Veritas CommandCentral™ Release Notes

for Microsoft Windows and UNIX

5.2 RU1

Symantec

CommandCentral Release Notes

Documentation version 5.2 RU1.0

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

CommandCentral 5.2 RU1 Release Notes

This document includes the following topics:

Upgrading to CommandCentral 5.2 RU1

CommandCentral 5.2 RU1 is an update to the CommandCentral 5.2 release. You can upgrade the following CommandCentral components to 5.2 RU1:

Management Server	See "Upgrading the Management Server" on page 7.
Control Host	See "Upgrading the Control Host" on page 9.

You can upgrade to CommandCentral 5.2 RU1 from version 5.2 only.

Upgrade your Management Server before you upgrade any Control Hosts.

Upgrading the Management Server

You can upgrade a 5.2 Management Server to 5.2 RU1.

To upgrade the Management Server (Solaris)

1. Log on to the Management Server as root or as a user with an ID equal to zero (UID=0).
2. If you have not already done so, download the installation file from the Symantec FileConnect Web site:

   https://fileconnect.symantec.com

   The file is named `VRTS_CommandCentral_5.2RU1_Solaris_MS.tar.gz`.
3. Type the following commands to uncompress the tar file:

   ```
   gunzip VRTS_CommandCentral_5.2RU1_Solaris_MS.tar.gz
   ```

   ```
   tar -xf VRTS_CommandCentral_5.2RU1_Solaris_MS.tar
   ```
4. Go to the following directory:

   installer_location`/MS/sol_sparc`

   Where *installer_location* is the directory in which you uncompressed the tar file.
5. Type the following command to start the upgrade:

   ```
   ./installrp host_name
   ```

   Where *host_name* is the fully qualified name of the host.
6. Follow the prompts to upgrade the Management Server.

To upgrade the Management Server (Windows)

1. Log on to the Management Server as a user with administrator-level privileges.
2. If you have not already done so, download the installation file from the Symantec FileConnect Web site:

   https://fileconnect.symantec.com

   The file is named `VRTS_CommandCentral_5.2RU1_Windows_MS.zip`.
3. Extract `VRTS_CommandCentral_5.2RU1_Windows_MS.zip`.
4. Go to the following directory:

   installer_location`\MS\win\patches`

   Where *installer_location* is the directory in which you extracted the zip file.
5. Run `MSSetup.exe`.
6. Follow the instructions in the wizard to upgrade the Management Server.

Upgrading the Control Host

You can upgrade a 5.2 Control Host to 5.2 RU1.

To upgrade the Control Host (Solaris)

1. Log on to the Control Host as root or as a user with an ID equal to zero (UID=0).
2. If you have not already done so, download the installation file from the Symantec FileConnect Web site:

   https://fileconnect.symantec.com

   The file is named `VRTS_CommandCentral_5.2RU1_Solaris_CH.tar.gz`.
3. Type the following commands to uncompress the tar file:

   ```
   gunzip VRTS_CommandCentral_5.2RU1_Solaris_CH.tar.gz
   ```

   ```
   tar -xf VRTS_CommandCentral_5.2RU1_Solaris_CH.tar
   ```
4. Go to the following directory:

   installer_location`/CH/sol_sparc`

   Where *installer_location* is the directory in which you uncompressed the tar file.
5. Type the following command to start the upgrade:

   ```
   ./installrp host_name
   ```

   Where *host_name* is the fully qualified name of the host.
6. Follow the prompts to upgrade the Control Host.

To upgrade the Control Host (Windows)

1. Log on to the Control Host as a user with administrator-level privileges.
2. If you have not already done so, download the installation file from the Symantec FileConnect Web site:

   https://fileconnect.symantec.com

   The file is named `VRTS_CommandCentral_5.2RU1_Windows_CH.zip`.
3. Extract `VRTS_CommandCentral_5.2RU1_Windows_CH.zip`.
4. Go to the following directory:

   installer_location`\CH\win\patches`

   Where *installer_location* is the directory in which you extracted the zip file.
5. Run `CHSetup.exe`.
6. Follow the instructions in the wizard to upgrade the Control Host.

