

Veritas CommandCentral™ Storage Migration Guide

for Microsoft Windows and UNIX

5.1



CommandCentral Storage Migration Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 5.1.0

Legal Notice

Copyright © 2008 Symantec Corporation. All rights reserved.

Symantec, the Symantec logo, Veritas, CommandCentral, NetBackup, SANPoint, SANPoint Control, and Storage Foundation are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice documentation accompanying this Symantec product for more information on the Third Party Programs.

- AIX is a registered trademark of IBM Corporation.
- HP-UX is a registered trademark of Hewlett-Packard Development Company, L.P.
- Linux is a registered trademark of Linus Torvalds.
- Solaris is a trademark of Sun Microsystems, Inc.
- Windows is a registered trademark of Microsoft Corporation.
- Oracle is a registered trademark of Oracle Corporation.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

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

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in

Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, 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
20330 Stevens Creek Blvd.
Cupertino, CA 95014
<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 maintenance 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 Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

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

www.symantec.com/techsupp/

Contacting Technical Support

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

www.symantec.com/techsupp/

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

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

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system

- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

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

www.symantec.com/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with 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 maintenance contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

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

Asia-Pacific and Japan	contractsadmin@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Technical Support	4
Chapter 1	CommandCentral Storage migration overview 9
	About migrating CommandCentral Storage 4.x migration to 5.1 9
Chapter 2	Migrating 4.x managed hosts (Agents) to 5.1 13
	About migrating managed hosts 13
	Upgrading high-priority Agent hosts first 15
	Running 4.x Agent hosts with the 5.1 Management Server 15
	The process for upgrading an Agent host 16
	Preparing to upgrade the Agent host 17
	Setting aside disk space 17
	Backing up data and files before migrating 18
	Ensuring compatibility with hardware and with other software 18
	Performing the upgrade on the Agent host 19
	Specifying installation options 19
	Specifying security and authentication options on Windows 20
	Installing the new software 20
	Performing post-upgrade steps on the managed host 20
	Verifying that the upgrade succeeded 21
	Re-enabling Data Module (DM) scans 21
	Verifying configuration settings for the managed host 21
	Closing firewall ports 22
	Disabling the migration explorer on the Management Server 22
Index	25

CommandCentral Storage migration overview

This chapter includes the following topics:

- [About migrating CommandCentral Storage 4.x migration to 5.1](#)

About migrating CommandCentral Storage 4.x migration to 5.1

The *CommandCentral Storage Migration Guide* pertains to upgrading your CommandCentral Storage 4.x storage environment to CommandCentral 5.1.

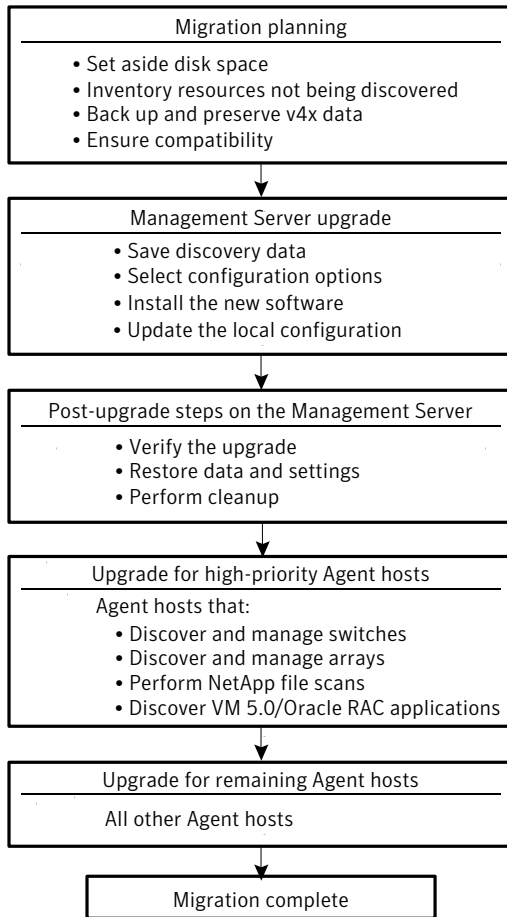
There are several stages to the process of migrating your CommandCentral Storage 4.x storage environment to CommandCentral version 5.1. In brief, you begin by upgrading the Management Server. Then you upgrade each Agent host (managed host).

As you perform the migration, you will use tools that help you preserve your existing configuration (settings and discovery data) and restore it in the new version 5.1 environment.

This *Migration Guide* outlines the migration process and describes each stage in turn.

[Figure 1-1](#) summarizes the stages of the migration process.

