Veritas CommandCentral™ Storage Release Notes

for Microsoft Windows and UNIX

5.2

Symantec™

CommandCentral Storage Release Notes

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 5.2.1

Legal Notice

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:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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 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	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec's enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

www.symantec.com/connect

Contents

Overview of this release

This chapter includes the following topics:

- Introduction to Veritas CommandCentral Storage

- What's new in CommandCentral Storage 5.2

- Supported versions of CommandCentral Storage for rolling up data to Enterprise Reporter

- About Symantec Operations Readiness Tools

Introduction to Veritas CommandCentral Storage

Veritas CommandCentral™ Storage by Symantec is a storage resource management (SRM) solution that helps you manage your storage infrastructure more effectively.

CommandCentral Storage includes the following capabilities:

- Offers a single console that lets you visualize your networked storage environment through graphical and textual displays. The CommandCentral Storage Console seamlessly integrates performance and policy management to ensure that the storage infrastructure runs efficiently. The Console also lets you set the policies that automate notification, recovery, and other user-definable actions.

- Discovers and tracks the utilization and allocation of storage resources down to the disk level. Reporting features provide a detailed view into how and where storage is used in your enterprise.

- Shows the usage trends. Armed with this data, you can analyze the return on your storage investment. You also have what you need to implement a program of departmental chargeback.

Using CommandCentral Storage with other Symantec software, IT managers have tools to perform end-to-end storage resource management and make strategic decisions about future storage needs.

What's new in CommandCentral Storage 5.2

CommandCentral Storage 5.2 includes the following new features and enhancements.

Table 1-1   New features and enhancements

Feature	Description
New look and feel for the Console	The CommandCentral Storage Console was revised to match the organization, interaction, and appearance of other Symantec enterprise applications. Most notably, the navigation bar now includes a drop-down menu and the task pane was removed. The content that was in the task pane (server information, alerts, favorites, and tasks) was moved to the header or the footer.
	For more information about interacting with the Console, see the *CommandCentral Storage User's Guide*.
Agentless discovery of hosts by running discovery scripts	CommandCentral Storage can now discover a remote host by running scripts that collect data from the host. This discovery feature does not require you to install any software on the host. The discovery provides end-to-end visibility from the file system to the spindle. Because an agent is not required, agentless discovery eliminates agent deployment and maintenance and minimizes CPU and memory consumption.
	You can run the scripts in one of two ways. You can let CommandCentral Storage remotely access the host and run the scripts. Or, you can copy the scripts to the remote host, run the scripts, and then send the output file to the Management Server.
	For information about how to configure agentless discovery of hosts, see the *CommandCentral Administrator's Guide*.

Table 1-1   New features and enhancements *(continued)*

Feature	Description
Discovery of Storage Foundation hosts through the Unified Agent	The Unified Agent is a part of Veritas Storage Foundation. It consists of the VRTSsfmh package, which collects information about a host that includes a Storage Foundation product. Wherever Storage Foundation is installed, CommandCentral Storage can use the agent to discover information about the host. This feature lets you leverage the existing agents that you have installed in your environment without having to install a Standard Agent. For information about how to install and configure the Unified Agent, see the *CommandCentral Installation Guide*.
Control Host	CommandCentral 5.2 introduces the Control Host component. The Control Host is similar to a Standard Agent (previously called the managed host), except that it can also discover: ■ Remote hosts through agentless discovery ■ Arrays and switches ■ VMware ESX servers **Note:** In previous versions of CommandCentral Storage, array and switch discovery was possible from a Standard Agent. Before this release, you could install a Standard Agent with array management capabilities. These capabilities are now available through the Control Host only. For information about how to install the Control Host, see the *CommandCentral Installation Guide*.
Red Hat Enterprise Linux 5.5 support	We support installation of the Standard Agent on a host that runs the Red Hat Enterprise Linux 5.5 operating system.
Discovery of Solaris ZFS file systems	CommandCentral Storage can now discover Solaris ZFS file systems. We support discovery of ZFS in Solaris 10 8/07 and higher. For information about how to configure discovery of ZFS, see the *CommandCentral Hardware and Software Configuration Guide*.

Table 1-1   New features and enhancements *(continued)*

Feature	Description
Discovery of Solaris Zones	CommandCentral Storage can now discover Solaris Zones. CommandCentral Storage discovers the objects in a zone (for example, volume managers and file systems) and the storage that is exported from the global zone to non-global zones.
	We support discovery of Solaris Zones in Solaris 10 11/06 and higher.
	For information about how to configure discovery of Solaris Zones, see the *CommandCentral Hardware and Software Configuration Guide*.
Discovery of VMware guest operating systems through VMware Tools	CommandCentral Storage can now discover information about a VMware guest operating system through VI SDK without requiring the installation of a CommandCentral Standard Agent. When you configure CommandCentral Storage to discover an ESX server, the VMware explorer can discover information about guest operating systems if you install VMware Tools. Installing VMware Tools on a guest operating system enables the ESX server to obtain configuration information, which the VMware explorer discovers using VI SDK.
	For information about how to configure discovery of ESX servers, see the *CommandCentral Hardware and Software Configuration Guide*.
VMware with NAS storage	When CommandCentral Storage discovers the storage pools in your VMware environment, it can now identify the storage pools that are consumed from NAS storage. For example, the Host Virtualization Storage Summary bar chart now includes the NAS Allocated slice, which identifies the capacity of NFS-based storage pools.

Table 1-1   New features and enhancements *(continued)*

Feature	Description
Reclamation reports	CommandCentral Storage has added reclamation reporting. Reclamation reports help you determine where you can reclaim storage from any resources that are underutilized. CommandCentral Storage provides host-level reclamation reports and storage array-level reclamation reports.
	Host-level reclamation reports show the utilization percentage for each server and provide details at the LUN, file system, volume manager, and application level. Virtualization server details are also provided. For example, you can get information about unused space in storage pools and unassigned virtual machine disks.
	Array-level reclamation reports show physical disk and RAID group available storage and provide visibility into unallocated LUNs.
	For information about reclamation reports, see the *CommandCentral Storage User's Guide*.
Thin provisioning	CommandCentral Storage provides visibility into thin provisioning. Thin provisioning is a virtualization technology that allows physical storage capacity to be allocated only when needed from a pool of free storage.
	CommandCentral Storage provides visibility into the following thin provisioning storage systems:
	■ Hitachi Universal Storage Platform V ■ EMC Symmetrix DMX-3 and DMX-4 ■ EMC Symmetrix V-MAX ■ IBM XIV
	For information about thin provisioning, see the *CommandCentral Storage User's Guide*.
Discovery of IBM XIV Storage Systems	CommandCentral Storage can now discover IBM XIV Storage Systems. We support models A14-2810 and A14-2812.
	For information about how to configure discovery of IBM XIV Storage Systems, see the *CommandCentral Hardware and Software Configuration Guide*.
Discovery of FalconStor NSS	CommandCentral Storage can now discover FalconStor Network Storage Servers (NSS). We support version 6.15 with patch 42.
	For information about how to configure discovery of FalconStor NSS, see the *CommandCentral Hardware and Software Configuration Guide*.

Table 1-1   New features and enhancements *(continued)*

Feature	Description
Discovery of IBM DS8700 storage arrays	CommandCentral Storage can now discover IBM DS8700 storage arrays.
Monitoring of EMC Symmetrix arrays	CommandCentral Storage can now monitor an EMC Symmetrix array that it discovers through a remote SYMAPI server.
EMC DLA	CommandCentral Storage now discovers the host HBA WWN-specific SCSI LUN IDs (Dynamic LUN Addresses) assigned to EMC Symmetrix devices.
Discovery of drive type and drive rpm for EMC Symmetrix physical disks	CommandCentral Storage can now discover the drive type and drive rpm for Symmetrix physical disks. This information helps to determine the tier of the storage within the array. For example, Enterprise Reporter can use the attributes to define storage tiers. Discovery is possible through SYMCLI version 7.1 and higher. **Note:** Drive rpm is not applicable to enterprise flash disks.
NetApp deduplication	CommandCentral Storage now supports NetApp deduplication. For information about how to configure NetApp deduplication, see the *CommandCentral Hardware and Software Configuration Guide*.
Support for NetApp cluster modes	In a cluster configuration, a NetApp LUN can be visible to hosts through the cluster partner's array ports, as well as the local array ports. In previous versions, CommandCentral Storage discovered masking information for the local array ports only. CommandCentral Storage can now discover masking information for the local array ports and the cluster partner's array ports. **Note:** This support is possible only when the same CommandCentral Storage explorer discovers both of the arrays in the cluster configuration.
Discovery of Cisco Device Node Alias	CommandCentral Storage now provides discovery for Cisco MDS 9000-family switches when they use Device Node Alias distribution.
Brocade MPR discovery through SNMP and telnet	CommandCentral Storage can now discover Brocade Multiprotocol Routers (MPR) through the BrocadeMcData explorer, which uses SNMP and telnet to perform discovery. **Note:** We have tested discovery of the Brocade MPR when it is configured as a switch only.

Table 1-1   New features and enhancements *(continued)*

Feature	Description
Storage Foundation 5.1 for UNIX	CommandCentral Storage now discovers Storage Foundation 5.1 for UNIX. This support provides information about file systems (VxFS), volumes (VxVM), and Dynamic Multipathing (DMP).
Veritas Cluster Server 5.1 for UNIX	CommandCentral Storage now discovers Veritas Cluster Server 5.1 for UNIX.
Kerberos support for DB2	CommandCentral Storage can now discover IBM DB2 instances that use Kerberos for authentication on Solaris hosts.
Oracle 11gR2 ASM	CommandCentral Storage now supports Automatic Storage Management (ASM) in Oracle Database 11g Release 2.
Discovery of Oracle ASM disks from udev devices	CommandCentral Storage can now discover Oracle ASM disks that are created using udev devices on Linux hosts.
SCSI tape discovery disabled by default	In previous releases, CommandCentral Storage automatically discovered SCSI tapes. If you install a new instance of the 5.2 Management Server, Standard Agent, or Control Host, discovery of SCSI tapes is disabled. **Note:** If you upgrade from a previous version, discovery is still enabled. To enable SCSI tape discovery, edit the StorageExplorer's registry settings by changing the registry key Disable_scsi_tape_inquiry to 0. For information about how to edit an explorer's registry settings, see the *CommandCentral Administrator's Guide*.

Supported versions of CommandCentral Storage for rolling up data to Enterprise Reporter

Table 1-2 identifies the supported versions of CommandCentral Storage from which Enterprise Reporter can roll up data.

Table 1-2   Supported versions of CommandCentral Storage from which
Enterprise Reporter can roll up data

CommandCentral Storage version	Enterprise Reporter 5.0	Enterprise Reporter 5.0 MP1	Enterprise Reporter 5.1	Enterprise Reporter 5.2
4.x	X	X		
5.0	X	X	X	X
5.0 MP1		X	X	X
5.1		X [1]	X	X
5.1.1			X [2]	X
5.1.2			X [2]	X
5.2				X

[1] Requires Rolling Patch 1 for Enterprise Reporter 5.0 MP1 (5.0 MP1-RP1). To download 5.0 MP1-RP1, go to the Symantec Operations Readiness Tools Web site: http://sort.symantec.com

[2] Requires Hotfix 1 (HF1) for Enterprise Reporter 5.1. To download the hotfix, go to the Symantec Operations Readiness Tools Web site: http://sort.symantec.com

About Symantec Operations Readiness Tools

Symantec™ Operations Readiness Tools (SORT) is a set of Web-based tools and services that lets you proactively manage your Symantec enterprise products. SORT automates and simplifies administration tasks, so you can manage your data center operations more efficiently and get the most of out of your Symantec products.

SORT lets you do the following:

■ Collect, analyze, and report on server configurations across UNIX or Windows environments. You can use this data to do the following:

■ Assess whether your systems are ready to install or upgrade Symantec enterprise products

■ Tune environmental parameters so you can increase performance, availability, and use

■ Analyze your current deployment and identify the Symantec products and licenses you are using

- Upload configuration data to the SORT Web site, so you can share information with coworkers, managers, and Symantec Technical Support

- Compare your configurations to one another or to a standard build, so you can determine if a configuration has "drifted"

- Search for and download the latest product patches

- Get notifications about the latest updates for:

  - Patches

  - Hardware compatibility lists (HCLs)

  - Array Support Libraries (ASLs)

  - Array Policy Modules (APMs)

  - VCS agents

- Determine whether your Symantec enterprise product configurations conform to best practices

- Search and browse the latest product documentation

- Look up error code descriptions and solutions

To access SORT, go to:

http://sort.symantec.com

System requirements

This chapter includes the following topics:

- Preinstallation configuration requirements
- Supported locales
- System requirements for the Management Server
- System requirements for the Standard Agent
- System requirements for the Unified Agent
- System requirements for the Control Host
- System requirements for the Agent Push Install Utility
- Operating system patches and packages required for CommandCentral
- CommandCentral Web browser requirements
- Co-existence of CommandCentral components with other Symantec products

Preinstallation configuration requirements

The largest share of configuration occurs prior to installing CommandCentral Storage. This configuration typically comprises a number of activities performed in this order:

- Making sure that your storage network devices and their firmware levels are supported by CommandCentral Storage
- Verifying that the device is physically connected to the storage network in a supported manner
- Configuring the device to the vendor's specifications and making any additional modifications required by CommandCentral Storage

For the latest support information, see the *CommandCentral Hardware and Software Compatibility List.* This document is updated regularly at:

www.symantec.com/business/support/index?page=content&key=50379
&channel=TECHNICAL_SOLUTION&basecat=COMPATIBILITY_LIST&sort=popular

Supported locales

You can install this release on operating systems whose locale is set to English, Chinese (Simplified and Traditional), Japanese, and German. This release is available in an English version only.

We support these locales on supported Windows and UNIX operating systems. We have tested the locales on Windows and Solaris.

System requirements for the Management Server

Table 2-1 lists the operating systems on which you can install the Management Server.

Table 2-1 Supported operating systems for the Management Server

Operating system	Notes
Solaris 8	SPARC systems only.
Solaris 9	SPARC systems only.
Solaris 10	SPARC systems only. We recommend that you install CommandCentral in the global zone only.
Windows Server 2000 (SP3 or later) [1]	Supported editions include: Server, Advanced Server, and Datacenter Server.
Windows Server 2003 [1]	Supported editions include: ■ 32-bit for the following editions: Standard, Web, Datacenter, and Enterprise. ■ 64-bit (Xeon/Opteron) for the following editions: Datacenter and Enterprise.
Windows Server 2008 [1]	Supported editions include (32-bit and 64-bit): Standard, Datacenter, Enterprise, and Web.

[1] You can install the Management Server on virtual machines that run this operating system. Run the virtual machine on an ESX server.

Table 2-2 lists the system resource requirements for the Management Server. The required amounts of memory and disk space are in addition to the resources already consumed by other software on the host.

Table 2-2 System resource requirements for the Management Server

OS	Dual CPU?	Physical memory	Disk space	Temp space
Solaris	Yes	8 GB (16 GB for CommandCentral Storage + CommandCentral Storage Change Manager)	Total: 2801 MB ■ Relocatable: 1320 MB ■ Non-relocatable in /opt: 761 MB	313 MB
Windows	Yes	8 GB (16 GB for CommandCentral Storage + CommandCentral Storage Change Manager)	Total: 1650 MB ■ Relocatable: 1400 MB ■ Non-relocatable: 250 MB	750 MB

Note the following:

■ On the Management Server, disk space requirements (as well as memory and CPU) increase as you add switches, storage devices, and file usage information to the CommandCentral database.

