version 2.0 or 2.2
  See “About integrating Apache Web Server with package server for Linux” on page 204.

The following server platforms are supported:
Package server for Linux supports alternate download locations. Paths for alternate locations are converted automatically from Windows style to UNIX style if you include the trailing slash. For example, if you have Patch Management Solution installed, you can change policy and package settings when rolling out patches. In Symantec Management Console, under Settings > All Settings > Software > Patch Management, you click a vendor settings page; for example, you would click Red Hat Settings > Red Hat Patch Remediation Settings. When you click the Policy and Package Settings tab, you see the Remediation Settings page for the selected product. This is where you can check Use alternate download location on Package Server. When you enter the alternate download location, you must use the full Windows path. In this and similar instances, include a trailing slash in the Windows-style path to ensure that it is converted correctly to a UNIX-style path.

Correct:  
C:\path\  
Trailing slash means that the Windows path is converted correctly to /path/.

Incorrect:  
C:\path  
If you omit the trailing slash, the Windows path is converted incorrectly.

About integrating Apache Web Server with package server for Linux

You integrate package server for Linux with the Apache Web Server to expose packages and Package Snapshots to Symantec Management Agent. Snapshots are downloaded from Notification Server to Symantec Management Agent on all supported platforms through HTTP URLs.

See “About package server for Linux” on page 203.

The packages and package snapshots are always downloaded to package server directories. The only files that are created in the Apache Web Server are directories, symbolic links, and .htaccess files. Symbolic links are created to the package files and snapshot files. The .htaccess files lock down package files with passwords.

When a Linux computer becomes a package server, the agent on that computer attempts to create an HTTP share in the Apache Web Server virtual web space.
The Package Manifest file is not used when a package server for Linux downloads a package for distribution. The exception is if the package is located in the same directory for the package server for Linux and Software Delivery. All package file permissions are set to allow Apache Web Server clients access. This access is typically through 0x744.

Depending on the specific configuration of the Apache Web Server, directories are created in the root of the web directory. An example is /var/www/html on a typical Linux Red Hat system. The package server agent reads the Apache Web Server configuration file to determine this location.

See “About detecting the Apache Web Server” on page 205.

If you choose, you can specify that package server create the directories in an alternate location. Use an Apache Web Server alias directive to specify a separate directory.

See “Requirements to configure package server and the Apache Web Server” on page 206.

See “Requirements to configure HTTPS and HTTP” on page 207.

About detecting the Apache Web Server

You can detect the Apache Web Server automatically or manually.

See “About integrating Apache Web Server with package server for Linux” on page 204.

See “Requirements to configure package server and the Apache Web Server” on page 206.

If you choose Automatic Detection, Symantec Management Agent looks for the Apache HTTPD or HTTPD2 executable in the following directory locations:

- /bin:/usr/bin:/sbin:/usr/sbin:/usr/lbin:/usr/etc:/etc:/usr/bsd:/usr/local/bin:/usr/contrib/bin/
- System PATH variable
- /opt/apache/bin:/usr/apache/bin:/usr/apache2/bin:/usr/local/apache/bin:/usr/local/apache2/bin:/usr/local/bin:/opt/freeware/apache/bin:/opt/freeware/apache2/bin:/opt/freeware/apache/sbin:/opt/hpws/apache/bin:/opt/apache2:/usr/local/apache+php

If both HTTPD and HTTPD2 executables are found, then both Apache 2.0 and Apache 2.2 are installed.

In addition, if both executable files are found, then the file that matches a running process is used. The default file is HTTPD2.
If the Apache Web Server cannot be detected automatically, you may need to detect it manually. The Apache Web Server might not be detected automatically if the executable file is renamed. If multiple installations have occurred, then the wrong Apache Web Server could be detected. In any of these situations, you should specify the Apache Web Server location manually.

To specify the Apache Web Server manually you should edit the [httpd Integration] section of the client.conf file in the agent. In this section, you should specify the "apache_exe_location" setting.