What's new in CommandCentral 5.2 RU1

CommandCentral 5.2 RU1 includes the following new features and enhancements.

Table 1-1 New features and enhancements

Feature	Description

New default port to connect to the Console	In CommandCentral 5.2 RU1, the default port that you use to connect to the CommandCentral Console has changed. When you upgrade to 5.2 RU1, the installer scans the range of ports between 14191 and 14200 and finds the first available port, which then becomes the new port for the Console.
	
	For example, to connect to CommandCentral Storage, you need to enter the following URL in your Web browser:
	`https://myhost.example.com:14191/cc`
	
	To connect to CommandCentral Storage Change Manager, you need to enter the following URL in your Web browser:
	`https://myhost.example.com:14191/sm`
	
	If you need to, you can change the default port. For example, you can change the default port back to 8443.
	
	See "Changing the port for the CommandCentral Console" on page 13.
	
	You need to connect to the Console through a new port because CommandCentral now uses an embedded Web server. Previous versions of CommandCentral used a Web server that other Symantec products shared. In 5.2 RU1, CommandCentral is the only Symantec product that uses the Web server.
	
	Note: To start and stop the Web server in 5.2 RU1, you can use the `vxccs` utility. For Solaris, the process is called `esmweb`. For Windows, the process is called `CCSGUI`. In addition, you can use Windows' Services utility to start and stop the Web server. In the Services utility, the name of the service is Veritas CommandCentral Web Console.

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

Feature	Description
Discovery of IBM logical partitions	CommandCentral can now discover information about IBM logical partitions (LPARs). For information on supported versions of IBM LPARs, see the *CommandCentral Hardware and Software Compatibility List*. This document is updated regularly at: http:/www.symantec.com/docs/TECH148619 See " IBM logical partition (LPAR) configuration requirements" on page 14. See "Viewing information about your IBM logical partition (LPAR) environment" on page 21.
Agentless discovery of Solaris Volume Manager	CommandCentral can now discover information about Solaris Volume Manager when it performs agentless discovery of hosts that run Solaris 9 or 10 (SPARC only). CommandCentral requires root access to discover information about Solaris Volume Manager disks and disk slices. See "Commands that require root access for agentless discovery of UNIX hosts" on page 24.

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

Feature	Description
Agentless discovery of HP-UX hosts	CommandCentral can now perform agentless discovery of remote hosts that run the HP-UX operating system. We support HP-UX 11.23 (IA-64) and HP-UX 11.31 (IA-64 and PA-RISC). See "What CommandCentral can discover with agentless discovery of hosts" on page 23. The requirements to discover HP-UX hosts are the same as they are for other UNIX hosts. CommandCentral requires: ■ A user account CommandCentral can discover most information with a non-root user account. However, privileged access is required to discover some information. See "Commands that require root access for agentless discovery of UNIX hosts" on page 24. ■ Network access between hosts ■ A shell on the remote host (sh, ksh, or bash) ■ Secure Shell (SSH) on the remote host If SSH is not installed on the host, you can install OpenSSH. See "Installing OpenSSH on HP-UX" on page 26. For more information about requirements to perform agentless discovery, see the *CommandCentral Administrator's Guide*. Agentless discovery of HP-UX hosts works the same as it does for other UNIX hosts. You can let CommandCentral remotely access the HP-UX host and run the script or you can manually run the script on the host. To manually run the HP-UX script (`RHHPUXScript.sh`), run the following command: **`/bin/sh ./RHHPUXScript.sh -d directory -t temp_directory`** For more 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 Hitachi Virtual Storage Platforms	CommandCentral can now discover information about Hitachi Virtual Storage Platform (VSP) storage arrays. For device support information, see the *CommandCentral Hardware and Software Compatibility List*. For example, you can identify supported features and the supported ancillary software. This document is updated regularly at: http://www.symantec.com/docs/TECH148619 For information about how to configure discovery of Hitachi VSP, see the *CommandCentral Hardware and Software Configuration Guide*. You configure discovery of Hitachi VSP like other Hitachi arrays that use the HiCommand management framework.
Support for Brocade Data Center Fabric Manager (DCFM) 10.4.x	CommandCentral 5.2 RU1 supports Brocade Data Center Fabric Manager (DCFM) 10.4.x, which includes an integrated SMI-S agent. CommandCentral can discover all fabrics and switches that the DCFM manages. See "Configuring CommandCentral to discover Brocade and McDATA switches through DCFM 10.4.x" on page 26.
NetApp deduplication view	CommandCentral 5.2 RU1 includes a new view that you can use when you create ad hoc reports. The view provides information about the deduplication of NetApp flex volumes with Single Instance Storage (SIS). See "View V_NETAPP_DEDUPLICATION_BASE" on page 29. For information about how to create ad hoc reports, see the *CommandCentral Storage User's Guide*. For information about database views, see the *CommandCentral Administrator's Guide*.