■ On Solaris, backup of binaries are created in /var/sadm/patch and /var/sadm/pkg

■ On Solaris, temporary space shows the space that must be in /var/tmp for tar.gz packages.

For processor requirements, see the *CommandCentral Hardware and Software Compatibility List*. This document is updated regularly at:

www.symantec.com/business/support/index?page=content&key=50379 &channel=TECHNICAL_SOLUTION&basecat=COMPATIBILITY_LIST&sort=popular

System requirements for the Standard Agent

Table 2-3 lists the operating systems on which you can install the Standard Agent.

Table 2-3   Supported operating systems for the Standard Agent

Operating system	Notes
AIX 5.2 (ML7 or later)	
AIX 5.3 (ML3 or later)	For ML5, install all IY92292 filesets on the host. To verify that the filesets are installed, type the following command: "instfix -ik IY92292".
AIX 6.1	
HP-UX 11.11	
HP-UX 11.23	
HP-UX 11.31	
Red Hat Enterprise Linux 3.0 [1]	■ AS and ES (32-bit) are supported. ■ Install is not supported if SE Linux is enabled. ■ Itanium processors are not supported.
Red Hat Enterprise Linux 4.0 [1]	■ AS (32-bit) and ES (32-bit and 64-bit) are supported. ■ Install is not supported if SE Linux is enabled. ■ Itanium processors are not supported.
Red Hat Enterprise Linux 5.0 and 5.5 [1]	■ 32-bit and 64-bit are supported. ■ Install is not supported if SE Linux is enabled. ■ Itanium processors are not supported.
Solaris 8	SPARC systems only.
Solaris 9	SPARC systems only.
Solaris 10	SPARC systems only. We recommend that you install CommandCentral in the global zone only.
SUSE Linux Enterprise Server 9	■ 32-bit and 64-bit are supported. ■ Install is not supported if SE Linux is enabled.
SUSE Linux Enterprise Server 10	■ 32-bit and 64-bit are supported. ■ Install is not supported if SE Linux is enabled.
Windows Server 2000 (SP3 or later) [1]	Supported editions include: Server, Advanced Server, and Datacenter Server.

Table 2-3 Supported operating systems for the Standard Agent *(continued)*

Operating system	Notes
Windows Server 2003 [1]	Supported editions include: ■ 32-bit for the following editions: Standard, Web, Datacenter, and Enterprise. ■ 64-bit (Xeon/Opteron) for the following editions: Datacenter and Enterprise.
Windows Server 2008 [1]	Supported editions include (32-bit and 64-bit): Standard, Datacenter, Enterprise, and Web.

[1] You can install the Standard Agent on the virtual machines that run this operating system. Run the virtual machine on an ESX server. If the ESX server uses QLogic's HBA, install the VMware version of QLogic's HBA API library on the server. The guest operating system requires installation of VMware Tools.

Table 2-4 lists the system resource requirements for the Standard Agent. The required amounts of memory and disk space are in addition to the resources already consumed by other software on the host.

Table 2-4 System resource requirements for the Standard Agent

OS	Dual CPU?	Physical memory	Disk space	Temp space
AIX	No	256 MB	Total: 381 MB ■ Non-relocatable in /opt: 380 MB ■ Binaries backup: 1 MB	154 MB
HP-UX	No	256 MB	Total: 478 MB ■ Relocatable: 339 MB ■ Non-relocatable in /opt: 136 MB ■ Binaries backup: 3 MB	186MB

Table 2-4 System resource requirements for the Standard Agent *(continued)*

OS	Dual CPU?	Physical memory	Disk space	Temp space
Linux	No	256 MB	Total: 224 MB ■ Relocatable: 153 MB ■ Non-relocatable in /opt: 70 MB ■ Binaries backup: 1 MB	29 MB
Solaris	No	256 MB	Total: 393 MB ■ Relocatable: 312 MB ■ Non-relocatable in /opt: 81 MB	187 MB
Windows	No	256 MB	Total: 360 MB ■ Relocatable: 310 MB ■ Non-relocatable: 50 MB	250 MB

Note the following:

■ On AIX, backup of binaries are created in /usr/lpp

■ On HP-UX, backup of binaries are created in /var/adm/sw/save

■ On Solaris, backup of binaries are created in /var/sadm/patch and /var/sadm/pkg

■ On UNIX, temporary space shows the space that must be in /var/tmp for tar.gz packages.

■ On HP-UX, the minimum values are required for the following HP-UX variables:

  ■ maxssiz—80MB (process maximum stack size)

  ■ maxdsiz—1.9GB (data segment)
    For more information about these variables, refer to your HP-UX documentation.

For processor requirements, see the *CommandCentral Hardware and Software Compatibility List*. This document is updated regularly at:

www.symantec.com/business/support/index?page=content&key=50379 &channel=TECHNICAL_SOLUTION&basecat=COMPATIBILITY_LIST&sort=popular

System requirements for the Unified Agent

Table 2-5 lists the operating systems on which you can install the Unified Agent.

Table 2-5   Supported operating systems for the Unified Agent

Operating system	Notes
AIX 5.2	On AIX hosts, the xlC runtime environment must be version 8 or later. Use the `lslpp -lc	grep xlC.rte` command to verify the version of the xlC runtime environment.
AIX 5.3	
AIX 6.1	AIX 6.1 for Storage Foundation 5.0 MP3 hosts only.
HP-UX 11.11	For Storage Foundation 3.5 hosts only. Supported architecture includes PA RISC.
HP-UX 11.23	
HP-UX 11.31	
Red Hat Enterprise Linux 4.0	Storage Foundation 5.0 is supported on 64-bit Xeon, x86, and PowerPC; Storage Foundation 4.1 is supported on x86 and Xeon (32-bit and 64-bit).
Red Hat Enterprise Linux 5.0 Update 2	For Storage Foundation 5.0 MP3 hosts only.
SUSE Linux Enterprise Server 9	Storage Foundation 5.0 is supported on 64-bit Xeon, x86, and PowerPC; Storage Foundation 4.1 is supported on x86 and Xeon (32-bit and 64-bit).
SUSE Linux Enterprise Server 10	For Storage Foundation 5.0 MP3 hosts only.
Solaris 8	
Solaris 9	
Solaris 10	Supported architecture includes SPARC and x86.
Windows Server 2000	Supported architecture includes x86 and x64.
Windows Server 2003	Supported architecture includes x86, x64, and IA64.
Windows Server 2008	Supported architecture includes x86, x64, and IA64.

For more information about operating system requirements, refer to your Storage Foundation documentation.

Table 2-6 lists the system resource requirements for the Unified Agent.

Table 2-6 System resource requirements for the Unified Agent

OS	CPU	Physical memory	Disk space
UNIX	Refer to your Storage Foundation documentation	Refer to your Storage Foundation documentation	50MB in `/var/opt` for discovery state files; 50MB in `/opt`
Windows	Refer to your Storage Foundation documentation	Refer to your Storage Foundation documentation	30MB in `Install_path`\Veritas\VRTSsfmh; 50MB in `%COMMONAPPDATAFOLDER%`\Symantec

System requirements for the Control Host

Table 2-7 lists the operating systems on which you can install the Control Host.

Table 2-7 Supported operating systems for the Control Host

Operating system	Notes
Solaris 8	SPARC systems only.
Solaris 9	SPARC systems only.
Solaris 10	SPARC systems only. We recommend that you install CommandCentral in the global zone only.
Windows Server 2000 (SP3 or later) [1]	Supported editions include: Server, Advanced Server, and Datacenter Server.
Windows Server 2003 [1]	Supported editions include: ■ 32-bit for the following editions: Standard, Web, Datacenter, and Enterprise. ■ 64-bit (Xeon/Opteron) for the following editions: Datacenter and Enterprise.
Windows Server 2008 [1]	Supported editions include (32-bit and 64-bit): Standard, Datacenter, Enterprise, and Web.

[1] You can install the Control Host on virtual machines that run this operating system. Run the virtual machine on an ESX server.

Table 2-8 lists the system resource requirements for the Control Host. The required amounts of memory and disk space are in addition to the resources already consumed by other software on the host.

Table 2-8   System resource requirements for the Control Host

OS	Dual CPU?	Physical memory	Disk space	Temp space
Solaris	No	512 MB	Total: 876 MB ■ Relocatable: 585 MB ■ Non-relocatable in /opt: 291 MB	187 MB
Windows	No	512 MB	Total: 460 MB ■ Relocatable: 360 MB ■ Non-relocatable: 100 MB	270 MB

Note the following:

■ On Solaris, backup of binaries are created in /var/sadm/patch and /var/sadm/pkg

■ On Solaris, temporary space shows the space that must be in /var/tmp for tar.gz packages.

For processor requirements, see the *CommandCentral Hardware and Software Compatibility List*. This document is updated regularly at:

www.symantec.com/business/support/index?page=content&key=50379 &channel=TECHNICAL_SOLUTION&basecat=COMPATIBILITY_LIST&sort=popular

System requirements for the Agent Push Install Utility

Table 2-9 lists the operating systems on which you can install the Agent Push Install Utility.

Table 2-9   Supported operating systems for the Agent Push Install Utility

Operating system	Notes
Windows Server 2000 (SP3 or later)	Supported editions include: Server, Advanced Server, and Datacenter Server.

Table 2-9 Supported operating systems for the Agent Push Install Utility
(continued)

Operating system	Notes
Windows Server 2003	Supported editions include: ■ 32-bit for the following editions: Standard, Web, Datacenter, and Enterprise. ■ 64-bit (Xeon/Opteron) for the following editions: Datacenter and Enterprise.
Windows Server 2008	Supported editions include (32-bit and 64-bit): Standard, Datacenter, Enterprise, and Web.

Table 2-10 lists the system resource requirements for the Agent Push Install Utility. The required amounts of memory and disk space are in addition to the resources already consumed by other software on the host.

Table 2-10 System resource requirements for the Agent Push Install Utility

Dual CPU?	Physical memory	Disk space	Temp space
No	512 MB	Total: 192 MB ■ Relocatable: 180 MB ■ Non-relocatable: 12 MB	165 MB

For processor requirements, see the *CommandCentral Hardware and Software Compatibility List.* This document is updated regularly at:

www.symantec.com/business/support/index?page=content&key=50379
&channel=TECHNICAL_SOLUTION&basecat=COMPATIBILITY_LIST&sort=popular

Operating system patches and packages required for CommandCentral

Table 2-11 lists the patches and packages that are required for the operating system on which you install the Management Server, Control Host, or Standard Agent.

Table 2-11   Patches and packages required for CommandCentral

OS version	Required patches or packages
AIX 5.2 and 5.3	■ `xlC.rte-6.0.0.0` ■ `xlC.aix50.rte-6.0.0.0`
HP-UX 11.11	■ PHSS_24304 ■ PHSS_26560 ■ PHSS_26946 ■ PHSS_31326
HP-UX 11.23	■ PHSS_31855 ■ PHSS_33903 ■ PHSS_34444 ■ PHSS_34445 ■ PHSS_34853 ■ PHSS_34859 ■ PHSS_35055 ■ PHSS_35528 ■ PHSS_35978 ■ PHSS_36336
HP-UX 11.31	■ PHCO_38048 ■ PHCO_38050 ■ PHSS_38141 ■ PHSS_39102 ■ PHSS_38527 ■ PHSS_38135 ■ PHSS_38861
Red Hat Enterprise Linux 3.0, 4.0, and 5.0	■ `openssl096b-0.9.6b-16` ■ `libstdc++-libc6.2-2.so.3` ■ `libstdc++.so.5.0.7`

Table 2-11   Patches and packages required for CommandCentral *(continued)*

OS version	Required patches or packages
Solaris 8	Required packages include: SUNWgss (for the Management Server only) Required patches include: ■ 108434 * ■ 108434-14 ■ 108435 ■ 108435-14 ■ 108528-29 ■ 108652-78 * ■ 108773-18 ■ 108921-19 ■ 108940-60 ■ 108987-13 ■ 108989-02 ■ 108993-18 ■ 108993-32 ■ 109147-27 ■ 109147-43 ■ 109326-13 ■ 110386-03 ■ 110615-10 ■ 111023-03 ■ 111111-03 ■ 111308-04 ■ 111310-01 ■ 111317-05 ■ 111721-04* ■ 112003-03 ■ 112396-02 ■ 112438-02 ■ 112472-01 ■ 113648-03 ■ 115827-01 ■ 116602-01 ■ 112438 An asterisk (*) indicates that the patch is required for the Management Server and Control Host only. It is not required for the Standard Agent.

Table 2-11   Patches and packages required for CommandCentral *(continued)*

OS version	Required patches or packages
Solaris 9	Required packages include: ■ SUNWgss (for the Management Server only) ■ SUNWscpux Required patches include: ■ 111722-04 * ■ 111703 * ■ 112785-30 * ■ 112963-25 ■ 113096-03 * An asterisk (*) indicates that the patch is required for the Management Server and Control Host only. It is not required for the Standard Agent.
Solaris 10	Required packages include: ■ SUNWgss (for the Management Server only) ■ SUNWscpu Required patches include: ■ 117461-08 ■ 119130-09

Table 2-12 lists the Solaris patches that are unsupported. If these patches are installed, you need to install a remedy patch.

Table 2-12   Solaris patches that are unsupported

OS version	Unsupported patches	Remedy patch to install [1]
Solaris 8	■ 109147-36 ■ 109147-37 ■ 109147-38 ■ 109147-39	109147-40
	■ 111095-26 ■ 111096-14 ■ 111097-22 ■ 111412-19 ■ 114475-06 ■ 119913-08	These patches indicate that SAN release 4.4.9 is installed. Upgrade the SAN release to a higher version.

Table 2-12   Solaris patches that are unsupported *(continued)*

OS version	Unsupported patches	Remedy patch to install [1]
Solaris 9	■ 112963-21 ■ 112963-22 ■ 112963-23 ■ 112963-24	112963-25
	■ 113039-13 ■ 113040-18 ■ 113041-11 ■ 113042-14 ■ 114476-07 ■ 119914-08	These patches indicate that SAN release 4.4.9 is installed. Upgrade the SAN release to a higher version.
Solaris 10	■ 117461-03 ■ 117461-04 ■ 117461-05 ■ 117461-06 ■ 117461-07	117461-08
	■ 119254-42 ■ 125978-08	119254-59

[1] Or a patch that is a higher equivalent.

Increasing semaphore limits on Solaris

The Veritas Provider Access Layer (VxPAL) and the Veritas Enterprise Administrator Service require more operating system semaphores than are usually set by default on Solaris.

To increase semaphore limits on Solaris

1   Open a UNIX console and log in as root on the target host.

2   Using a text editor, open: `/etc/system`

3   Locate a line similar to the following. If the line is not there, add it:

    ```
    set semsys:seminfo_semmni=0x10
    ```

4   Make sure that the value is something larger than what is currently there. For example, set sminfo_semmni to 0x10.

5   Save the file and reboot the host.

Management Server installation on a core Solaris 10 host requires additional Solaris packages

When you attempt to install the Management Server on a host with core Solaris 10 installed, the installation fails. One or both of the following messages appear:

```
The installer could not locate the Solaris SUNWzoneu package or the
file /usr/bin/zonename from the SUNWzoneu package on the target host.
You must add the package or the file before you install CommandCentral
Storage.
```

```
The installer could not locate the Solaris SUNWxcu4 package or the
file /usr/xpg4/bin/sed from the SUNWxcu4 package on the target host.
You must add the package or the file before you install CommandCentral
Storage.
```

Before you install the Management Server, you need to install additional packages from the Solaris operating system CD.