When the Apache Web Server executable is located, it is used to determine the default location of the Apache Web Server configuration file. The configuration file is required to determine if the Apache Web Server setup is suitable for package server use. The configuration file also lets the installation program determine the settings that are applicable to the package server. Applicable settings include the ports that are used or whether the server is SSL-enabled.

If Symantec Management Agent for UNIX, Linux, and Mac cannot find the Apache Web Server configuration file, it searches in the following locations:

- /etc/httpd/conf
- /etc/httpd/2.0/conf

As an alternative to Automatic Detection you can edit the [Httpd Integration] section of the Symantec Management Agent for UNIX, Linux, and Mac client.conf file. When you edit the file, specify the apache_config_location. Any setting that you change becomes the default.

You can use the Apache Web Server "-f" option during the installation to relocate the configuration file from its default location. If you relocate the file, you must specify the location of the apache_config_location. Package server for Linux does not support mod_perl generated httpd.conf files.

### Requirements to configure package server and the Apache Web Server

For the package server for Linux to work with the Apache Web Server, certain requirements must be met. When these requirements are met, the Symantec Management Agent for UNIX, Linux, and Mac sends the Apache HTTP Server role. This role allows the computer to be used as a package server for Linux.

See “About detecting the Apache Web Server” on page 205.

The configuration requirements are as follows:

- Apache Web Server version 2.0 or 2.2 is installed.
The package server for Linux uses only the main Apache Web Server or the default Apache Web Server. All other virtual host sections in the Apache Web Server configuration are ignored, with the following exceptions:

- The global settings and the _default_ virtual host are read for the main server settings.
- The first virtual host that defines an SSL server is considered to be the main SSL server. Its settings are used for integrating and all other SSL virtual hosts are ignored.

The Apache Web Server web space location where the package server files and directories are to be created must have the following options enabled:

- FollowSymLinks
- AllowOverride

The usage of HTTP and/or HTTPS for the Apache Web Server depends on the **Published Codebase Types** value defined as part of the **Package Service Settings** for the Notification Server.

- Non-standard ports are detected and used, but the main Apache Web Server must be accessible through the hostname of the computer. The **Listen** directive for the main server must come before all other **Port** statements and Listen directives in the configuration file.
- The Apache Web Server must be running.
- No compressing modules are used with the Apache Web Server. This requirement exists because Package Delivery does not support those modules.
- You may need to restart Symantec Management Agent for UNIX, Linux, and Mac after you make changes to the httpd.conf file. The files may not take effect until after you restart the agent.

### Requirements to configure HTTPS and HTTP

Symantec Management Agent for UNIX, Linux, and Mac uses whichever type of Apache Web Server is available. It can use either HTTP or HTTPS.

See “Requirements to configure package server and the Apache Web Server” on page 206.

If the Apache Web Server supports both types of Web server, the package server for Linux uses HTTPS. Integrating with SSL through HTTPS is the default option because it is the most secure. If you want to use the HTTP server, you can change the [httpd Integration] "integrate_with" setting.
Table 16-1  Recommended approaches for installing the Apache Web Server to support package servers for UNIX and Linux

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install a packaged version of Apache Web Server. On Linux, the distributed Apache Web Server is most suitable.</td>
<td>This installation contains the executable files and the technical support exe files in /usr/sbin or /usr/bin.</td>
</tr>
<tr>
<td>Install the Apache Web Server package in the recommended location.</td>
<td>An example of a suitable default location is /usr/local or /opt.</td>
</tr>
<tr>
<td>Leave the Configuration directory in its default location. This requirement ensures that Symantec Management Agent for UNIX, Linux, and Mac can easily detect the Apache Web Server and the configuration file. If you do not move the configuration directory, you do not have to specify extra manual settings.</td>
<td>The default configuration directory is the location that was compiled into your .exe, or /etc/httpd/conf.</td>
</tr>
</tbody>
</table>

If you change the Apache Web Server configuration files while Symantec Management Agent is running, data is sent to Notification Server after a short time. After the Apache Web Server role data is sent to Notification Server, the computer becomes a candidate package server. If you want to speed up this process you should run the `aex-sendbasicinventory` executable file manually. Run the executable file from the shell on the client computer that is targeted for the package server installation. Update Notification Server with the changes.