Figure 1-1 Summary of the migration process



[Table 1-1](#) lists the migration stages, which are explained in this *Migration Guide*:

Table 1-1 Stages of the CommandCentral Storage 5.1 migration

Stage	Topic
Management Server Migration planning	<p>You cannot upgrade a 4.x Management Server to 5.1. If you want to upgrade a 4.x Management Server to 5.1, you need to first upgrade to 5.0 MP1. To upgrade to 5.0 MP1, refer to the 5.0 MP1 <i>CommandCentral Storage Installation Guide</i> and <i>CommandCentral Storage Migration Guide</i>.</p>
Management Server upgrade	
Post-upgrade steps on the Management Server	
Upgrade of high-priority Agent hosts	<p>Preparing to upgrade the Agent host Performing the upgrade on the Agent host Performing post-upgrade steps on the managed host</p>
Upgrade of remaining Agent hosts	<p>Preparing to upgrade the Agent host Performing the upgrade on the Agent host Performing post-upgrade steps on the managed host</p>

Migrating 4.x managed hosts (Agents) to 5.1

This chapter includes the following topics:

- [About migrating managed hosts](#)
- [Preparing to upgrade the Agent host](#)
- [Performing the upgrade on the Agent host](#)
- [Performing post-upgrade steps on the managed host](#)

About migrating managed hosts

After you upgrade the CommandCentral Management Server to version 5.1, the next step is to upgrade each of the associated managed hosts (Agents) that connect to the Management Server.

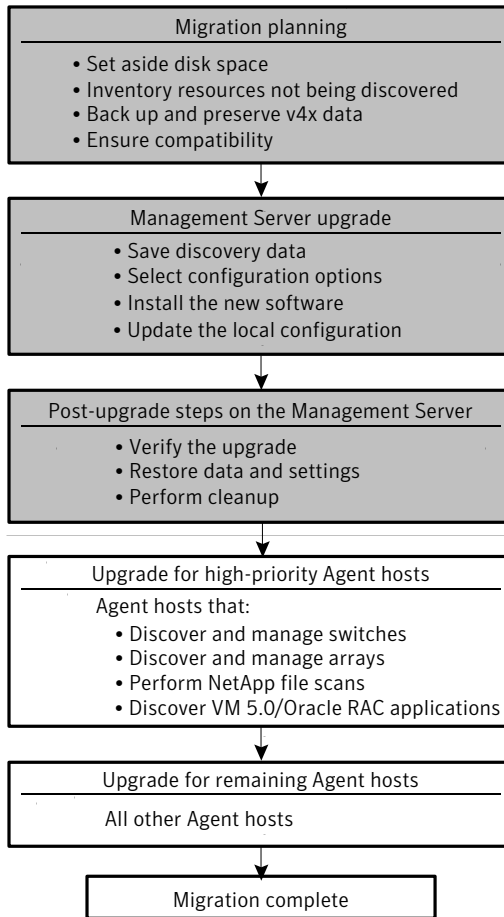
Use the information in this chapter in conjunction with the detailed upgrade procedures.

See the *CommandCentral Installation Guide*.

Note: Throughout this chapter, the term installation routine refers to both the CommandCentral installer (on UNIX hosts) and the CommandCentral Install Wizard (on Windows hosts).

[Figure 2-1](#) shows where you are in the migration process.

Figure 2-1 Migration operations



After upgrading the Management Server to version 5.1, your next task is to upgrade each of the managed hosts (Agents) that interact with the Server.

We strongly recommend that you perform the Agent migration in the following stages:

- First, upgrade high-priority Agent hosts: those requiring functionality that is not provided by the migration explorer on the Management Server, for example switch and array discovery and management. See [“Upgrading high-priority Agent hosts first”](#) on page 15.
- Then, upgrade the rest of your Agent hosts. As you perform these upgrades, there is a transitional period during which the version 5.1 Management Server is interacting with both version 5.1 managed hosts and version 4.x Agent hosts.

See [“Running 4.x Agent hosts with the 5.1 Management Server”](#) on page 15.

The same sequence of steps is used to upgrade every Agent host, regardless of priority.

See [“The process for upgrading an Agent host”](#) on page 16.

A 4.x Agent host that has been upgraded to version 5.1 is known as a managed host.

Upgrading high-priority Agent hosts first

After you upgrade your CommandCentral Management Server to version 5.1, we recommend that you migrate the attached version 4.x Agent hosts as soon as you can. From a practical standpoint, however, there will be a transitional period during which your version 5.1 Management Server is managing a mixture of version 4.x Agent hosts and version 5.1 managed hosts.