To install the Management Server on a host with core Solaris 10 installation

1   Add the following packages from the Solaris operating system CD:

- SUNWzoner—Solaris zones configuration files

- SUNWctpls—Portable layout services for Complex Text Layout support

- SUNWmfrun—Motif 2.1 libraries, headers, xmbind and bindings

- SUNWxwrtl—X Window system and graphics runtime library links

- SUNWxwice—Library and utilities to support the X Window System Inter-Client Exchange

- SUNWxwfnt—X Window system platform required fonts

- SUNWxwplr—X Window system platform software configuration

- SUNWxwplt—X Window system platform software

- SUNWj5rt—JDK 5.0 Runtime Environment (1.5.0_07)

- SUNWpoolr—Resource pools (root)

- SUNWpool—Resource pools

- SUNWlur—Live upgrade (root)

- SUNWluu—Live upgrade (usr)

- SUNWluzone—Live upgrade (zones support)

- SUNWzoneu—Solaris zones (usr)

- SUNWadmc—System administration core libraries

- SUNWadmfw—System and network administration framework

- SUNWadmfr—System and network administration framework configuration

- SUNWbindr—BIND DNS name server and tools

- SUNWbind—BIND name server manifest

- SUNWscpr—Source compatibility (root)

- SUNWscpu—Source compatibility (usr)

- SUNWxcu4—XCU4 utilities

- SUNWxcu4t—XCU4 make and sccs utilities

Type the following command to add each package:

```
pkgadd package_name
```

2 Create the `/etc/resolve.conf` file with a DNS entry for the host on which you plan to install the Management Server.

3 Add the following entry to the `/etc/nsswitch.conf` file:

```
hosts: files dns
```

4 Retry the Management Server installation. You can now install the Management Server.

CommandCentral Web browser requirements

One of the following Web browsers is required to run the Console:

- Microsoft Internet Explorer 6.x or 7.x (Windows only)

- Mozilla 1.7 (Solaris only)

- Mozilla Firefox 2.0.0.x or 3.x (Windows only)

Note the following requirements:

- Your browser must support either JScript 5.5 (provided with Microsoft Internet Explorer 6 or later) or JavaScript 1.2 . Additionally, for Internet Explorer, Secure Sockets Layer (SSL) 3.0 ActiveX scripting must be enabled.

- If you use pop-up blockers, either disable them or configure them to accept pop-ups from the CommandCentral Management Servers to which you will connect.

- To display the CommandCentral Storage Topology Map in a Web browser, install at least Java 5 (version 1.5).

- The minimum recommended resolution for the Console is 1024 x 768.

- For Internet Explorer 6.0 on Windows 2000 (Server, Advanced Server, or Datacenter Server) and Windows 2003 Server (Standard Edition, Datacenter Edition, Enterprise Edition, or Web Edition), set the default Intranet zone security level to MEDIUM or lower.

Co-existence of CommandCentral components with other Symantec products

Several Symantec products may be installed on the same host in a typical data storage management environment. The following tables identify if a product (or product component) can co-exist on a host where CommandCentral 5.2 components are installed. The tables only include the products that were tested for this release.

Table 2-13 identifies if a Symantec product can co-exist with the CommandCentral Management Server.

Note: The CommandCentral Management Server includes the CommandCentral Storage and CommandCentral Storage Change Manager modules only. It does not pertain to CommandCentral Enterprise Reporter.

Table 2-13   Management Server co-existence with other Symantec products

Symantec product	Co-existence supported?
CommandCentral Enterprise Reporter	No
Symantec NetBackup 7.0 Client	Yes
Veritas Operations Manager Management Server	No
Veritas Operations Manager managed host	No
Veritas Storage Foundation 5.1 for UNIX	Yes
Veritas Storage Foundation 5.1 SP1 for UNIX	Yes
Veritas Storage Foundation for Windows 5.1 SP1	Yes

Table 2-14 identifies if a Symantec product can co-exist with the CommandCentral Control Host.

Table 2-14 Control Host co-existence with other Symantec products

Symantec product	Co-existence supported?
Symantec NetBackup 7.0 Client	Yes
Veritas Operations Manager Management Server	No
Veritas Operations Manager managed host	No
Veritas Storage Foundation for Windows 5.1 SP1	Yes

Table 2-15 identifies if a Symantec product can co-exist with the CommandCentral Standard Agent.

Table 2-15 Standard Agent co-existence with other Symantec products

Symantec product	Co-existence supported?
Symantec NetBackup 7.0 Client	Yes
Veritas Storage Foundation for Windows 5.1 SP1	Yes

No longer supported

This chapter includes the following topics:

■ Features that are no longer supported in CommandCentral 5.2

Features that are no longer supported in CommandCentral 5.2

Table 3-1 lists the features that are no longer supported in CommandCentral 5.2

Table 3-1   Features that are no longer supported

Feature	Description
File and mail scanning through the Data Module	CommandCentral 5.2 does not include the ability to scan file systems and Microsoft Exchange mail servers. All Data Module features have been removed, except for the file systems projections feature, which provides projected storage consumption for file systems. If you want to continue to use all Data Module features, you should not upgrade to CommandCentral 5.2.
4.x agents	We do not support 4.x agents reporting to a 5.2 Management Server.
CNT switches	CommandCentral 5.2 does not support the discovery of CNT switches.
Change detection for storage arrays	You can no longer enable change detection for array explorers. With change detection, array explorers would listen to SNMP traps or frequently poll storage arrays to detect configuration-related changes to storage arrays.

Fixed issues

This chapter includes the following topics:

■ Issues fixed in CommandCentral Storage 5.2

Issues fixed in CommandCentral Storage 5.2

Table 4-1 lists the issues that are fixed in CommandCentral Storage 5.2.

Table 4-1 Issues that are fixed in CommandCentral Storage 5.2

Incident	Description
859670	Default agent password cannot be changed using CommandCentral product installer on UNIX.
1239973	Discovery of NetApp unified storage devices fails if NetApp explorer debug level is set to 6.
1404832	Discovery of RAID-6 and SSD devices is not supported for EMC DMX-4 storage arrays.
1449432	Mistyped Management Server name cannot be corrected in Windows installer.
1786011	Incorrect masking status for the LUNs for a Celerra unified storage system.
1810799	LUNs not masked to array ports for Celerra unified storage devices do not appear.
1898826	An EMC Celerra storage array does not appear in the Console if file system names or share names have European characters.
1907351	The topology does not display the correct connections for virtual switches.
1910005	For backend Symmetrix arrays, incorrect data appears in the Array Overview and Total Online Storage charts.

Table 4-1 Issues that are fixed in CommandCentral Storage 5.2 *(continued)*

Incident	Description
1913191	The Host Consumption report takes several minutes to load.
1914190	The McDataSwitchExplorer does not properly discover and monitor IBM-branded McDATA switches.
1917423	Cannot detect the correlation between unidentified adapters and hosts when you use agentless rules.
1923179	No monitoring for Symmetrix arrays after you enable monitoring through the Edit Device Configuration wizard.
1923197	After upgrade, monitoring does not update for some arrays and switches.
1923275	Security vulnerability in libssl32.
1925591	CommandCentral Storage does not discover MirrorView LUNs for EMC CLARiiON CX-960 storage arrays.
1929129	Array discovery status is INACTIVE even when discovery is normal.
1933272	In the Array Performance reports, data is not available for EMC CLARiiON storage arrays if you change the scope to 24 hours.
1933475	Monitoring does not work for Cisco switches.
1933840	Installer closes during Management Server installation on a Windows host that includes Storage Foundation 5.1 SP1.
1935250	LUN icons indicate the wrong type of LUNs in several tables.
1937375	Data is incorrect for EMC DMX4 storage arrays.
1942819	Cannot configure discovery of Microsoft SQL 2000 servers.
1962416	After upgrade, the DB2 explorer crashes on AIX Standard Agents.
1970762	SMI-S monitoring of IBM DS8000 series storage arrays does not work if SMI-S is not version 1.1 or 1.2.
1987089	On Linux hosts, the StorageExplorer causes tapes to rewind.
2008430	Zone information is not available for Brocade switches.
2014884	Capacity values are incorrect for a NetApp filer.
2043874	Cannot view performance data for all RAID groups in the Array Performance Summary report.

Table 4-1   Issues that are fixed in CommandCentral Storage 5.2 *(continued)*

Incident	Description
2051702	CommandCentral does not discover EMC Symmetrix storage arrays, because the EMCSymmetrixExplorer crashes.
2070461	Environmental monitoring does not work for HP-XP storage arrays.
2070582	The exchange explorer crashes during discovery of a Microsoft Exchange 2007 server.
2077917	CommandCentral Storage processes do not run, because DCT files are not processed into the database.
2086490	The capacity of an Oracle database is incorrectly listed as 0 GB.

Software limitations

This chapter includes the following topics:

- Discovery and management limitations
- Console and report limitations
- Agentless discovery limitations

Discovery and management limitations

The following notes pertain to discovery and management-related limitations that you might encounter when you use CommandCentral 5.2.

Reports show incorrect capacity for NetApp LUNs with space reservation turned off

If thin (over) provisioning is used in NetApp MultiStore Virtual Systems, the total LUN capacity displayed in the Storage Capacity reports might be greater than the actual logical capacity of the volume. This can occur when a LUN is created with space reservation turned OFF.

This option allows the creation of LUNs that are larger than the volume capacity.

NetApp does not provide a way to identify the used capacity in a LUN when space reservation is turned off. As a result, there may be inconsistencies when CommandCentral Storage calculates LUN capacity.

For the same reason, the NAS Used value for a NetApp MultiStore Virtual System might display as a negative number.

Example: On a 50 GB volume, create a LUN of 40 GB with space reservation OFF. At first, the Used Logical capacity is approximately zero but the LUN capacity is 40 GB. If you subsequently create another 40 GB LUN with space reservation on, the resulting LUN capacity for the volume is 80 GB but the Used Logical capacity

is −40 GB. The Used Logical capacity will increase as you write data onto the LUN with space reservation OFF or onto a file system in NAS mode.

NAS Used equals Used Logical capacity minus Total LUN Capacity. In the example, this is 40 GB minus 80 GB, yielding the result of −40 GB.

Because reports ignore negative values, they will display NAS Used as zero and LUN capacity as 80 GB. Thus, in the Storage Capacity reports, the total LUN capacity displayed will be greater than the actual logical capacity of the volume.

The problem does not occur when you are using other thin provisioning scenarios such as FlexVols.

Volume layout not discovered for LDM-managed volumes mounted without a drive letter

CommandCentral does not discover the volume layout for volumes mounted without a drive letter on a Windows host when the volume manager type is Microsoft LDM. As a result, the Volume Layout column is blank when you display such volumes in the Console.

There is no workaround.

Capacity not discovered for LDM-managed volumes without file systems

CommandCentral does not discover the capacity for volumes on a Windows host when the volume manager type is Microsoft LDM and the volume contains no file systems. In this instance, the volume capacity displays incorrectly as zero.

There is no workaround.

Restoring Brocade switch configuration may fail when reboot required

Restoring the switch configuration for a Brocade switch may fail if the restored configuration requires a switch reboot. To workaround this issue, we recommend that you initiate the switch restoration through a Brocade switch Telnet session with the saved configuration file.

Unable to remove disk groups via HP EVA SSSU version 4.0 and 4.1

Versions 4.0 and 4.1 of the HP EVA Storage System Scripting Utility (SSSU) CLI do not remove disk groups when specified from the CommandCentral Storage Console (**Managing Summary > Array > EVA > Disk Groups > Destroy Disk Group**).

There is no workaround. Contact your HP support representative.

Detect Devices command applies only to objects that use device managers

The CommandCentral Console Detect Devices command does not apply to objects that do not rely on device managers for their operation. For example, if you run the Detect Devices command on Cisco switches using SNMP (Settings > Devices > Detect Devices), the Console does not output an error message.

Cannot discover storage pools that do not have names (1435403)

If a storage pool does not have a name, CommandCentral does not discover that storage pool.

Size of a Celerra disk volume does not match Celerra Manager (1747844)

CommandCentral Storage reports a different size for a Celerra disk volume than Celerra Manager does. This difference occurs because Celerra Manager rounds the values where as CommandCentral Storage does not.

CommandCentral Storage does not discover NetBackup media changers on Windows (1810148)

By default, the Windows operating system does not include a device driver that can handle media changers. Because of this, a Windows host cannot create device paths for media changers.

If CommandCentral Storage discovers a NetBackup instance that runs on Windows and an associated media changer does not have a device handle, CommandCentral Storage cannot discover the media changer.

Discovery of HBAs fails on an AIX host (1839014)

Discovery of HBAs may fail on an AIX host that has stale device handles. A stale device handle occurs when the host had access to the LUNs, but the access was lost. For example, this might occur if you unzone the array port from the HBA port or unmask a LUN that was masked earlier.

Workaround

Run the appropriate operating system tools on AIX to purge the stale device handles. Then, refresh the storage explorer.

To refresh the storage explorer

1   In the CommandCentral Console, click **Settings > Host Management**.

2   In the Hosts table, click the AIX host for which discovery failed.

3   In the Explorers table, check **StorageExplorer**.

4   In the drop-down list, click **Refresh Explorer**. Then, click **Go**.

5   In the Refresh Selected Explorer(s) dialog box, click **OK**.

Capacity values for IBM XIV storage arrays do not match the IBM XIV Storage GUI (2145984)

The capacity values for IBM XIV storage arrays that appear in CommandCentral Storage do not match the values in the IBM XIV Storage GUI. The capacities do not match because the IBM XIV Storage GUI uses a factor of 1000 to convert bytes to gigabytes, where as CommandCentral Storage uses a factor of 1024. CommandCentral Storage uses a factor of 1024 for all storage arrays.

For example:

■   CommandCentral Storage converts 32212254720 bytes to 30 GB by performing the following calculation:
    32212254720 / (1024 x 1024 x 1024)

■   The IBM XIV Storage GUI converts 32212254720 bytes to 32.2 GB by performing the following calculation:
    32212254720 / (1000 x 1000 x 1000)

Capacities for IBM XIV storage pools different than reported by XIV GUI (2078611)

The capacities that CommandCentral Storage reports for IBM XIV storage pools do not match the capacities in the XIV storage GUI. This happens because CommandCentral Storage obtains capacities from the XCLI that are rounded off. For example, a LUN size might be 34.36 GB, but the LUN size is rounded off in the XCLI output to 34 GB.

Console and report limitations

The following notes pertain to limitations that you might encounter when you use the Console and its reports.

Reports ToolTips are truncated in Firefox

In the CommandCentral Storage reports, column headers in tables display ToolTips when you point your mouse cursor over them. Each ToolTip contains a description for the column.

In Firefox 2.x, the ToolTip text is truncated after about 70 characters, and an ellipsis (...) is substituted for the remaining text. This is a browser limitation. This limitation is fixed in Firefox 3.x.