Two configuration examples are available.

See “Package server configuration example that uses main web directory for package server links” on page 208.

See “Package server configuration example using an alias for package server links” on page 211.

Package server configuration example that uses main web directory for package server links

This configuration generally requires the minimal modification to an out-of-the-box or default Apache Web Server setup. In this configuration a virtual directory that is called `/Altiris/PS` is created automatically under the main Apache HTML directory.

See “Requirements to configure HTTPS and HTTP” on page 207.

The example configuration contains the `Packages` directory.
Symbolic links are created in these directories to each shared package. The packages themselves are stored under the package server agent VAR directory. This configuration includes both an HTTP and an HTTPS Apache server. The package server uses the HTTPS server if it is available. The HTTPS server ensures a more secure operating environment and allows the use of Package Access credentials.

Several configuration file checks are performed. The configuration files that are listed in this section are examples. These examples are from the default installation of the Apache Web Server as part of a legacy Red Hat Linux Distribution.

**Check number 1; Listen statement** is as follows:

```bash
...## When we also provide SSL we have to listen to the ## standard HTTP port (see above) and to the HTTPS port ## <IfDefine HAVE_SSL>
Listen 80 Listen 443 Listen 10.10.10.10:8080 </IfDefine>...
```

Ensure that the Listen statement for each of the main servers is the first Listen statement of its type in the configuration file. The main HTTP and HTTPS servers should be the first two Listen statements.

You should remove the IP or ensure that it is the same IP to which the hostname resolves, as reported to Notification Server.

**Check number 2; Main directory options** is as follows:

```bash
...

# DocumentRoot: The directory out of which you will serve your Notification Server Reference 62
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
DocumentRoot "/var/www/html" ...

# This should be changed to whatever you set DocumentRoot to.
#<Directory "/var/www/html">
# This may also be "None", "All", or any combination of "Indexes", # "Includes", "FollowSymLinks", "ExecCGI", or "MultiViews".
# Note that "MultiViews" must be named *explicitly* --- "Options All" # does not give it to you.
Options Indexes FollowSymLinks
# This controls which options the .htaccess files in directories can
Find the `<Directory>` node for the `DocumentRoot` directory, and ensure that the following options are set:

- `FollowSymLinks`
- `AllowOverride AuthConfig` or `Allow override All`

**Check number 3; Check SSL host** is as follows:

```
## SSL Virtual Host Context
<VirtualHost _default_:443>
  # General setup for the virtual host
  DocumentRoot "/var/www/html"
  ErrorLog logs/error_log
  TransferLog logs/access_log
  Notification Server Reference 63
  # SSL Engine Switch:
  # Enable/Disable SSL for this virtual host.
  SSLEngine on

... 
```

Ensure that the `_default_` SSH Virtual host has the correct port. The port should match the first SSH Listen. Ensure that the `DocumentRoot` of the virtual host is the same as the `DocumentRoot` of the main server.

The `DocumentRoot` of the host can be different from the `DocumentRoot` of the main server. The `DocumentRoot` of the host must have a `<Directory>` node that is configured with the same options that are specified in Check number 2.
Package server configuration example using an alias for package server links

You may want to keep the package server for Linux virtual directory completely separate from the Apache Web Server directory. To keep them separate, follow this configuration example. This configuration example keeps all the symbolic links out of the main Apache Web Server directory. It ensures that the FollowSymLinks options are not required in the main directory.

See “Requirements to configure HTTPS and HTTP” on page 207.

An alias is used in the Apache Web Server configuration file to separate the `/Altiris/PS` virtual directory. The package server for Linux automatically detects this alias and creates the required subdirectories in the correct location.

The subdirectories are as follows:

- Packages
- Snapshots

The actual packages are downloaded to the `VAR` directory on the agent.

The configuration files that are used in this section are an example. The example is from the default installation of the Apache Web Server as part of a legacy Red Hat Linux Distribution.

The Check number 1; Listen statement is as follows:

```bash
...## When we also provide SSL we have to listen to the
## standard HTTP port (see above) and to the HTTPS port
##
<IfDefine HAVE_SSL>
Listen 80
Listen 443
Listen 10.10.10.10:8080
</IfDefine>
...
```

Ensure that the Listen statement for each of the main servers is the first Listen statement of its type in the configuration file. The main HTTP and HTTPS servers should be the first two Listen statements.

You should remove the IP or ensure that it is the same IP to which the hostname resolves, as reported to Notification Server. You can use port numbers other than
80 and 443. The package server for Linux detects the ports. However, it always uses the port of the first Listen in the Apache Web Server configuration file.

Check number 2; Create Alias and aliases directory options is as follows:

```
... 
# Aliases: Add here as many aliases as you need (no limit). The format is

# Alias fakename realname 
#

<IfModule mod_alias.c>
...
Alias /Altiris/PS /var/altiris/www/ps 
<Directory /var/altiris/www/ps >
Options FollowSymLinks 
AllowOverride All 
</Directory> </IfModule>

# End of aliases.
```

You should perform these steps in the following order:

- Create both the Alias statement and the `<Directory>` node for the destination directory of the alias.
- Ensure that the following options are set on that directory:
  - `FollowSymLinks`
  - `AllowOverride AuthConfig` or `Allow override All`
- Create the destination directory.
- Set the correct permissions on the destination directory to ensure that Apache Web Server clients can download files from there.
- To ensure that the directory works, place a text file in it. Then browse to a URL such as http://your.server.name/ Altiris/PS/testfile.txt. In this example, your.server.name and testfile.txt are your own server name and the name of the text file that you created.

Check number 3; Check SSL host is as follows:

```
... 
## SSL Virtual Host Context
```
<VirtualHost _default_:443>
  # General setup for the virtual host
  DocumentRoot "/var/www/html"
  ErrorLog logs/error_log
  TransferLog logs/access_log
  # SSL Engine Switch:
  # Enable/Disable SSL for this virtual host.
  SSLEngine on

  Ensure that the _default_ SSH Virtual host has the correct port. It should match the first SSH Listen. Ensure that its DocumentRoot is the same as the DocumentRoot of the main server.
Symbols
6.x software delivery reports 108

A
about
  automation folder 22
adding
  system configuration 32
advanced software delivery. See Managed Software Delivery
aex-bootstrap
  ULM agent manual install 74
agent 101
  See also plug-in
agent registration policy
  creating 70
agent registration request
  allowing 76
  blocking 76
agent registration status
  report 76
agent trust
  about 65
  accept 70
  block 70
  establishing 65
  registration policy 70
  revoking 76
agent-based monitoring
  setting up credentials for 163
  versus agentless monitoring 156
agentless inventory
  about 57
  portal page 62
  task status 62
agentless inventory task (continued)
  viewing status 62
agentless inventory wizard 57, 59
agentless monitoring 148
  about 155
  versus agent-based monitoring 156
agents, used by Software Management Solution 100
alert management
  about 168
alerts
  about 168
  filtering 171
analyzing vulnerabilities. See assessing systems
Apache HTTP server
  gathering inventory 40
application management
  reports 108
application metering reports 45
assessing systems 89
assigning severity levels 93
automation folder
  about 22

B
best practices
  Monitor Solution 166

C
capabilities, of Server Management Suit for
  UNIX/Linux 15
capture
  preparing a disk image 25
collect full server inventory
  running 43
compliance analysis. See system assessment scan
compliance check
  reports 108
computer
  configuring maintenance window 83
  configuring Symantec Management Agent policies 80
computer (continued)
  global agent settings 81
  maintenance window 83
  manually installing Symantec Management
  Agent 67
  Symantec Management Agent for UNIX, Linux,
  and Mac pull installation 73
  targeted agent settings 81
computer, delivery destination. See destination,
delivery
configuring
  Patch Management Solution core settings 94
  severity levels 93
connection profiles
  agentless inventory 57–58
  associating credentials with 164
  discovering resources to bind to 165
Core Services settings
  configuring 94
Create Image
  task options 26
creating
  managed software delivery policy 114
credentials
  associating with a connection profile 164
  for agentless monitoring 163
  protocol-specific 164
custom data class
  about 46
custom inventory
  gathering 48
disk image
  Prepare for Image Capture 25
  preparing to capture 25
distributing software updates
  viewing update summary reports 92
download location 94
E
  ESX servers, deploying 142
  ESXi servers, deploying 142
  Event Console alert filters
    about 169
F
  filescan.rule file
    about 54
    customizing 54
    software inventory 55
H
  historical performance data
    viewing 175
  historical performance viewer 148
host
  adding 126
  discovering 126–127
I
  image
    preparing to capture 25
  implementing
    Software Management Solution 99
import policy
  creating 154
installation settings
  Symantec Management Agent for UNIX, Linux,
  and Mac 72
installing
  Software management solution plug-in 101
  software update plug-in 88
  Symantec Management Agent 66
Inventory
  gathering 42
inventory
  agentless inventory 57
  Apache HTTP server 40
  collecting 43, 89. See system assesment scan
  methods for gathering 38
inventory (continued)
  MySQL and Oracle DB 39
  network devices 59
  of the native UNIX/Linux package system 45
  servers 39
  SNMP devices 57
  software 38
inventory data
  viewing in reports 45
Inventory Pack for Servers
  about 39
Inventory Plug-in
  installing 42
inventory plug-ins
  enabling 42
inventory policies
  predefined 44
inventory reports 45
Inventory Solution
  supported platforms 37
IT Analytics, generating reports with 180

L
Linux 98
  See also UNIX, Linux, and Mac
discovering computers 36
  patching 87
Server Management Suite capabilities 15
  support in Software Management Solution 98
  supported functionality 15
Linux kernel
  patching 94
Linux System Assessment Scan page
  about 89

M
Mac 98
  See also UNIX, Linux, and Mac
  support in Software Management Solution 98
maintenance window
  configuring policy 83
Managed Software Delivery
  about 110
  destination 116
  policy creation 113–114
  wizard 113
managed software delivery policy
  creating 114
Monitor
  report on metrics trends 178
Monitor Alerts dashboard, viewing 177
Monitor Metrics cube, generating reports with 180
monitor packs 148
  components of 151
  downloading custom 155
  importing 154
Monitor Plug-in 148
monitor policies 148
monitor server
  configuring 153
  preparing 153
monitor service
  about 157
  adding to a site server 160
monitor site server
  configuring settings 162
  reports 162
Monitor Solution
  about 147
  best practices, scalability 166
  components 148
  in UNIX/Linux environments 147
Monitoring and Alerting
  home page 173
Monitoring and Alerting home page
  about 173
MySQL and Oracle DB
  inventory 39

N
native package
  ULM agent manual install 76
native package system
  gathering inventory 45
network devices inventory. See agentless inventory
Network Discovery 35
network topology
  saving 196
  viewing 196
network topology diagram
  about 196
  saving 196
  viewing 196
options
  Create Image task 26

Package Delivery
  creating 106
  scheduling 107