You should upgrade your 4.x Agent hosts starting with the ones you use for the following purposes:

- Discovering switches or arrays
- Managing storage, for example creating LUNs and provisioning to hosts
- Managing switches
- Discovering Veritas Veritas Volume Manager 5.0 and Oracle RAC applications
- Performing file scans of NetApp storage devices

The version 5.1 Management Server can perform these functions only by interacting with a version 5.1 managed host. These functions are not provided by the migration explorer.

Only this configuration—when both the Management Server and the managed host are running version 5.1—gives you access to the full set of features associated with the CommandCentral 5.1 product license you have purchased.

Running 4.x Agent hosts with the 5.1 Management Server

Other 4.x Agent hosts—those performing discovery that is supported by the migration explorer on the Management Server—can be upgraded later.

During the transitional period, when a version 5.1 Management Server manages a version 4.x Agent host that has not yet been upgraded, a migration explorer on the Management Server discovers objects attached to the Agent host.

However, some limitations exist when a version 5.1 Management Server manages a version 4.x Agent host.

See the *CommandCentral Storage Release Notes*.

The process for upgrading an Agent host

You can upgrade a 4.x Agent host to version 5.1 from any of the following versions:

- 4.1
- 4.2
- 4.2FP1
- 4.3

The upgrade to version 5.1 is not supported for an Agent host running version 4.0 or earlier. Such a host must be upgraded to one of the supported 4.x releases before you attempt to upgrade it to version 5.1.

The following steps summarize the process of migrating a version 4.x Agent host to a version 5.1 managed host.

- Prepare to upgrade: Ensure that there is sufficient disk space, back up key files, and ensure that the system is ready to upgrade.
See [“Preparing to upgrade the Agent host”](#) on page 17.
- Perform the upgrade: Use the installation routine (either the Install Script on a UNIX host or the Install Wizard on a Windows host) to uninstall version 4.x components and install version 5.1 on the managed host.
See [“Performing the upgrade on the Agent host”](#) on page 19.
- Perform post-upgrade steps: Verify that the upgrade completed successfully and recover local customization that was not upgraded automatically.
See [“Performing post-upgrade steps on the managed host”](#) on page 20.

There is a fundamental difference between version 4.x and version 5.1 in the way connections are defined between a Management Server and an Agent (managed) host. In version 4.x, such a connection was defined by a user who was connected to the Management Server. In version 5.1, however, the connection is defined when you install the managed host.

As a result, the process of upgrading an 4.x Agent host to a 5.1 managed host includes a step where you specify the name of the Management Server to which the managed host will connect.

Review the list of version 4.x features that are no longer supported in version 5.1.

See the *CommandCentral Storage Release Notes*.

Preparing to upgrade the Agent host

Before you begin the upgrade on an Agent host, you must ensure that you have allocated enough disk space. In addition, we strongly recommend that you back up key data and files.

Setting aside disk space

Before you upgrade an Agent host to CommandCentral version 5.1, ensure that there is enough disk space on the host. In addition to the space already dedicated to your version 4.x installation, the upgrade process requires temporary space for storing copies of product code, user data, and installation logs.

[Table 2-1](#) lists the temporary space requirements in addition to the disk-space size requirements for version 5.1.

See the *CommandCentral Storage Release Notes*.

Table 2-1 Temporary space requirements for upgrading an Agent host

Temporary space for...	Should be...
Product components	<p>The size of the largest component package you are installing, plus the size of the associated <code>tar</code> file, plus ten percent.</p> <p>The installation routine (either the Install Script on a UNIX host or the Install Wizard on a Windows host) copies all <code>tar.gz</code> files to a temporary directory:</p> <ul style="list-style-type: none"> ■ UNIX—<code>/var/tmp</code> ■ Windows—<code>\CommandCentral Storage Upgrade</code> <p>The installation routine installs the component and then deletes the <code>tar.gz</code> files from the temporary directory.</p>
Installation logs	<p>Somewhat greater than the total size of the existing log files, which are stored by default in the following locations:</p> <ul style="list-style-type: none"> ■ UNIX—<code>opt/VRTS/install/logs/installccstor-GUID</code> (<i>GUID</i> is a unique identifier for the host.) ■ Windows—<code>\Documents and Settings\All Users\Application Data\VERITAS\CommandCentral\VxCommandCentralInstall.log</code> <p>If 4.x log files already exist, new log data is appended to the existing files during installation of version 5.1.</p>

Backing up data and files before migrating

Most of your key files configuration settings are automatically preserved for you during the upgrade process. However, it is a good practice to back up all configuration and data files as a redundancy measure.