Cannot log in to the Console using Internet Explorer when the host name includes an underscore (1447601)

If the Management Server's host name includes an underscore, you cannot log in to the Console using Internet Explorer. This occurs because of a limitation in Internet Explorer.

Workaround

Do one of the following:

- If you use Internet Explorer, connect to the Console using the Management Server's IP address. For example, type `https://ipaddress:8443` in the browser's address field.

- Use Firefox to connect to the Console.

Dialogs overwritten when new dialogs are opened (606871)

If a Console user launches a dialog (either a wizard or a standalone dialog box) while another dialog is already open, the second dialog overwrites the first one.

Workaround

Ensure that all dialogs are closed before opening a new one.

Agentless discovery limitations

The following software limitations pertain to agentless discovery of hosts.

Non-super user capacity not discovered for file systems (1891194)

When CommandCentral discovers an agentless host that runs a UNIX operating system, it does not discover the non-super user capacity of associated file systems.

Cannot view association between some objects (1888735)

When CommandCentral discovers an agentless host that runs Windows or UNIX, the following limitations apply:

- You cannot view the associations between internal disks (LUNs) and the corresponding OS handles.
- You cannot view the associations between file systems and OS handles if the file system is mounted directly on the raw OS handle.

Null or 10 character serial number discovered for Solaris disks (1805190)

When you view the attributes for a LUN, you can view the serial number for the associated disk. If a Standard Agent discovers the host to which the disk is attached, a 20 character serial number appears. If you use agentless discovery to discover a Solaris host, CommandCentral may not discover the disk's serial number. If CommandCentral does discover the disk's serial number, a 10 character serial number appears.

DASState attribute not discovered for disks (1805388)

When CommandCentral performs agentless discovery of a Windows or Solaris host, it does not discover the DASState attribute for the disks that are directly attached to the host.

Some attributes not discovered for HBAs (1890705 and 1975453)

When CommandCentral performs agentless discovery of remote hosts, it does not discover some attributes for HBAs.

When CommandCentral discovers a Solaris host, it does not discover the following HBA attributes:

- Product Name
- Firmware Version (there are some instances where CommandCentral discovers this attribute)

When CommandCentral discovers a Red Hat Enterprise Linux 4 host or a SUSE 9 host, it does not discover the following attributes for QLogic HBAs:

- Product name
- Product serial number
- Port ID

- Port type

- Unique LUN ID

Device handles for multipathing LUNs identified as separate disks and capacities multiplied (1928661)

You can configure agentless discovery of a remote host that uses multipathing software. If you discover this type of host, configure CommandCentral to discover the storage arrays from which the multipathing LUNs are allocated to the host. Otherwise, CommandCentral cannot discover the IDs for the LUNs that are allocated to the host. As a result, CommandCentral identifies the device handles for the LUNs as separate disks and capacities are multiplied in the Storage Consumption reports.

For information about supported multipathing software, see the *CommandCentral Hardware and Software Compatibility List.*

www.symantec.com/business/support/index?page=content&key=50379 &channel=TECHNICAL_SOLUTION&basecat=COMPATIBILITY_LIST&sort=popular

Known issues

This chapter includes the following topics:

- Install, uninstall, and upgrade issues
- Management Server and database issues
- Standard Agent issues
- Unified Agent issues
- Console issues
- Discovery and discovery data issues
- Report issues
- User management issues
- Monitoring issues

Install, uninstall, and upgrade issues

The following are known issues that you might encounter when you install, uninstall, or upgrade CommandCentral Storage.

Error message about VRTSweb during upgrade on Windows (542244)

If the Symantec Web Server (`VRTSweb`) is running when you perform an upgrade, you may receive the following error message:

```
Executed the command("C:\WINDOWS\system32\net.exe" start
VRTSweb). Return code (2)!!!
```

Workaround

If you encounter this error message, restart VRTSweb and its dependent services—including Veritas CommandCentral Common Login Service (`VRTScclogin`) and Veritas CommandCentral Storage Web Engine (`VRTSccsweb`). Then click OK to continue the upgrade.

Alternatively, you can wait and restart `VRTSweb` and its dependent services after the upgrade completes.

Summary file not created during Standard Agent installation on UNIX (1143138)

At the end of a Standard Agent installation on a UNIX host, you see a message similar to the following:

```
Installation log files, summary file, and response file are saved at:
```

```
/opt/VRTS/install/logs/installccstor-qvChRb
```

However, the summary file is not created.

Workaround

Use the installation log files to view the summary of the Standard Agent installation.

Erroneous reference to response file at end of Management Server install on Solaris (1140473)

At the end of the Management Server install on a Solaris host, a message similar to the following displays:

```
Installation log files, summary file, and response file are saved at:
```

```
/opt/VRTS/install/logs/installccstor-qvChRb
```

The reference to the response file is erroneous. No such file is created when you install the Management Server. You should disregard this reference.

CommandCentral installations on Windows fail while configuring SICL (1171143)

Management Server, Control Host, and Standard Agent installations on Windows hosts may fail while configuring SICL. The installations may fail if you have multiple directory paths defined in the `TEMP` environment variable.

Workaround

First, uninstall CommandCentral. Then, set a single directory path in the `TEMP` environment variable and re-run the installation.

Error message appears during uninstall of the Management Server from a Windows host (1432751)

When you uninstall the Management Server from a Windows host, the following error message may appear:

```
ERROR: RemoveDirectory(E:\ccs_nondef\CommandCentral Storage\Web
Engine\spc\tasks) failed.

Error=0x00000020!!!
```

The error message appears because there is an active connection to the CommandCentral Console.

Before you proceed with the uninstall, log out of the Console and close your web browser. Then, click OK to proceed with the uninstall.

Authentication Service fails to upgrade during Management Server installation on Windows (1427441)

When you install the CommandCentral Management Server on Windows, the installer may detect that a previous version of the Symantec Product Authentication Service exists on the host. During installation of the Management Server, the installer upgrades the Authentication Service. If the previous version of the Authentication Service was installed in Client mode, upgrade of the Authentication Service fails and the CommandCentral installer closes with an error.

Workaround

To correct the issue, do one of the following:

- If no other Symantec products are using the Authentication Service, uninstall it before installing the Management Server. To remove the Authentication Service, use Windows' Add or Remove Programs tool.

- If there are other Symantec products using the Authentication Service, run the following command:
  ```
  msiexec /qn /i "VERITAS Authentication Service.msi" /l*v "At.log"
  INSTALLDIR="C:\Program Files\VERITAS\Security"
  UUIDINSTALLDIR="C:\Program Files\Veritas" INSTALLLEVEL=2
  ADDLOCAL=Server REINSTALL=Client REINSTALLMODE=vomus BROKERMODE=rab
  ```

```
PASSWORD1=Vxadmin PASSWORD2=Vxadmin STARTSERVICE=NO DOUPGRADE=YES
REBOOT=ReallySuppress
```

where the values of INSTALLDIR and UUIDINSTALLDIR can be different depending on the default and non-default install location of the existing AT client.

VRTSWeb folder remains after uninstalling the Management Server on Windows (1292780)

After you uninstall the Management Server from a Windows host, the VRTSWeb folder remains in the directory in which you installed CommandCentral. You can safely delete this folder.

Error message about inability to copy files to /var/tmp displays during install (1438157)

When you install the Management Server, Control Host, or Standard Agent on UNIX, an error message similar to the following may display:

```
CPI ERROR V-9-0-0 Cannot copy ./Support/platform to
/var/tmp/installccstor-Unique_ID on hostname installccstor log files
are saved at /opt/VRTS/install/logs/installccstor-Unique_ID
```

The error message displays because there is insufficient space in /var/tmp

Before you proceed with installation, create more space in /var/tmp

HAL configuration fails during Standard Agent install on AIX 5.3 TL06 or TL07 (1431432)

When you install the Standard Agent on an AIX 5.3 host with Technology Level 6 (TL06) or Technology Level 7 (TL07), configuration of the Hardware Abstraction Layer (HAL) may fail with the following error message:

```
System error: bad address
```

Workaround

For AIX 5.3 TL06, install the following patch: IZ05077

For AIX 5.3 TL07, install the following patch: IZ06832

After you install the patch, use the following command to reconfigure the Standard Agent:

```
./installccstor -configure
```

For more information about reconfiguring the Standard Agent, see the *CommandCentral Installation Guide*.

installccstor command lists unsupported options (1402292)

On a UNIX Standard Agent, when you run the `installccstor` command from `/opt/VRTS/install` the following usage message displays:

```
The -configure, -license, or -security option is required when
installccstor is not run from the install media.
```

This message is incorrect. The `-license` and `-security` options are not required and are not supported.

Incorrect folder appears when clicking View ReadMe in Windows installer (1449592)

When you install or upgrade a Standard Agent on Windows, in the final panel of the installation wizard, if you click the View ReadMe link, an incorrect folder appears.

Workaround

Select (check) the View ReadMe checkbox and click Finish. The correct README file displays.

Standard Agent silent install fails with message about inability to open log file at line 966 (1363772)

When you perform a silent install of the Standard Agent on UNIX, installation may fail with the following message:

```
pl_log cannot open <location of log> at CPI/common/misc.pl line 966
```

This message displays if you omitted the `-responsefile` option from the command.

For more information about Standard Agent silent installs, see the *CommandCentral Installation Guide*.

In Push Install Utility, Add IP button not enabled after pasting host name (1423059)

In the Push Install Utility, in the Select Hosts for Managing Installations dialog box, if you use your mouse to paste the name or IP address of a host in the Host

Name or IP Address field, the Push Install Utility does not enable the Add IP button.

Workaround

In the Host Name or IP Address field, either paste the text using your keyboard or, if you already used your mouse to paste the text, press a key on your keyboard. The Push Install Utility enables the button.

Data and configuration files remain after uninstalling the Standard Agent from a Linux host (1397051)

If you uninstall the Standard Agent from a Linux host and do not choose to save data and configuration files, after the Standard Agent uninstalls, files remain in the /opt/VRTSccs folder. You can safely delete these files.

Error message appears when uninstalling Symantec Product Authentication Service on a Windows Control Host (1368709)

On a Windows host, after you upgrade a Control Host to version 5.2, if you try to uninstall the Symantec Product Authentication Service, the following error message appears:

```
Another application has exclusive access to file -
"Install_directory\Security\Authentication\systemprofile\certstore\keystore\KeyStore.lock
file"
```

The Authentication Service was used by your previous version of the Control Host. The 5.2 Control Host does not depend on the Authentication Service.

If you need to uninstall the Authentication Service, then you need to uninstall the Control Host first.

Symantec Production Authorization Service stops after uninstalling CommandCentral from a Windows host (1465585)

When you uninstall CommandCentral 5.2 from a Windows host, the Symantec Production Authorization Service stops.

Workaround

If there are other Symantec products that use the Authorization Service, open Windows Service Control Manager and start the Symantec Production Authorization Service.

CommandCentral Storage installations fail on UNIX hosts if installed on auto-mounted volumes (1173776)

If you install the Management Server or the Standard Agent on UNIX from an auto-mounted volume, the installation fails with the message that the required disk space is not available. The installation fails even when you have the required disk space for the installation.

Workaround

Ensure that you have the required disk space.

See "System requirements for the Management Server" on page 26.

See "System requirements for the Standard Agent" on page 27.

Use the -nospacecheck option of the installer.

`./installccstor -nospacecheck`

The -nospacecheck option skips the disk space check and lets you proceed with the installation.

Uninstalling CommandCentral from UNIX fails (1673272)

When you use the uninstall script from `/opt/VRTS/install` to uninstall the CommandCentral Management Server or Standard Agent, an error message that includes the following might appear:

`Couldn't load Crypt::Blowfish_PP: Can't locate Crypt/Blowfish_PP.pm`

This error occurs when the host runs a version of VRTSperl that is higher than the version that CommandCentral ships with. Because of this error, uninstallation fails.

Workaround

Uninstall the Management Server or Standard Agent with the product installer.

To uninstall the Management Server with the product installer

1 Log on to the host from which you want to uninstall the Management Server.

2 In an operating system console, navigate to the following directory:

installer_location/MS/sol_sparc

Where *installer_location* is one of the following:

■ The directory in which you extracted the tar file

■ The location in which the DVD is mounted

3 Type the following command:

`./installer`

4 At the Task Menu, type U and press Enter.

Follow the prompts to uninstall the Management Server.

To uninstall the Standard Agent with the product installer

1 Log on to the host from which you want to uninstall the Standard Agent.

2 In an operating system console, navigate to the following directory:

installer_location/MH/*platform*

Where:

installer_location	is one of the following: ■ The directory in which you extracted the tar file ■ The location in which the DVD is mounted
platform	is one of the following: ■ aix ■ hpux ■ linux_i686 ■ sol_sparc

3 To uninstall the Standard Agent, type the following command:

`./uninstallccsmh`

Follow the prompts to uninstall the Standard Agent.

Installer freezes during install of the Management Server on a Windows host that runs Storage Foundation (1800374)

When you install the Management Server on a host that includes Storage Foundation for Windows, the CommandCentral installer may freeze.

Workaround

Before you proceed with installation, stop the following services:

■ Veritas Action Agent (actionagent)

■ Veritas GridNote (vxgn)

■ Veritas Storage Agent (vxvm)

■ Veritas Enterprise Administrator Service (vxob)

In Windows' Task Manager, ensure that the vxsvc.exe process is not running. vxsvc.exe is the process name for the Veritas Enterprise Administrator Service.

Install on a HP-UX host may fail if run from a Linux NFS server's mounted volume (1742038)

Installation (clean install or upgrade) of the CommandCentral Storage package on a host that is running the HP-UX operating system may fail. This issue relates to NFS and occurs if you run the installer from a mount volume that is located on a Linux NFS server.

The Linux NFS server may not be providing a lock to the HP-UX admin commands, such as swinstall and swcopy. If so, it is possible that the Linux NFS server was created without the insecure_lock lock option being provided. When this issue occurs, the following lock creation error displays:

```
ERROR: <host_name>:/<mount_location>:

This target or source is already in use either within this same
session or by another session. A read or write lock was denied.

* Source connection failed for <host_name>:<mount_location>
```

Workarounds: Use either workaround A or B as appropriate for your situation:

A. Run the installer from a host that is running an operating system other than Linux, and mount that host on the HP-UX host.

B. Edit the /etc/exports file to add the two required options, insecure_locks and insecure (if they are missing).

These options allow the HP-UX admin commands to create a read lock on the file system. You want the following entry in /etc/exports file on the Linux host to appear as follows:

```
/cc_downloads/cc_builds *.*(rw)
```

To edit the /etc/exports file

1   On the Linux host, open the /etc/exports file in a text editor.

2   Add the two required options, insecure_locks and insecure (if needed).

3 Edit the `/etc/exports` file as follows:

</cc_downloads/cc_builds> `*.*(rw,sync,insecure_locks,insecure)`

where

</cc_downloads/cc_builds> is the NFS name you used to create the NFS server,

`*.*` represents any machine can use this NFS server, and

data in the () are the options provided to the NFS.