Package Server for inux
  configuration examples 208
Package Server for Linux 203
  about 203
  about configuring HTTPS and HTTP 207
  about configuring with the Apache Web Server 206
  about integrating Apache Web Server 204
  detecting the Apache Web Server 205
  supported platforms 203
patch
  installing 91
Patch Management
  differences between platforms 87
Patch Management Solution for Linux
  about 86
  supported platforms 86
patch metadata
  importing 90
  selecting 90
patching
  Linux kernel 94
Platform Support, Software Management Solution 98
plug-in 101
  See also Software Management Solution plug-in
plug-ins, used by Software Management Solution 100
Pluggable Protocols Architecture
  installing 159
policy
  global agent settings 81
  maintenance window policy 83
  targeted agent settings 81
  user-based, software delivery 116
PPA, See Pluggable Protocols Architecture
predefined inventory policies
  cloning 44
  using 44
prepare
  capturing a disk image 25

prerequisites
  Symantec Management Agent for UNIX, Linux,
  and Mac installation 69
Process Manager, reporting 190
Product Name Portal page
  about 193
protocol settings
  agentless inventory task 58
  protocol-specific credentials, creating 164
Quick Delivery
  about 103
  creating 105–106
  process 103
  scheduling 107
  wizard
    creating tasks 105
real-time performance data
  viewing 176
real-time performance viewer 148
remote management
  of UNIX/Linux servers, methods 199
Remote Monitoring Server
  configuring 162
remote monitoring site server
  setting up 157
reports
  generate for Monitor Metrics trends 178
  generating ad-hoc with IT Analytics 180
  Process Manager 190
reports, software
  6.x software delivery 108
  about 108
  application management 108
  compliance check 108
  limiting access to data 108
  running 108
  scoping 108
  software delivery 108
  Software Portal 108
  virtual software 108
resource scoping
  software reports 108
Scoping resources. See resource scoping scripts, executing on UNIX and Linux systems through SSH 189
Sequential software delivery delivering 111
Server applications inventory data 39
Server inventory about 39
Server Management Suite Portal page about 193
accessing 193
viewing 193
Web parts 193
Server Management Suite, capabilities on UNIX/Linux 15
Server Resource Manager about 201
accessing 201
viewing 201
Server virtualization method about 120
Server virtualization technique about 120
Severity levels assigning 93
configuring 93
SMS. See Server Management Suite
Snapshot creating 140
Software channels selecting 90
Software delivery 96, 103, 110
See also Managed Software Delivery
See also Quick Delivery
See also Software Management Solution advanced 110
reports 108
sequential. See sequential software delivery
Software inventory gathering 38
UNIX, Linux, Mac 55
Software Management Solution 108
See also reports, software about 96
implementing 99
key tasks 98
platform support 98
task. See task, Software Management Solution
Software Management Solution agent. See Software Management Solution plug-in
Software management solution plug-in installing 101
upgrading 101
Software Management Solution plug-in, Mac 101
Software Portal reports 108
Software reports. See reports, software running 108
Software update plug-in about 88
installing 88
Software updates viewing update summary reports 92
Software Virtualization task creating 106
scheduling 107
Source Path Update task creating 106
scheduling 107
SSH, executing scripts through 189
Symantec Management Agent about 64
configuring agent policies 80
configuring maintenance window policy 83
global settings 81
installing 66
local settings 81
maintenance window 83
manual installation process 67
targeted settings 81
Symantec Management Agent for UNIX, Linux, and Mac .csv template file 68
creating .csv file for computer details 68
installation requirements 69
manual installation process 67
manual pull installation 73
prerequisites 69
specifying installation settings 72
Symantec Workflow about 184, 187
components 184
on UNIX and Linux 182
System assessment scan configuring 89
System configuration adding 32
System configuration (continued)
settings 32

T
task
  Create Image options 26
task options
  Create Image 26
task, Quick Delivery. See Quick Delivery
task, Software Management Solution
  about 106
  creating 106
  scheduling 107
  selecting computers 107
  types 106
topology view
  customizing 197
  options 197
Topology View Web part
  about 196
  customizing 197
  options 197
  viewing 196

U
ULM agent
  manual install using aex-bootstrap 74
  manual install using native packages 76
UNIX 98
  See also UNIX, Linux, and Mac
discovering computers 36
Server Management Suite capabilities 15
  support in Software Management Solution 98
  supported functionality 15
UNIX, Linux, and Mac
  support in Software Management Solution 98
upgrading, Software management solution plug-in 101
user-based policy
  software delivery 116

V
virtual disk
  creating 138
virtual environment
  creating 130
virtual machine
  creating 131
  discovering 127
  (continued)
  wizard 131
Virtual Machine Management
  about 118
  getting started 124
  permissions required 121
Virtual Machine Management Task Server Plug-in
  installing 125
Virtual Machine Management Task Server Plug-in policy
  installing 125
virtual machines
  gathering inventory 128
virtual network
  creating 139
virtual software
  reports 108
virtualization platforms 118
vulnerability analysis. See system assessment scan

W
what you can do with Symantec Workflow 187
Windows
  Server Management Suite capabilities 15
  supported functionality 15
Windows Installer repair
  scheduling 107
  task
    creating 106