With this in mind, we strongly recommend that you preserve copies of the files and data listed in [Table 2-2](#).

Table 2-2 Data to back up before upgrading an Agent host

Data	Default location
SAL configuration files	Solaris—all .conf files in /opt/VRTSsal/bin Windows—all .conf files in \Program Files\VERITAS\vxSAL\bin)
Data Module (DM) configuration	Solaris—all .conf files in /opt/VRTScddam Windows—all .conf files in \Program Files\VERITAS\CommandCentral\Data Module Agent\
SICL configuration	Solaris—/opt/VRTSsicls/bin/ccstor-sicl.conf Windows—\Program Files\VERITAS\CommandCentral\VRTSsicls\bin\ccstor-sicl.conf

Ensuring compatibility with hardware and with other software

Before migrating, check to be sure that the version 5.1 software will continue to interact with hardware devices and with other software products. This step is especially important if you have local (user-written) routines that interact with the hardware and software by means of CLIs and APIs.

CommandCentral Service (Veritas Backup Reporter) components—including the Management Server, Agent, view builder, and automation adapters—can run on the managed host with CommandCentral Storage version 5.1. However, components shared by the two products, such as the Symantec Private Branch Exchange and the Authentication Service, will be upgraded to the version 5.1 level.

Compatibility considerations for other hardware and software are the same as those for the Management Server.

See the following topics for more information:

- [Ensuring compatibility with hardware](#)
- [Ensuring compatibility with other software](#)

Ensuring compatibility with hardware

To verify that CommandCentral version 5.1 will run properly on the host on which you plan to install it, check the host and firewall requirements.

See the *CommandCentral Installation Guide*.

Verify that resources in your storage network are compatible with CommandCentral version 5.1.

See the *CommandCentral Hardware and Software Compatibility List*.

This document is updated regularly at:

<http://seer.entsupport.symantec.com/docs/311599.htm>

Ensuring compatibility with other software

Before migrating, verify that CommandCentral version 5.1 will continue to run with other software products such as Veritas Volume Manager (VxVM), Veritas Cluster Server (VCS), and software products from other vendors.

See the *CommandCentral Hardware and Software Compatibility List*.

Performing the upgrade on the Agent host

The following topics describe what happens as the installation routine (either the Install Script in UNIX or the Install Wizard in Windows) runs on the managed host, including some of the prompts you will receive.

- [Specifying installation options](#)
- [Specifying security and authentication options on Windows](#)
- [Installing the new software](#)

Review detailed information on responding to the installation prompts.

See the *CommandCentral Installation Guide*.

Specifying installation options

If you are upgrading from a 4.x version, the installation routine prompts you about whether array management and NetApp file scanning (on Windows and Solaris managed hosts only; not on UNIX managed hosts) should be installed.

You are also prompted for the name of the Management Server to which this managed host is connected.

Review detailed information on responding to the installation prompts.

See the *CommandCentral Installation Guide*.

Specifying security and authentication options on Windows

On Windows, the Install Wizard includes one security-related prompt. When you configure the managed host, you should check Advanced Security Settings if a non-default password is required for administrator-level accounts to use when they access the managed host.

In most cases this option is not necessary, and CommandCentral will access the managed host using default credentials. Use this option only if you previously configured the managed host so that it requires a non-default password.

Review security and authentication considerations for CommandCentral 5.1.

See the *CommandCentral Administrator's Guide*.

Installing the new software

After stopping any active 4.x processes on the managed host and uninstalling the 4.x software, the installation routine installs version 5.1 in its place. It issues periodic status messages so that you can follow its progress. However, you will not have to respond to any more prompts.

During the installation, the following local configuration settings are automatically carried forward from version 4.x to version 5.1:

- Switch configuration user ID and password
- Array configuration user ID and password
- Application configuration
- Array management settings
- Explorer attributes
- Router configuration settings

At the end of the upgrade, common components (such as the Authentication Service and Authorization Service) restart automatically. The configuration settings from your version 4.x system will be in effect at the time of the restart.

Performing post-upgrade steps on the managed host

When the installation routine completes, use the information in the following topics to verify the installation and restore configuration settings that were not upgraded automatically.

Verifying that the upgrade succeeded

The upgrade is complete when the installation routine completes. Check the installation log for details about each phase of the installation and about any problems that were encountered.

You will find the installation log in the following locations:

UNIX—`opt/VRTS/install/logs/installccstor-GUID`

Windows—`\Documents and Settings\All Users\Application Data\Veritas\CommandCentral\VxCommandCentralInstall.log`

Immediately after the upgrade, some resources might briefly be duplicated in Console displays as their object keys are updated. This does not indicate a problem.