4 Run the following command:

`` `exportfs -ra` ``

5 Run the installer again.

Installation of the Management Server fails on a Solaris 10 host with local zones and Storage Foundation 5.1 (1843473)

If you try to install the Management Server on a Solaris 10 host that has one or more local zones configured and Storage Foundation 5.1 installed, installation fails with the following message:

```
Installation will terminate now on <hostname> due to the presence of
modified Symantec packages.
```

Workaround

Do one of the following:

■ Use a CPI patch

■ Change the value of SUNW_PKG_ALLZONES from false to true

To use a CPI patch

1 Go to the Symantec Operations Readiness Tools Web site to download the CPI patch.

http://sort.symantec.com

2 Follow the instructions in the patch's readme.

To change the value of SUNW_PKG_ALLZONES from false to true

1 On the host where you want to install the Management Server, go to `/var/sadm/pkg/VRTSat`

2 Open the file `pkginfo`

3 Change the value of SUNW_PGK_ALLZONES from false to true.

4 Install the Management Server.

5 After installation completes, change the value of SUNW_PGK_ALLZONES from true to false.

Cannot uninstall the VRTSsfmh 2.1 package from a Windows host (1893083)

If you try to uninstall the VRTSsfmh 2.1 package from a Windows host, the uninstall wizard runs, but it may not remove the package. This issue happens when the Unified Agent is configured to report to the CommandCentral Management Server. Before you uninstall the VRTSsfmh 2.1 package, unconfigure the Unified Agent from the CommandCentral Management Server.

"Cannot downgrade the Symantec Authorization service" appears during upgrade on Windows (1861783)

The Symantec Product Authorization Service is a shared component that runs on the Management Server. The Authorization Service typically installs in one of the following ways:

- Through `VERITAS Authorization Service.msi`. When you install the Management Server, the CommandCentral product installer invokes this installation package to install the Authorization Service.

- Through `VRTSatzsetup.exe`. This executable is included with the ICS installer, which is available from FileConnect. You might use this executable to manually install the Authorization Service.

When you do either of the following:

- Upgrade the Management Server through the CommandCentral product installer

- Upgrade the Symantec Product Authorization Service through the ICS installer (`VRTSatzsetup.exe`)

You might receive the following error message:

`Cannot downgrade the Symantec Authorization service.`

This issue occurs in the following scenarios:

- The Authorization Service was originally installed through the CommandCentral product installer and you try to upgrade the Authorization Service through the ICS installer (`VRTSatzsetup.exe`).

- The Authorization Service was originally installed through the ICS installer (`VRTSatzsetup.exe`) and you upgrade the Management Server through the CommandCentral product installer.

Workaround

To upgrade the Authorization Service, use the same installer that you used to originally install the service.

Error occurs during upgrade or uninstall of Control Host on Solaris (2147140)

An error occurs when you do either of the following on a Solaris host:

- Upgrade a 5.1, 5.1.1, or 5.1.2 managed host with Fibre Channel switch and array management capabilities to a 5.2 Control Host

- Uninstall the 5.2 Control Host

The following error displays:

```
CPI ERROR V-9-0-0 Failed to open for reading!
```

Workaround

This issue is fixed in a patch. To download the patch, go to the Symantec Operations Readiness Tools Web site.

https://sort.symantec.com/patch/detail/4206

Cannot extract VRTS_CommandCentral_5.2_ICS_MULTI.tar.gz with WinRAR utility (2151898)

`VRTS_CommandCentral_5.2_ICS_MULTI.tar.gz` is available through FileConnect. This compressed image contains files that you can use to install or upgrade shared components. If you download this file and try to extract it with the WinRAR utility, the following error message appears:

Cannot copy file: Cannot read from the source file or disk.

We recommend that you use the WinZip utility to extract the file on a Windows host.

Database upgrade errors during Management Server upgrade (2033234)

When you upgrade the Management Server to version 5.2, the following error message may appear before the installer starts the database upgrade:

```
ERROR: vxdbms_start_db: Unknown error. The return error code (7).!!!
```

```
ERROR: vxdbms_start_db: Unknown error. The return error code (7).!!!
```

If you resume the upgrade before you resolve the error, the following error message appears:

```
ERROR: DB upgrade failed...
```

This issue happens when:

■ The Management Server is installed on Windows in a non-default directory

■ Automatic short file name generation is disabled

Workaround

If you encountered the first error message and you have not yet proceeded with the upgrade, update server.conf and databases.conf.

See "To update `server.conf` and `databases.conf`" on page 70.

If you encountered the first error message, proceeded with the upgrade, and encountered the second error message which states database upgrade failed, do the following:

1. Update server.conf and databases.conf.

    See "To update `server.conf` and `databases.conf`" on page 70.

2. Launch the database upgrade.

    See "To launch the database upgrade" on page 71.

3. Start CommandCentral services.

    See "To start CommandCentral services" on page 72.

4. Configure the Storage Change Manager server.

    See "To configure the Storage Change Manager server" on page 72.

5. Configure the Storage Change Manager user interface.

    See "To configure the Storage Change Manager user interface" on page 73.

6. Configure the collectors.

    See "To configure the collectors" on page 74.

7. Run the mode change script.

    See "To run the mode change script" on page 74.

To update server.conf **and** databases.conf

1   Go to the following directory:

    install_directory\VxDBMS3\Server\conf\

2   Open server.conf in a text editor.

3   Add the following text:

    -c 1750M -cl 1500M -ch 1900M -gn 50 -n VERITAS_DBMS3_*host_name*
    -xtcpip(port=2994) -ct+ -gd DBA -gk DBA -gl DBA -gp 4096 -ti 0
    "*install_directory*\VxDBMS3\Server\conf\vxdbms.db"

    Where:

install_directory	is the directory where you installed CommandCentral program files.
host_name	is the host name of the Management Server. This host name should match the host name in the ASA service name: Adaptive Server Anywhere - VERITAS_DBMS3_*hostname*

4   Save and close *server.conf*.

5   Open *databases.conf* in a text editor.

6   Add the following text:

    "*data_directory*/CommandCentral Storage Data/Database/ccstor.db" -n
    ccstor -m

    "*data_directory*/CommandCentral Storage Data/Database/ccstordm.db"
    -n ccstordm –m

    Where *data_directory* is the directory where you installed CommandCentral data files.

7   Save and close databases.conf.

8   Open a command prompt and type the following command:

    `Net start ASANYs_VERITAS_DBMS3_host_name`

    Where *host_name* is the host name of the Management Server. This host name should match the host name in the ASA service name: Adaptive Server Anywhere - VERITAS_DBMS3_*hostname*

To launch the database upgrade

◆ Type the following command:

```
"install_directory\CommandCentral
Storage\Tools\DbUpgrade\RunSQLScripts.bat" "install_directory"
"data_directory\CommandCentral Storage Data\Database" host_name
```

Where:

install_directory	is the directory where you installed CommandCentral program files.
data_directory	is the directory where you installed CommandCentral data files.
host_name	is the host name of the Management Server.

For example:

```
"D:\My install location\CommandCentral
Storage\Tools\DbUpgrade\RunSQLScripts.bat" "D:\My install
location" "D:\My install location\CommandCentral Storage
Data\Database" CCS-Win2k8
```

To start CommandCentral services

◆ Type the following commands, one by one:

```
Net stop VRTSaz
```

```
Net stop VRTSat
```

```
Net start ASANYs_VERITAS_DBMS3_host_name
```

```
Net start VRTSpbx
```

```
Net start VRTSat
```

```
Net start VRTSaz
```

```
Net start vxtrapd
```

```
Net start VRTShal
```

```
"install_directory\CommandCentral Storage\HAL\bin\halagentcfg.exe"
start-all
```

```
Net start vxasd
```

```
Net start vxamccs
```

```
Net start vximporterd
```

```
Net start dmexplorer
```

```
Net start vxsicld
```

Where *install_directory* is the directory where you installed CommandCentral program files.

To configure the Storage Change Manager server

1   Open Windows Registry Editor and locate the following registry key:

    HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\VRTSjre\JRE1.5

2   For the **Path** value, copy the **Data** location.

3   Locate the following registry key:

    HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\CommandCentral SCM Server

4 Edit the value of the **JavaExePath** entry with the value that you copied in step 2.

5 Open a command prompt and type the following command:

```
"install_directory\CommandCentral Storage\HAL\bin\perl.exe"
"install_directory\CommandCentral Storage\Storage Change
Manager\inst\scms_inst_uninst.pl" -i
"install_directory\CommandCentral Storage\Storage Change Manager"
-d "data_directory\CommandCentral Storage Data\Data\Storage Change
Manager" -l "data_directory\CommandCentral Storage
Data\Log\Storage Change Manager" -c "data_directory\CommandCentral
Storage Data\Conf\Storage Change Manager" -P
"install_directory\CommandCentral Storage\HAL\bin\perl.exe" -S
-I -b machine_config >> "%allusersprofile%\Application
Data\VERITAS\VCC\52\scms_postinstall.log"
```

Where:

install_directory	is the directory where you installed CommandCentral program files.
data_directory	is the directory where you installed CommandCentral data files.
machine_config	is either **32** or **64**, which corresponds to a 32-bit or 64-bit operating system.

To configure the Storage Change Manager user interface

◆ Open an operating system console and type the following command:

```
"install_dir\CommandCentral Storage\HAL\bin\perl.cmd"
"install_dir\VRTSsmweb\webgui\sm\plugins\scm\inst\scmui_postinst_actions.pl"
-l "%allusersprofile%\Application
Data\VERITAS\VCC\52\scmui_postinstall.log"
```

Where *install_dir* is the directory where you installed CommandCentral program files.

To configure the collectors

1   Open Windows' Services utility and verify that the Veritas Storage Foundation Messaging Service is running.

2   If the service is not running, start it.

3   Open an operating system console and type the following command:

    ```
    "install_directory\CommandCentral Storage\bin\perl.exe"
    "install_directory\CommandCentral Storage\bin\ccch_configure.pl"
    configure --explorer-name all --password password >>
    "%allusersprofile%\Application
    Data\VERITAS\VCC\52\CCCHConfigOutput.log"
    ```

    Where:

install_directory	is the directory where you installed CommandCentral program files.
password	is the password of the Management Server's Agent principal account. The default password is agent123

To run the mode change script

◆   Open an operating system console and type the following command:

    ```
    "install_directory\CommandCentral
    Storage\Tools\ModeChangeScripts\Mode_Change.bat" mode -force
    ```

    Where:

install_directory	is the directory where you installed CommandCentral program files.
mode	is one of the following:

    - **CCS**
      This option enables CommandCentral Storage and disables CommandCentral Storage Change Manager.
    - **SCM**
      This option enables CommandCentral Storage Change Manager and disables CommandCentral Storage.
    - **ALL**
      This option enables both CommandCentral Storage and CommandCentral Storage Change Manager.

Management Server and database issues

The following are known issues that you might encounter with the Management Server or database.

Management tasks not terminated when Management Server can no longer contact Standard Agent (604446)

If a management task (for example, a create LUN operation) is in process, and the Management Server loses contact with the Standard Agent, the process may take up to 60 minutes to terminate.

Shared components stop-start order (856750)

If the Symantec Private Branch Exchange (PBX) is stopped and restarted, then the Symantec Product Authentication and Authorization Services need to be stopped and restarted in the correct order.

Here is the proper stop-start order for these shared processes:

1. Stop the Authorization Service.

2. Stop the Authentication Service.

3. Stop PBX.

4. Restart PBX.

5. Restart the Authentication Service.

6. Restart the Authorization Service.

Status of user-created HAL process does not display when running vxccs status (1437246)

After you create a new Hardware Abstraction Layer (HAL) process—for example, a process under which you want to run a new explorer—when you run the command `vxccs status`, the status of that new process does not display.

Workaround

Use the command `halagentcfg list-processes` to verify the status of the user-created process.

To use the command halagentcfg list-processes

1   On the host on which you created the process, open an operating system console and log in as root (UNIX) or as a user with administrator-level privileges (Windows).

2   Change to the Hardware Abstraction Layer (HAL) bin directory. By default, the directory is:

- HP-UX, Linux, Solaris: `/opt/VRTSccs/VRTShal/bin`

- AIX: `/opt/VRTShal/bin`

- Windows: `\Program Files\VERITAS\CommandCentral Storage\HAL\bin`

3   To see the status of HAL processes, type the following command:

    `halagentcfg list-processes`

The status of the processes display.

Array and CIMVAIL log files consume large amount of disk space (1458508)

You may notice a decrease in disk space due to the array and CIMVAIL log files growing to large sizes. This occurs if you change the debug level of the array and CIMVAIL explorers to a level higher than 1.

Workaround

Do the following:

- Delete the log files

- Change the explorer's debug levels to either 0 or 1
For information about configuring explorers, see the *CommandCentral Administrator's Guide*.

Refreshing the storage explorer fails on a host with no physical Fibre Channel HBAs (1798710)

If you run the Management Server or Standard Agent on a host that has no physical HBAs and you refresh the storage explorer, the task fails. If you view the Task Status pane, the status detail for the task is as follows:

```
Detect Devices for Devices failed. Explorer Name: StorageExplorer.
ExplorerID: StorageExplorer@host_name.com.
StorageExplorer SNIA Common HBA API library is not properly
```

```
installed on this computer (V-32-35-73)
Request Failed
```

You can ignore this error. Even though the error appears, rediscovery completed successfully.

The command "net start VRTSsmweb" fails (1806029)

If you run the command "net start VRTSsmweb" on a Windows Management Server, the command may fail:

```
The Veritas Storage Management Web Console service is starting........

The Veritas Storage Management Web Console service could not be
started.
```

Workaround

Use Windows' Service Control Manager to start the Veritas Storage Management Web Console service.

The halnetcheck utility fails (1795572)

If you run the halnetcheck utility, an error may appear. For example, if you run the command "halnetcheck check-connectivity -h *host_name*" the following error may appear:

```
Failed to contact host_name halnetcheck.

Segmentation fault
```

This error occurs when the current working directory from which you run the utility is not writable by the login user. The utility attempts to open and write to a log file in the current working directory. If that directory is not writable, halnetcheck cannot create the file, and the utility fails.

Workaround

Run the command from a writable directory.

Standard Agent issues

The following are known issues that you might encounter with the Standard Agent.

Explorers do not start after rebooting a SUSE Linux Standard Agent (1469398)

After you reboot a SUSE Linux Standard Agent, the Standard Agent's explorers do not start.

Workaround

Start the explorer processes manually.

To start the explorer processes manually

1   On the Standard Agent, open an operating system console and log in as root.

2   Type the following command:

/opt/VRTS/bin/vxccs start

The explorer processes start.

CommandCentral services do not start after you reboot a Windows Standard Agent (1799326)

After you reboot a Windows Standard Agent, CommandCentral services may not start.

Workaround

You can use the vxccs script to restart the services. However, to ensure that the services start after you reboot the host, you need to create or modify the ServicesPipeTimeout registry setting.

To modify the ServicesPipeTimeout registry setting

1   Click **Start > Run**.

2   In the Run dialog box, type **regedit** and click **OK**.

3   In Registry Editor, navigate to the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

4   Do one of the following:

If the ServicesPipeTimeout value is present	Proceed to step 5.
If the ServicesPipeTimeout value is not present	Do the following: ■ Click **Edit > New > DWORD Value**. ■ Type **ServicesPipeTimeout** and press **Enter**.

5   Right click **ServicesPipeTimeout** and click **Modify**.

6   In the Base field, select **Decimal**.

7   In the Value data field, enter **300000** and click **OK**.

The value 300000 is in milliseconds and is equivalent to five minutes.

Standard Agent services do not start after reboot of SUSE Linux host (2143660)

After you reboot a SUSE Linux host, some services on the Standard Agent may not start. For example, the Local HAL Manager and explorers may not start. As a result, the condition for the Standard Agent may be Stopped or Faulty.