Changing the port for the CommandCentral Console

You can change the port that you use to connect to the CommandCentral Console. You can use any port that is not in use by another application.

For example, you might want to change the default port from 14191 to 8443. 8443 was the default port before the 5.2 RU1 release. You can still use port 8443 as long as no other products use the port. For example, 8443 is the default port for the Symantec Web server (VRTSweb). Other Symantec products might use that port.

To change the port for the CommandCentral Console

1. Log on to the Management Server.
2. Go to the following directory:

Solaris	/opt/VRTSccs/VRTSccstw/esmweb/conf
Windows	\Program Files\VERITAS\CommandCentral Storage\Web Engine\esmweb\conf

3. Open `esmweb.cfg` in a text editor.
4. Change the value of the `SSLPORT` parameter to the desired port number.
5. Save and close `esmweb.cfg`.
6. In an operating system console, change to the following directory:

Solaris	/opt/VRTSccs/VRTS/bin/vxccs
Windows	\Program Files\VERITAS\CommandCentral Storage\Support\Tools\Vxccs

7. Type the following commands to restart the Web server:

Solaris	**`./vxccs stop esmweb`** **`./vxccs start esmweb`**
Windows	**`vxccs.bat stop CCSGUI`** **`vxccs.bat start CCSGUI`**

You can now connect to the Console through the new port.

IBM logical partition (LPAR) configuration requirements

For CommandCentral to properly discover IBM LPARs, ensure that your storage network's physical connections, device settings, and CommandCentral settings are properly configured.

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

http://www.symantec.com/docs/TECH148619

Configuring CommandCentral to discover your IBM logical partition (LPAR) environment involves several steps.

Table 1-2 Configuring CommandCentral to discover your LPAR environment

Step	Action	Description
Step 1	Review how LPAR discovery works	Identify how you need to configure discovery of your LPAR environment. See "How CommandCentral can discover your IBM logical partition (LPAR) environment" on page 15.
Step 2	Review set up requirements	Identify how you need to set up your LPAR environment to ensure proper discovery. See "Setup requirements for IBM logical partitions" on page 18.
Step 3	Configure discovery of the Hardware Management Console (HMC)	Configure CommandCentral to discover the HMC using the Configure a New Device tool. See "Configuring CommandCentral to discover the Hardware Management Console (HMC)" on page 19.
Step 4	Configure discovery of each LPAR	Configure CommandCentral to discover each LPAR by doing one of the following: ■ Configure agentless discovery of the LPAR. For information about how to configure agentless discovery, see the *CommandCentral Administrator's Guide*. ■ Install the Standard Agent in the LPAR. For information about installing a Standard Agent, see the *CommandCentral Installation Guide*.