See [“Displaying data for discovered resources”](#) on page 21.

Displaying data for discovered resources

As resources are rediscovered after the upgrade, there might be a short time when the same resource appears twice in Console displays. This is because discovery data is stored in a different format in version 5.1. When the migration explorer begins to run on the Management Server, the database can briefly contain discovery data in both formats for the same resource.

No operator intervention is required to update discovery data from the 4.x format to the 5.1 format.

Re-enabling Data Module (DM) scans

If DM scans were enabled on the managed host in version 4.x, you must re-enable the scans after completing the upgrade.

See the *CommandCentral Administrator’s Guide*.

Verifying configuration settings for the managed host

If your version 4.x system used modified configuration settings such as those for SICL and DM, the settings need to be reapplied after you upgrade the Management Server to version 5.1. No additional configuration is required on the managed host.

It is good practice, however, to check these settings on the managed host, verify that they are still appropriate in the version 5.1 environment, and adjust them as needed.

Review information on setting configuration options.

See the *CommandCentral Administrator's Guide*.

Closing firewall ports

Because CommandCentral 5.1 includes public branch exchange (PBX) functionality, it does not use some host ports that were required in the 4.x environment.

As a result, you have the option of locking down the following ports on each managed host after the upgrade. They are no longer required in version 5.1.

- 5431 (Alert Manager)
- 2148 (Veritas Enterprise Administrator)
- 2802 (SAL)

Disabling the migration explorer on the Management Server

A migration explorer enables the Management Server to discover objects attached to version 4.x Agent hosts until all of the Agent hosts have been upgraded to become version 5.1 managed hosts.

After you have upgraded all of your managed hosts to version 5.1, we recommend disabling the migration explorer on the Management Server.

To turn off the migration explorer

- 1 On the Solaris or Windows command line, navigate to the directory that contains the `halagentcfg` process:
 - Solaris—`opt/VRTSccs/VRTShal/bin`
 - Windows—`\Program Files\VERITAS\CommandCentral Storage\HAL\bin`
- 2 Stop the migration explorer by issuing the following command:

```
halagentcfg stop-process -p HALMIGA
```
- 3 Delete the migration explorer by issuing the following command:

```
halagentcfg delete-explorer -e SALToHALMigration
```
- 4 Perform cleanup by deleting directories associated with the migration explorer:
 - Solaris—`remove /var/VRTSccs/data/VRTShal/migration`
 - Windows—`remove \CommandCentral Storage Data\Data\HAL\migration`

The migration explorer is stopped and removed from the Management Server. The Management Server no longer attempts to receive discovery data from version 4.x Agent hosts.

Index

A

- Agent host
 - coexistence with Management Server 15
 - installation options 19
 - preparing to upgrade 17
- authentication
 - managed host 20

B

- backup
 - managed host 18

C

- coexistence 15
- CommandCentral Service
 - compatibility 18
- compatibility
 - CommandCentral Service 18
 - hardware 18–19
 - software 18–19
 - Symantec products 18–19
 - Veritas Backup Reporter 18
- components
 - reserving space 17
- configuration settings
 - verifying 21
- connection 13

D

- Data Module (DM)
 - configuration
 - files on managed host 18
 - re-enabling scans 21
- discovery data
 - displaying 21
- displaying
 - discovery data 21

F

- firewall ports
 - managed host 22

L

- locations
 - log files 17
 - product components 17
- logs
 - reserving space 17

M

- managed host
 - closing firewall ports 22
 - coexistence with Management Server 15
 - connection to Management Server 13
 - installation options 19
 - re-enabling DM scans 21
 - specifying password 20
 - verifying configuration 21
 - verifying upgrade 21
- Management Server
 - coexistence with 4.x Agent host 15
 - stopping migration explorer 22
- migration explorer
 - discovery data 21
 - managing 4.x Agent hosts 15
 - stopping 22

O

- objects
 - displaying 21
- options
 - installation
 - Agent host 19

P

- passwords
 - managed host 20

- ports (firewall)
 - managed host 22
- post-upgrade steps
 - managed host 20

R

- resources
 - verifying compatibility 19

S

- SAL configuration files 18
- scans
 - Data Module (DM) 21
- security
 - managed host 20
- SICL
 - backing up configuration 18
- space
 - for logs 17
 - for product components 17

T

- troubleshooting
 - managed host upgrade 21

U

- upgrade
 - managed host
 - verifying 21

V

- verifying
 - managed host upgrade 21
- Veritas Backup Reporter
 - compatibility 18