Workaround

Do the following:

■ Restart the services.

■ To prevent the issue from happening again, modify /etc/init.d/.depend.start

To restart the services

1   Log on to the Standard Agent and open an operating system console.

2   To start the services, type the following command:

    /opt/VRTS/bin/vxccs start

To modify /etc/init.d/.depend.start

1   Open /etc/init.d/.depend.start in a text editor.

2   Add the following line:

vrtshal: vxpbx_exchanged

3   Save and close the file.

Unified Agent issues

The following are known issues that you might encounter with the Unified Agent.

Discovery issues for the Unified Agent

Table 6-1 identifies the discovery issues that you might encounter with the Unified Agent. The issues that you encounter depend on the version of VRTSsfmh that is installed on the Unified Agent. The table identifies if the issue affects version 2.1

(which includes 2.1 RP1), version 3.0, and version 3.1. An X indicates that the issue affects that version.

Table 6-1 Unified Agent discovery issues

Known issue	2.1	3.0	3.1
A host's physical memory is not discovered.	X		
A Linux guest operating system is not discovered as a virtual machine.	X		
The port state for SCSI targets is not discovered.	X		
The connection protocol for internal disks and iSCSI disks is not available. As a result, the IDE storage is not counted in the Storage Consumption Detail report and the disk's capacity is counted as fibre storage in the Online Storage Capacity reports.	X	X	X
If an internal disk is not initialized by Veritas Volume Manager, disk size is not available. As a result, detailed information about the OS handle is not available and the IDE storage is not counted in reports. This issue affects UNIX hosts.	X	X	X
A file system's non-super user capacity is not discovered. As a result, the used capacity of the file system is higher than expected.	X		
If a file system is not initialized by Veritas Volume Manager, the correlation of the file system to the device path is not available. As a result, reports do not include the file system's capacity (in the Online Storage Capacity Summary report, the storage is counted as unknown consumption).	X	X	X
NFS and CIFS shares are not discovered.	X	X	X
A volume's disk group free capacity and disk group capacity are greater than the capacities reported by the CommandCentral Standard Agent.	X		
If LUNs are not initialized by Veritas Volume Manager, CommandCentral cannot correlate the LUNs to volume managers, file systems, or applications. As a result, LUN capacity is classified as Unknown in the Storage Consumption report and as Potentially Unassigned LUNs in the Allocated LUNs Reclamation report.	X	X	X
CommandCentral cannot correlate Veritas Cluster Server with databases (MS SQL, Oracle, Exchange, and DB2).	X	X [1]	X [1]

Table 6-1   Unified Agent discovery issues *(continued)*

Known issue	2.1	3.0	3.1
If the name of a redo log file includes a space, CommandCentral cannot discover the file.	X		
For DB2 and Oracle instances, tablespaces on raw Veritas Volume Manager volumes are not discovered.	X		
If the Unified Agent discovers an MS SQL instance that Veritas Operations Manager also discovers, discovery of the database fails in Veritas Operations Manager.		X [2]	
If a database resides on a file system that does not reside on a Veritas Volume Manager volume, end-to-end correlation with the LUN is not available. If a database resides on a device that is not a Veritas Volume Manager volume, end-to-end correlation with the LUN is not available.	X	X	X
If the name of a VCS volume resource does not match the name of a Veritas Volume Manager volume, CommandCentral cannot correlate the VCS resource with the volume. As a result, the storage capacity of the volume is not accounted for in the online shared storage capacity for the cluster.	X	X [2]	
The used size and available size for Sybase databases is incorrect. The used size is always reported as equal to the total size, which means the available size is always 0.		X	
The Unified Agent cannot discover Oracle RAC 11g R2 on Linux.		X	X
If a redo log file is created on a raw Veritas Volume Manager volume, CommandCentral cannot correlate the tablespace to the database storage unit.	X	X [2]	
The association between Sybase log segments and logical devices is not available.		X	
The total size of logical devices is not discovered for Sybase databases.		X	X
The association between Sybase databases and LUNs is not available.		X	

Table 6-1   Unified Agent discovery issues *(continued)*

Known issue	2.1	3.0	3.1
The following information is not discovered for Emulex HBAs on Solaris hosts: ■ Firmware version ■ Driver information ■ HBA mode ■ Serial number	X	X	X
If the Unified Agent discovers an Oracle RAC database and a standalone or clustered database, and the databases have the same Oracle home directory, CommandCentral identifies the standalone or clustered database as a RAC database.	X	X	X
If an internal disk is not initialized by a volume manager (Veritas Volume Manager or logical volume manager), the IsDirectAttached attribute is not discovered correctly on HP-UX hosts.	X	X	X

[1] The issue does not affect correlation with Oracle databases in VRTSsfmh version 3.0 and 3.1.

[2] This issue is fixed in 3.0 RP1.

Console issues

You might encounter the following known issues as you use the CommandCentral Storage Console.

Device configuration name does not change after modification (853400)

The Console's Edit Device Configuration command does not change the device configuration name.

Workaround

First remove the device manager, then remove the arrays managed by the device manager. Then re-add the device.

Do not use an existing IP address for array configuration (582094)

The array configuration dialogs do not check whether a specified IP address is already in use. When configuring a new array or editing an existing configuration, care should be taken not to specify an IP address that is already in use for a configured array.

HP EVA: Disabling discovery of Management Appliance does not disable discovery of arrays (614523)

If you edit the configuration for a Management Appliance host that manages HP EVA arrays and deselect Enable Discovery, the Management Appliance changes to the inactive state. However, CommandCentral continues to discover the arrays it manages.

Workaround

Disable discovery for each managed array individually.

Mismatch between time on Management Server and time displayed in scheduling dialogs (851525)

The Schedule Task controls in dialog windows display date and time values according to the clock on the local computer. However, the scheduling of tasks is actually based on the clock on the CommandCentral Management Server. If the Console user is in a different time zone from the Management Server, therefore, the time displayed might not match the time on the Management Server.

Workaround

Be sure to specify dates and times with regard to the Management Server host, not the local client.

Port Bundle Builder Tool displays only one fabric (629557)

The Port Bundle Builder tool is a feature that involves two switches that are E/TE ported together. The Port Bundle Builder tool should list E/TE ports, even if their Admin status is down. Upon selecting the E/TE port pairs to be bundled, the CommandCentral Storage Port Bundle creation wizard should first complete the operation on the first switch, and then on the second. Both ports should come online. If the operation fails, an error message is returned.

Currently the Port Bundle creation wizard only displays the E/TE port that is Online. Upon selecting the E/TE port pairs to be bundled, the switch performs a port bundle creation for the first switch. The ports go Offline on the switch and the CommandCentral Storage GUI stops. It does not complete the operation on the second switch. This results in an incomplete operation. Since the ports are down, there is no other way to complete the Port Bundle operation using CommandCentral Storage.

There is currently no workaround. Do not use the Port Bundle creation/edit feature in 5.2.

The Topology Map's Print Preview displays a blank page (1206846)

The Topology Map's Print Preview displays a blank page in the following situations:

- In Internet Explorer, when you open the Topology Map in a new browser window and click the Print Preview icon

- In Firefox, when you click the Print Preview icon either from the Console or after you open the Topology Map in a new browser window

Workaround

If you want to print the Topology Map in Internet Explorer, do either of the following:

- Without opening the Topology Map in a new browser window, click Print Preview

- Save the Topology Map as an image and then print the saved image

If you want to print the Topology Map in Firefox, you can save the Topology Map as an image and then print the saved image.

For more information about saving the Topology Map as an image, see the *CommandCentral Storage User's Guide.*

Favorites link for the Host Editor no longer works (1456338)

If you had a favorites link for the Host Editor in your previous version of CommandCentral Storage, the link no longer works after you upgrade to CommandCentral 5.2. The link no longer works because the Host Editor was replaced by the Pattern Based Correlation Wizard and the CSV Based Correlation Wizard. You should edit your favorites to remove the link to the Host Editor.

Table column values that contain plus signs are not saved (1795869)

When you save any table that contains a plus sign (+) in any value in the table columns, the value appears as "#NAME" in the exported file. For example, Oracle database instances contain a plus sign in their display names, so they exhibit this issue.

There is no workaround.

Edit Remote Host wizard and Unconfigure Remote Host wizard contain information about incorrect host (1944264 and 1944318)

If you use the Edit Remote Host wizard or Unconfigure Remote Host wizard and close them without pressing Cancel or Finish, the session remains open. As a

result, if you use the wizards for a different host, the fields in the wizards contain information about the previous host.

Workaround

Do one of the following:

- In the wizard, click **Cancel**.
- Refresh the Host Management pane.

You can now open the wizard in a new session.

Exception appears in the Host Management pane (2133634)

When you click the Host Management tab, an exception might appear in the Console. The exception states that a runtime error occurred.

Workaround

Click your Web browser's Refresh icon.

"Report: Error rendering report" error appears in the Console (2147074)

When you click a tab in the Console, the following error might appear:

```
Report: Error rendering report
```

Workaround

Click your Web browser's Refresh icon.

Logs and Database tabs do not appear in the Console (2169442)

When you click Settings > Diagnostics, the Logs tab and the Database tab may not appear in the Diagnostics pane.

Workaround

This issue is fixed in a patch. To download the patch, go to the Symantec Operations Readiness Tools Web site.

https://sort.symantec.com/patch/detail/4236

Discovery and discovery data issues

The following issues relate to the discovery of your hardware and software and the data that CommandCentral Storage discovers. The discovery data issues typically pertain to the information that appears in the **Managing** pane. Issues that relate to the data that appears in reports are covered in another section.

Disk state not discovered (859207)

On UNIX hosts, CommandCentral does not discover the state of disks in VxVM volumes.

Incomplete information displayed for newly discovered objects (865845)

When an object is discovered for the first time, there is a brief period of time during which the CommandCentral Storage Console displays incomplete information about the object. The incomplete information is reflected in the object view and also may be reflected in reports and other views where information about multiple objects is rolled up. Currently there is no indication that the information being displayed is incomplete.

Incorrect LUN capacity estimates when CX Meta LUNs created from mixed RAID groups (1016679)

If you create a CX Meta LUN from mixed RAID groups, the LUN is referred to as a mixed Meta. Due to an issue in CommandCentral Storage 5.2, such mixed Meta LUNs appear within both RAID groups. This causes incorrect LUN capacity estimates for both RAID groups. The LUN capacity total in both RAID groups will be higher than expected.

There is no workaround. If the production environment contains mixed Meta LUNs, then you should be aware that such a discrepancy in existing LUN capacity can occur.

Discovery failure for storage arrays configured as SMI-S managed arrays (1185347)

Device discovery of SMI-S managed arrays may fail if the operational state of the array is in either an attention or a failed state.

To determine an array's state

1   Click on an array to go to the array's overview pane.

2   Click the Monitoring tab.

3   Under State Collectors, check the "OperationalState" collector value.

There is no workaround for this issue.

Windows Logical Manager not discovered on Windows Server 2008 host that includes Veritas Volume Manager (1402934)

If a Windows Server 2008 host includes Windows Logical Disk Manager (LDM) and Veritas Volume Manager 5.1, CommandCentral Storage cannot discover a few LDM attributes, even though capacity and correlation information are accurate.

Consumption information missing for shares mounted on a Windows host (1169224)

CommandCentral does not discover consumption information for shares mounted on a Windows host. Because of this, the following occurs in the Console:

- In the Storage Capacity Detail report, the Shares/Exports table does not display values for consumer and consumer mount points when the share is mounted on a Windows host.

- In a hosts' overview pane, the Remote Shares Consumed table does not display data for Windows hosts when the host has mounted a share.

- In the overview pane for a NetApp share, the Consumers table does not display data for NetApp shares mounted on a Windows host.

Wrong operating system displays for a storage view (1232117)

After you build a storage view for SMI-S managed IBM DS4000 storage arrays or Engenio (LSI) storage arrays, the OS Type for that storage view displays as Solaris, even if that is not the correct operating system.

There is no workaround.

Product name and version do not display for Sybase 15 instance (1439468)

When you view the Overview pane for a Sybase 15 instance, the product name and version of that instance may not appear. This occurs when the instance's ASE directory name and OCS directory name were either not supplied or were entered incorrectly when you configured the instance for discovery.

Workaround

Edit the device's configuration to supply the instance's ASE directory name and OCS directory name.

For more information about editing a device's configuration, see the *CommandCentral Administrator's Guide*.

> **Note:** Enter the directory name without the trailing slash. For example,
> `/xyz/ASE-15_0/bin/` is incorrect where as `/xyz/ASE-15_0/bin` is correct.

Incorrect name displayed for file systems on unmounted or unnamed volumes (864757)

When a Standard Agent has unmounted and/or unnamed VxVM volumes that contain file systems, then the file systems' names might display incorrectly in the CommandCentral Storage Console. Specifically, the error occurs in the host's object view, Volumes tab, Volumes table, File System column.

The name displayed might be the name of the volume itself, or it might be the string *Volume-GUID* on *fully-qualified-host-name*.

Example:

```
\?\Volume{75a7abe6-ff5a-4398-8de7-a99b26306fe0}\ on
host1.example.com
```

There is no workaround.

Array Storage Summary report displays incorrect capacity for IBM DS6000 and DS8000 storage arrays (1437378)

When you view the Overview pane for a IBM DS6000 or DS8000 storage array, in the Array Storage Summary report, the total capacity of the extent pool may not equal the total physical configured capacity. This occurs due to the multiple levels of virtualization involved in IBM DS storage arrays.

Virtualization Server Claimed Capacity attribute displays incorrect value (1447060)

When you view a virtualization server's Attributes pane (Managing > Hosts and HBAs > Virtualization Servers > *click a server* > Attributes), the Attributes table includes the attribute "Virtualization Server Claimed Capacity (GB)." The value of this attribute always displays "0."

Workaround

If you want to view a virtualization server's claimed capacity, scope the Host Virtualization Summary report (Reporting > Storage > Host Virtualization) to the virtualization server.

Console shows disk as part of an Oracle ASM disk group after it was removed from the disk group (1823721)

If you remove a disk from an Oracle ASM disk group, the Console continues to show the disk as part of that disk group until one of the following occurs:

■ You add the disk to another disk group

■ The disk is no longer accessible to the ASM instance

Even though the Console continues to show the disk as part of the disk group, the capacity values for the disk group do not include the disk.

Duplicate device handles appear for an ESX server after migrating discovery from SMI-S to VI SDK (1451189)

If you migrate discovery of an ESX server from SMI-S to VI SDK and you have a Standard Agent installed on the ESX server, when you view the ESX server's device handles, duplicate device handles appear.

Workaround

If you remove the Standard Agent from the ESX server, CommandCentral Storage removes the duplicate device handles once the database purge runs.

Celerra explorer does not discover all file systems (1802239)

CommandCentral Storage discovers default file systems (uxfs) and raw file systems (rawfs) for an EMC Celerra unified storage system.

CommandCentral Storage does not discover the following types of file systems for an EMC Celerra unified storage system:

■ Mount

■ Group

■ Mirrored

■ Migration

Hitachi HiCommand WMS storage array appears twice after upgrade (1796494)

If CommandCentral discovers a Hitachi HiCommand WMS storage array before you upgrade to 5.2, the device appears twice in the Console after you upgrade. The discovery state for one of the devices displays as missing. You can either

manually delete the missing array or you can wait until CommandCentral automatically purges the array from the database.

Because the device appears twice, the following occurs:

- In the Configured Devices Summary table, the state of the discovered device does not appear until the following occurs:

  - You manually delete the missing array or CommandCentral automatically purges the array from the database.
    See

  - You restart the explorer that discovers the device.
    See

- In CommandCentral Storage Change Manager, if a policy is applied on a host-to-LUN pair for the array, then you have to remove the policy and then re-apply it.
  For information about policies, see the *CommandCentral Storage Change Manager User's Guide*.

- In CommandCentral Storage Change Manager, if you view the changes that are associated with the array before you upgraded and click any links that appear in the change message, an error appears.

- In CommandCentral Storage, if click the "Change History" link, when CommandCentral Storage Change Manager loads, the Changes pane does not include the changes that were associated with the array before you upgraded.

To manually delete the missing array

1 In the CommandCentral Console, click **Managing > Storage > Arrays**.

2 In the **Arrays** pane, select the missing array.

3 In the drop-down list, click **Delete Array**. Then, click **Go**.

4 In the **Delete** dialog box, click **OK**.

To restart a device explorer or application explorer

1 On the host on which you want to restart the explorer, open an operating system console and log in as root (UNIX) or as a user with administrator-level privileges (Windows).

2 Change to the directory where the `halagentcfg` script resides. By default, the location is as follows:

   UNIX: `/opt/VRTSccs/VRTShal/bin`

   Windows: `\Program Files\VERITAS\CommandCentral Storage\HAL\bin`

3 To identify the name of the explorer that you want to stop, type the following command:

```
halagentcfg list-explorer-types
```

For more information about each explorer, see the *CommandCentral Administrator's Guide*.

4 To identify the process under which the explorer runs, type the following command:

```
halagentcfg list-explorers --explorer-name ExplorerName --details
```

Where *ExplorerName* is the name of the explorer that you obtained in the previous step.

5 To stop the process under which the explorer runs, type the following command:

```
halagentcfg stop-process --process-name ProcessName
```

Where *ProcessName* is the name of the process that you obtained in the previous step.

6 To start the process under which the explorer runs, type the following command:

```
halagentcfg start-process --process-name ProcessName
```

The process restarts.

Discovery error for EMC Celerra unified storage system if debug level is not 1 (1835013)

If you discover an EMC Celerra unified storage system on a Windows host and change the debug level for the Celerra explorer to something other than 1, a discovery error occurs.

To ensure that CommandCentral discovers an EMC Celerra unified storage system, keep the explorer's debug level at 1.

No correlation between storage pool and associated disk volume for an EMC Celerra unified storage system (1785031)

When you view details about a storage pool for an EMC Celerra unified storage system, the Console does not show the disk volumes from which the storage pool was created.

Incorrect number of file systems for an EMC Celerra unified storage system (1803708)

When you view the Overview pane for an EMC Celerra unified storage system, in the attributes box next to the Physical Capacity chart, the total for the # of NAS File Systems is incorrect. The count is incorrect because it includes the number of root file systems. You cannot mount a root file system to a data mover. The total number of file systems should include only those file systems that you mount to a physical data mover or a virtual data mover.

To view the correct number of file systems, view the NAS File Systems table.

The available capacity for an Oracle ASM disk group is incorrect (1835478)

Oracle calculates the available capacity for an ASM disk group based on the capacity of the failure group that is the smallest. Oracle recommends that all failure groups have the same capacity for better utilization and performance.

CommandCentral Storage calculates the available capacity for an ASM disk group by taking the total capacity of all failure groups and dividing it by the redundancy level. Because of this calculation, if all failure groups do not have the same capacity, CommandCentral Storage displays an incorrect available capacity for an Oracle ASM disk group.

The following example shows how Oracle and CommandCentral Storage calculate the capacity for two failure groups that have different capacities.
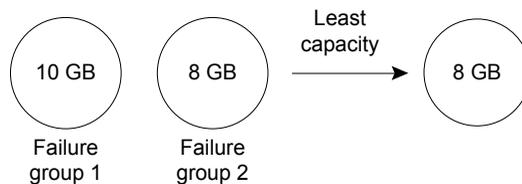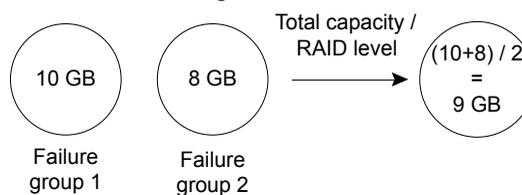
IP address may not display for a Celerra unified storage system (1798405)

If you view the NAS and Unified Storage Systems pane, in the Virtualization NAS and Unified Storage Summary table, an IP address may not appear for a Celerra unified storage system.

Workaround

Restart the NASExplorers process.

To restart the NASExplorers process

1   Log on to the host that discovers the Celerra unified storage system and open an operating system console.

2   Change to the Hardware Abstraction Layer (HAL) bin directory. By default, the directory is:

Solaris	/opt/VRTSccs/VRTShal/bin
Windows	\Program Files\VERITAS\CommandCentral Storage\HAL\bin

3   Type the following commands:

```
halagentcfg stop-process -p NASExplorers
```

```
halagentcfg start-process -p NASExplorers
```

Device mapping only discovered for port 0 of directors for EMC Symmetrix V-Max arrays (1926195)

For EMC Symmetrix V-Max arrays, CommandCentral only discovers device mapping for port 0 of ESCON and FICON directors. If a device is mapped to other ports of ESCON and FICON directors, errors similar to the following appear in the explorer logs:

```
ERROR: Port object not found for <symid:director_id:port_num> hence
deleting binding
```

```
Error V-31-1057-83 Property Uid not set for object of type
[emc_symmetrix_binding].
```

Because of this issue, the following occurs in the CommandCentral Storage Console:

■   Port 0 is the only port that appears in the **Connectivity** pane for an array or adapter.

■ In the device's Overview pane, port 0 is the only port that appears in the **Port Mappings** table.

Connection protocols for SAN and RDM LUNs display as UNKNOWN (2082659)

The connection protocols for SAN and RDM LUNs might display in the Console as UNKNOWN. This issue occurs in the following situations:

■ You have a 5.1.x Standard Agent installed on a guest operating system and you upgrade the Standard Agent to 5.2.

■ CommandCentral Storage discovers a guest operating system through the 5.2 Standard Agent or through agentless discovery before it discovers the associated ESX server.

Note: We recommend that you configure discovery of ESX servers before you discover guest operating systems.

Workaround

This issue is fixed in a patch. To download the patch, go to the Symantec Operations Readiness Tools Web site.

For Solaris hosts: https://sort.symantec.com/patch/detail/4236

For Windows hosts: https://sort.symantec.com/patch/detail/4235

Oracle 11G R2 ASM RAC instances have the same instance names (2136266)

If Oracle 11G R2 ASM RAC instances run on multiple nodes and have unique names (for example, +ASM1 and +ASM2), CommandCentral Storage discovers the same name for each instance. The name for each instance is "+ASM." The capacity-related values are correct for each instance.

Unconfigured raw capacity incorrect for IBM XIV storage arrays (2146627)

CommandCentral Storage incorrectly calculates the unconfigured raw capacity for IBM XIV storage arrays. For example, if you display the Overview pane for an IBM XIV storage array, the Physical: Unconfigured capacity in the Array Storage Summary chart is incorrect.

Workaround

This issue is fixed in a patch. To download the patch, go to the Symantec Operations Readiness Tools Web site.

For Solaris hosts: https://sort.symantec.com/patch/detail/4238

For Windows hosts: https://sort.symantec.com/patch/detail/4239

Host objects for VMware guest operating systems are not created after upgrade to 5.2 (2145819)

After you upgrade your Management Server to 5.2, CommandCentral Storage does not create host objects (managed virtual machines) for the guest operating systems that it discovers using VMware Tools. As a result, you cannot view information about the guest operating systems in the Console.

Workaround

Refresh the VMware explorer.

To refresh the VMware explorer

1   Click **Settings > Host Management**.

2   In the **Hosts** table, click the host that discovers your VMware ESX servers. Typically, the Management Server discovers your ESX servers.

3   In the **Explorers** table, check the **VmwareExplorer**.

4   In the **Explorers** drop-down list, click **Refresh Explorer**. Then, click **Go**.

5   In the **Refresh Selected Explorer(s)** dialog box, click **OK**.

As the refresh operation completes, CommandCentral Storage creates host objects for the associated guest operating systems.

Report issues

You might encounter the following known issues as you use the CommandCentral Storage reports.

LUN capacity displayed as "Assigned to VM" for Sun VM disk slice (637435)

If a Sun disk slice is created on a LUN and the disk slice is given to Sun Volume Manager, then the Storage Consumption reports list the entire LUN capacity as "Assigned To VM"—whether or not other slices are used by file systems or databases.

The assignment capacity is the LUN capacity and not the actual usage capacity of a slice. The assignment also assumes single ownership—meaning that a device handle can be owned by a disk group, a file system, or a database. If the disk slice is used by more than one source, then the report categorizes it as VM, a file system, or a database in the order given.

Example: Three Sun disk slices (A, B and C) are created, each of 1 GB on a LUN of 3 GB. Slice A is used for Volume creation, sliced is used B for directly creating a file system, and slice C is used for directly creating a tablespace. The Storage Consumption reports will display the following:

- 3 GB Assigned to VM
- 0 GB Directly Assigned to File Systems
- 0 GB Directly Assigned to Databases

Emailed report does not reflect column sorting (615330)

If you sort a report on any column other than the default sorted column and then send the report by email, the sorting is not preserved. Only the default sorting is reflected in the emailed report.

There is no workaround.

Table filter does not disable in a custom report (1445762)

If you enable a table filter in a custom report and then try to disable that filter, the filter does not disable.

Workaround

Uncheck the checkbox on which the filter is set.

To uncheck the checkbox on which the filter is set

1   In the Console, click **Reporting > Custom**.

2   In the Custom Reports table, click the name of the report on which you want to remove the filter.

3   In the table that has the filter set, click the **Filter Table** icon.

4   In the Filter Table dialog box, select (uncheck) the checkbox(es) for which you want to remove the filter.

5   Click **OK**.

    The filter disables.

Total values do not display for tables in ad hoc reports (1446963)

In an ad hoc report that contains a table, if you modify the table's settings or filter the table, after the table refreshes, total values does not display in the table's footer.

There is no workaround.

Oracle ASM Disk Group's "ASM DG Used by Other Hosts" value misplaced (1795293)

When you view the **Host Storage Usage** table, on the **Reporting > Storage > Storage Consumption Detail** pane, a capacity value for a particular host can appear in the wrong table cell. In certain circumstances, the value for the **ASM DG Used by Other Hosts (GB)** column appears in the **ASM DG Used: Unknown (GB)** column.

The misplaced table value occurs with a host that contains a standalone Oracle database, which is consuming storage from a shared ASM Disk Group (DG), and when the shared ASM DG has following characteristics:

■ It is shared across at least three hosts

■ It bears a RAC instance on other hosts

There is no workaround.

Unknown storage capacity used by Celerra's storage hierarchy (1800033)

A gap exists between the reported capacity values that are shown for **Physical** and **Logical** storage. You can view this issue in the **Total Unified Storage** bar chart in the **Online Storage Capacity Summary** pane at **Reporting > Storage**. The Celerra's storage hierarchy uses the unknown storage capacity within that gap. The **Logical Unknown category** accounts for this capacity.

There is no workaround.

Distribution of Storage by Interface is displaying "Fibre" for unmasked LUNs (1832384)

Unmasked iSCSI LUNs appear under the **Fibre** category in the **Online Storage Capacity Summary**'s **Distribution of Storage by Interface** pie chart.

Also, when you click the **Fibre** category in the **Distribution of Storage by Interface** pie chart, the **Online Storage Capacity Detail** report appears with its **LUNs** table.

In the **LUNs** table's **Interface** column, the unmasked iSCSI LUNs are marked as **Fibre**.

Workaround: None available.

Allocation of Array Storage by Vendor for EMC displays NetApp arrays (1832996)

This issue is visible if you drill down in Reporting > Online Storage Capacity > Summary > Allocation of Array Storage by Vendor" bar chart, and click a capacity value (other than Logical Virtualizer Source Capacity) for a particular vendor.

For vendors (other than NetApp), the Online Storage Capacity Detail report appears with its NAS and Unified Storage table and Arrays table. The data in the NAS and Unified Storage table is not filtered according to the vendor that was clicked in the Summary pane, so the table's Vendor column includes not only the NAS devices for the arrays for the vendor selected, but also those for other vendor's NAS devices.

Workaround: Use the **NAS and Unified Storage** table's table-settings to filter so that the **vendor** column shows only the applicable vendor.

Reported 3PAR storage capacity numbers do not match (1834265)

If your environment contains configured 3PAR arrays as well as other arrays that have the same RAID configuration as the 3PAR arrays, two entries for that RAID configuration appear in the **Online Storage Capacity Summary** pane's **Distribution of Storage by RAID Level** pie chart. The capacity numbers shown in the **Summary** pane will not match those shown in the **Detail** pane's report.

Workaround: None exists.

Shared virtual machine disks appear multiple times (2074661)

If disks are shared across multiple VMware virtual machines, the disks appear multiple times in the Console. The impact of this issue is as follows:

- In the Storage Consumption Summary report, the claimed capacity of the disks is counted multiple times.

- In the Host Virtualization reports, the disk capacity is included multiple times where ever the virtual machine storage is counted.

Host Consumption Distribution chart includes incorrect unknown assignment for ESX servers in the host scope (2139029)

You can change the scope of the Storage Consumption Summary report to display data for specific VMware ESX servers. If you change to the host scope and select an ESX server, the Unknown Assignment value in the Host Consumption Distribution chart is incorrect. The value is incorrect, because the LUNs that are given to a storage pool are not treated as assigned. The Unknown Assignment value is correct when the scope of the report is for the enterprise (the default value).

To find the correct unknown assignment capacity for ESX servers, go to the Host Virtualization Detail report and view the Virtualization Server Storage Usage table.

Capacities for NAS Used (NFS SP) and NAS Allocated are 0 (1974701)

In the Total Unified Storage chart, the capacities for the NAS Used (NFS SP) slice and the NAS Allocated slice are always 0. The capacities are always 0 because CommandCentral Storage does not support the correlation of NFS-based storage pools to unified storage devices. The Total Unified Storage chart appears in the Online Storage Capacity Summary report.

Configuration repository LUNs from FalconStor storage arrays not counted as administrative storage (2136116)

In CommandCentral Storage reports, configuration repository LUNs from FalconStor Network Storage Servers (NSS) are not counted as administrative storage. Rather, these types of LUNs are included in the:

■ Logical: Unknown capacity in the Online Storage Capacity report, in the Total Online Storage chart and the Total Array Storage chart.

■ Unallocated capacity in the Unallocated LUNs Storage report and in the Online Storage Capacity Detail report's LUNs table.

Allocated File Storage capacity not populated for VMware ESX servers that consume NFS-based storage (2142902)

In the Storage Consumption Detail report, the Allocated File Storage capacity is not populated for VMware ESX servers that consume NFS-based storage. This issue occurs when NAS storage from an EMC Celerra or NetApp unified storage system is given to an ESX server and a storage pool is created from the NAS storage.

Allocated LUN Reclamation report may take several minutes to load (1991351)

The Allocated LUN Reclamation report may take several minutes to load if there are thousands of LUNs in the enterprise. As a workaround, you can do the following:

■ Scope the report on an array or host.

■ If you want to see data for the enterprise scope, you can create a custom report and schedule it for archiving or emailing.

Device handle capacity for virtualization server is double counted in Allocated LUNs Reclamation report (2143688)

In the Allocated LUNs Reclamation report, the block storage that is given to virtual machines is double counted. This issue happens in following situations:

■ For VMware, when a virtual machine disk (vmdk) is assigned to virtual machine from a SAN-based or DAS-based data store.

■ For Solaris zones, when a device handle is exported from a global zone to a non-global zone.

The issue affects the following categories in the report:

■ Assigned

■ Potentially unassigned

Note: This issue does not occur if you scope the report to the virtualization server only or the virtual machines only.

% Volume Manager Capacity Unused is greater than 100% (2104549)

In the Host Storage Assessment Report, in the Host Storage Reclamation table, a host's % Volume Manager Capacity Unused may be greater than 100%. The capacity is greater than 100% if a ZFS volume is created on a ZFS storage pool that CommandCentral Storage discovers.

In SAN scope, the Host Storage Assessment report includes DAS-based data for disk groups (2129330)

By default, the Host Storage Assessment report includes data for SAN-based storage only. To include DAS-based storage, you need to check the **Include DAS** checkbox. However, the report might include DAS-based storage even if you do

not check the **Include DAS** checkbox. The report includes DAS-based storage in the storage capacity of a disk group if the disk group consumes LUNs from both SAN-based and DAS-based storage.

User management issues

The following issues relate to user management.

Domains not available for user accounts and user groups (1792352)

If you install the Management Server on a host that includes Veritas Cluster Server One, you may experience problems with domains. For example, if you add a new user account or user group, domains may not appear when you try to select a domain from the drop-down list.

Workaround

Use the command `addbrokerdomain` to map a domain to the Authentication Broker.

To use the command addbrokerdomain to map a domain to a broker

1   Log on to the Authentication Broker host and open an operating system console. For example, if you run the Management Server in RB+AB mode (the default mode when you install), log on to the Management Server.

2   Change to the Authentication Service CLI (vssat) directory. By default, the directory is:

Solaris	`/opt/VRTSat/bin`
Windows	`\Program Files\VERITAS\Security\Authentication\bin`

3   Type the following command:

`vssat addbrokerdomain -b host:port -d domain_type:domain_name`

Where:

host	is the host name of the Authentication Broker host. For example, if you run the Management Server in RB+AB mode (the default mode when you install), enter the host name of the Management Server.
port	is the port for authentication. By default, the port is 2821.

domain_type	is one of the following:

- GSS
- ldap
- nis
- nisplus
- nt
- pam
- unixpwd
- vx

domain_name	is the name of the domain.

After you run the command, you can select the domain in CommandCentral.

Monitoring issues

The following issues relate to monitoring your storage network.

Monitoring data not displayed for SnapMirror destination (621024)

The CommandCentral Storage Console may fail to display monitoring data for a NetApp volume that is a destination for SnapMirror operations.

This happens because NetApp SnapMirror monitoring requires that the CommandCentral Storage Standard Agent be capable of resolving the host name of the destination Storage System.

Workaround

To enable monitoring for the SnapMirror destination volume, perform the following operation on the Standard Agent that is discovering the destination Storage System:

UNIX: Edit the file `/etc/resolv.conf` and add the domain name of the destination Storage System to the `search` line.

Example: `search mynetappdomain.example.com`

Windows: From the Control Panel, go to Network Connections. In the Advanced IP properties window, add the domain name of the destination Storage System to the DNS suffixes list.

Monitoring status not available for ESX server (1122802)

In the CommandCentral Storage Console, the host status details of an ESX server does not display in the monitoring views.

There is no workaround.

Alerts about CommandCentral Storage processes may display after reboot or upgrade (1183630)

When you shutdown your Management Server or Standard Agent—for example, to reboot or upgrade—the following may occur:

■ If CommandCentral Storage processes stop before the Simple Instrumentation Collection Layer (SICL) stops, an alert displays in the Console for each CommandCentral Storage process that is not running.
For example, the following alert may display: `CommandCentral process not running: vxtrapd`
After SICL shuts down, the alert may display with a status of Unknown.

■ When SICL shuts down, an alert displays in the Console to inform you that SICL is disconnected.
For example, the following alert may display: `SICL (CC Storage monitoring service) on host myhost.example.com is Disconnected.`

If you receive these alerts during a planned shutdown of your Management Server or Standard Agent, you can reset the alerts to remove them from the Console.

For more information about resetting alerts, see the *CommandCentral Administrator's Guide*.

Multiple alerts display for offline Veritas Cluster Server service group (1212311)

If you install the CommandCentral Standard Agent on more than one node within a Veritas Cluster Server cluster that hosts a service group and that service group's state changes to OFFLINE, multiple alerts for the offline service group will display in the CommandCentral Storage Console.

If you receive multiple alerts about an offline Veritas Cluster Server service group, you can reset the multiple alerts to remove them from the Console.

For more information about resetting alerts, see the *CommandCentral Administrator's Guide*.

Alerts display for devices for which monitoring is disabled (1300864)

If you disable monitoring for a device (for example, a storage array) that a Control Host discovers, and a policy exists for a child object of that device (for example, a LUN), alerts will generate for that device, even though you disabled monitoring.

Workaround

On the Control Host, restart the Simple Instrumentation Collection Layer (SICL).

To restart SICL

1   On the Control Host, open an operating system console and log on as root (Solaris) or as a user with administrator-level privileges (Windows).

2   Change to the directory where the script vxccs resides. By default, this is:

Solaris: `/opt/VRTSccs/VRTSccsta/bin`

Windows: `/Program Files/Veritas/CommandCentral Storage/Support/Tools/Vxccs`

3   Type the following command to stop SICL:

Solaris: `vxccs stop vxsicld`

Windows: `vxccs stop VRTSsicls`

4   Type the following command to start SICL:

Solaris: `vxccs start vxsicld`

Windows: `vxccs start VRTSsicls`

5   Do the following to verify that SICL is running:

Solaris: Type the following command: `vxccs status vxsicld`

Windows: Use the Windows Service Control Manager to verify that the process Veritas CommandCentral Storage SICL is STARTED.

The Control Host now has an updating status of monitoring for the devices that it discovers.

Numeric collector "Hitachi DKCCSW Moderate Count" does not display a value (1439498)

When you view monitoring information for a Hitachi storage array, in the Numeric Collectors table, the collector "Hitachi DKCCSW Moderate Count" may not display a value. This collector determines the number of Hitachi disk controllers that are experiencing moderate internal bus errors.

There is no workaround.

Incorrect or no values display for state collectors "Device Status" and "HitachiDfArrayStatus" (1439527)

When you view monitoring information for a Hitachi storage array, in the State Collectors table, the collectors "Device Status" and "HitachiDfArrayStatus" may display incorrect values or they may not display a value.

There is no workaround.

IBM SAN Volume Controller (SVC) SICL Status value unavailable (1743398)

When you select an IBM SVC object on the **Managing Summary** > **Arrays** pane, and then select the **Monitoring** tab, no value appears for the object's **SICL Status** in the **State Collectors** table.

Monitoring favorites not available after an upgrade (1781686)

Monitoring favorites that are set before upgrading CommandCentral Storage are unavailable following the upgrade. The upgrade process intentionally discards the monitoring links' session ID as part of the upgrade, which causes the favorites to also be discarded. The upgrade does not cause this issue, and the upgrade is unaffected.

Workaround

Reset the monitoring favorites following an upgrade.

Monitoring data for Cisco ports does not appear after upgrade to 5.2 (1834204)

After you upgrade to CommandCentral 5.2, monitoring data for Cisco ports may not appear in the Console.

Workaround

After you upgrade to 5.2, wait a few hours for the data to appear. If the data does not appear after a few hours, restart the Alarm Service.

To restart the Alarm Service (Solaris)

1 Log on to the Management Server and open an operating system console.

2 Change to the following directory:

   `/opt/VRTSccs/VRTSccsts/bin`

3 Type the following commands:

   `./vxccs stop vxasd`

   `./vxccs start vxasd`

To restart the Alarm Service (Windows)

1 Log on to the Management Server and open Windows' Services utility.

2 Restart the following process:

   Veritas CommandCentral Storage Alarm Service

Alarm Service configuration reverts to default values after upgrading Solaris Management Server to 5.2 (1714407)

When you upgrade a Solaris Management Server to CommandCentral 5.2, configuration parameters for the Alarm Service (VxAS) are reset to default values. In other words, if you had modified any configuration parameters for the Alarm Service in a previous release, those changes are not retained. The only configuration parameters that are retained are those related to internal SNMP polls and alarms. If you did not modify configuration parameters for the Alarm Service, this issue does not affect your Management Server.

For example, some of the common configuration parameters that you might have changed are as follows.

Table 6-2   Commonly changed configuration parameters for the Alarm Service

Parameter	Default value
QueueSizeHighWaterMark	10000
QueueSizeLowWaterMark	2500
ServerConnPort	32604
MaxLogEntryAge	120
MaxLogFileSize	5024
MaxQueueDepth	1000

Table 6-2   Commonly changed configuration parameters for the Alarm Service
                 (continued)

Parameter	Default value
DefaultPort	161
DefaultSnmpCommunity	public
SnmpInterval	10
SnmpRetry	3
VxAMServerPort	5431
RegisterAttributesAsIds	yes

Workaround

To change the configuration parameters back to their previous values, contact Symantec Technical Support.

SICL-based monitoring does not work on the Management Server after upgrade to version 5.2 (2147895)

Monitoring through the Simple Instrumentation Collection Layer (SICL) may not work on the Management Server after you upgrade to version 5.2. This issue happens if you upgrade from a 5.1.2 Management Server that was configured to discover Brocade or McDATA switches through the BrocadeMcDataExplorer.

SICL-based monitoring includes:

■ Self-monitoring of the Management Server, which monitors the Management Server's processes for availability and performance

■ Monitoring of the arrays that the Management Server discovers

■ Monitoring of certain host objects, such as databases

Workaround

This issue is fixed in a patch. To download the patch, go to the Symantec Operations Readiness Tools Web site.

https://sort.symantec.com/patch/detail/4236

Documentation addenda and errata

This chapter includes the following topics:

■ Incorrect storage terms listed in the "Virtualization server consumption" topic

Incorrect storage terms listed in the "Virtualization server consumption" topic

The CommandCentral Storage online Help includes definitions of the storage terms that are used in the Host Virtualization Storage Summary chart. The following errors are present for these terms:

■ The definition of the Overhead term is incorrectly listed in the "Virtualization server consumption" topic. The definition should appear in the "Virtualization server usage" topic.

■ The "Virtualization server consumption" topic lists the Unassigned term. The name of this term is incorrect. The correct name is Unknown.

These errors are not present in the *CommandCentral Storage User's Guide*. You can access the guide from the following location:

http://www.symantec.com/enterprise/support/documentation.jsp?pid=50379

Getting help

This chapter includes the following topics:

- About CommandCentral Storage documentation

- Displaying online help

- Contacting Symantec

About CommandCentral Storage documentation

You can access CommandCentral Storage documentation at the Symantec Technical Support Web site:

http://www.symantec.com/enterprise/support/documentation.jsp?pid=50379

Table 8-1 describes the CommandCentral Storage documentation.

Table 8-1 CommandCentral Storage documentation

Guide	Description
CommandCentral Administrator's Guide	Provides information about how to administer the product. For example, the guide describes how to manage licenses and user accounts, configure product components, and work with diagnostic information.
CommandCentral Getting Started Guide	Provides a high-level overview of how you can use CommandCentral Storage.
CommandCentral Hardware and Software Configuration Guide	Provides setup requirements for applications and devices and instructs you how to configure CommandCentral Storage to discover them.
CommandCentral Hardware and Software Compatibility List	Lists the devices and applications that CommandCentral Storage supports.

Table 8-1   CommandCentral Storage documentation *(continued)*

Guide	Description
CommandCentral Installation Guide	Instructs you how to install CommandCentral Storage.
CommandCentral Storage Release Notes	Provides information about supported operating systems, host resource requirements, software limitations, and known issues.
CommandCentral Storage User's Guide	Describes how you can use CommandCentral Storage to monitor, manage, and report on your storage infrastructure.
CommandCentral Third-Party License Agreements	Provides information about third-party software that is used in CommandCentral Storage and CommandCentral Storage Change Manager.

Commenting on product documentation

Submit comments about the product documentation to the following email address:

storage_management_docs@symantec.com

Please include the following information with your documentation comments:

■ The title and product version of the guide you are commenting on

■ The topic (if relevant) you are commenting on

■ Your comment

■ Your name

Displaying online help

CommandCentral includes online help as well as UNIX manual pages.

To display online help

1   Do one of the following:

■ In the Console, click the appropriate **Help** link or menu item.

■ In any dialog window, click the **Help** button.

2 On UNIX systems, you can use manual pages to find reference and usage information about product-specific commands. When you install the product, the `pkgadd` command installs the nroff-tagged manual pages in the appropriate directories under `/opt/VRTS/man`. However, the install does not update the windex database.

To ensure that new manual pages display correctly

1 Update your:

■ `MANPATH` environment variable to point to `/opt/VRTS/man`

■ `windex` database

2 Refer to the `catman(1M)` manual page for more information about updating windex.

Contacting Symantec

You can contact Symantec on the Web, by email, or by telephone.

Using the support web site

For technical assistance with any Symantec product, visit the Symantec Support Web site:

http://www.symantec.com/enterprise/support/assistance_care.jsp

From there you can:

■ Contact the Symantec Support staff and post questions to them

■ Get the latest software patches, upgrades, and utilities

■ View updated hardware and software compatibility lists

■ View Frequently Asked Questions (FAQ) pages for the products you are using

■ Search the knowledge base for answers to technical support questions

■ Receive automatic notice of product updates

■ Find out about training in the Storage Foundation products

■ Read current white papers related to the Storage Foundation products

Subscribing to email notification service

Subscribe to the Symantec Email notification service to be informed of software alerts, newly published documentation, Beta programs, and other services.

Go to the following Web site:

http://www.symantec.com/enterprise/support/assistance_care.jsp

Select a product and click E-mail Support at the bottom of the page. Your customer profile ensures that you receive the latest Symantec technical information pertaining to your specific interests.

Accessing telephone support

Telephone support is available with a valid support contract. To contact Symantec for technical support, dial the appropriate phone number listed on the Support Guide included in the product box and have your product license information ready for quick navigation to the proper support group.

Obtaining support by email

Licensed customers can use the following email address to obtain help with technical questions:

support@veritas.com

To obtain software updates by email, send your requests to the following email address:

swupdate@veritas.com

Obtaining license information

To obtain license information, contact Symantec in one of the following ways:

- U.S. and Canada telephone: 1-800-634-4747 option 3
- Worldwide fax: +1-650-527-0952
- Email:
  amercustomercare@veritas.com

Purchasing products

For help with purchasing Symantec products, visit the Symantec Web site:

http://www.symantec.com

where you can chat with product experts or link to information about the products.

You can also contact a Symantec product representative by email at the following address:

sales.mail@veritas.com

To speak with a Symantec product representative by telephone, customers in the U.S. and Canada can call 1-800-327-2232.