How CommandCentral can discover your IBM logical partition (LPAR) environment

Note: CommandCentral Storage does not support configuring VIO servers as agentless hosts. It also does not support installing a Standard Agent on the VIO server. If you have already installed a Standard Agent on a VIO server, disable the agent so that it doesn't report to the Management Server before you upgrade the Management Server to version 5.2 RU1. Installing a Standard Agent on a VIO server or configuring it for agentless discovery can lead to unpredictable behavior.

You can configure CommandCentral to discover your LPAR environment in one of two ways.

Table 1-3 Configuration options to discover your LPAR environment

Option	Configuration	Provides
1	■ Configure CommandCentral to discover the Hardware Management Console (HMC). ■ In each LPAR, install the Standard Agent with the 5.2 Release Update (RU1) Hotfix for AIX Managed Host, which adds LPAR discovery support.	■ End-to-end visualization of your LPAR environment ■ Information to perform capacity management of your LPAR environment ■ Application to spindle mapping for LPARs
2	■ Configure CommandCentral to discover the Hardware Management Console (HMC). ■ Configure agentless discovery of each LPAR.	■ End-to-end visualization of your LPAR environment ■ Information to perform capacity management of your LPAR environment ■ File system to spindle mapping for LPARs

The following table provides further information about the discovery of the HMC, LPARs, and VIO servers.

Table 1-4 Discovery information from the HMC, LPAR, and VIO server

Object	Discovery information

Hardware Management Console (HMC)	To communicate with the HMC using HMC CLIs, CommandCentral uses ssh and a user account that is assigned the hmcoperator role or hmcsuperadmin role. The CommandCentral Management Server and Control Host can communicate with the HMC, as they both run the LPAR explorer.
	
	Through this communication, CommandCentral can discover the following:
	
	■ The managed systems that the HMC manages
	■ LPARs and their associations to managed systems and VIO servers
	■ VIO servers, which includes the following information:
	  ■ Their association to LPARs
	  ■ Their associations to managed systems
	  ■ HBAs
	  ■ OS handles
	  ■ Storage that is exported from VIO servers to LPARs (no information about the OS handles inside the LPARs)
	  CommandCentral Storage supports native device handles only, as backing devices for the virtual target devices exported from the VIO server to an LPAR. CommandCentral Storage does not support logical volumes, Veritas DMP devices, file devices, or any device type except the native device, as the virtual target device's backing device.
	  The LPAR-VIO Server association is discovered only when at least one virtual target device (exported from the VIO server to the LPAR) is backed by native device handle. If there are no virtual target devices exported to the LPARs that are backed by native device handles, the LPAR-VIO Server association is absent.
	
	Note: CommandCentral Storage does not support discovery of LPARs through the Integrated Virtualization Manager (IVM).

Table 1-4 Discovery information from the HMC, LPAR, and VIO server *(continued)*

Object	Discovery information
LPAR	You need to either install the CommandCentral 5.2 Standard Agent with the 5.2 Release Update (RU1) Hotfix for AIX Managed Host, which adds LPAR discovery support in the LPAR or configure the LPAR for agentless discovery. This step is required to discover information about the storage resources in the LPAR. For discovering LPARs agentlessly, the same requirements as for a normal AIX host apply here. Discovery provides the following: ■ Basic host information ■ HBAs (only when they are directly assigned to LPARs as slots on the managed system) ■ OS handles, including VSCSI OS handles (provides correlation to the storage that is exported from VIO servers when you configure discovery through the HMC, and if the backing device in the VIO server is a native device handle) ■ Logical volume manager (LVM) volumes ■ File systems ■ Applications and databases (not available if you use agentless discovery) If you configured LPAR hosts for agentless discovery prior to upgrading to CommandCentral Storage 5.2 RU1, refresh the hosts so that you can see the correlated data immediately.

Setup requirements for IBM logical partitions

CommandCentral uses Secure Shell (ssh) to discover logical partitions (LPARs) through the Hardware Management Console (HMC).

See "How CommandCentral can discover your IBM logical partition (LPAR) environment" on page 15.

Make sure that the HMC allows ssh access from the Management Server or Control Host for an account that has the hmcoperator role or hmcsuperadmin role. Also, ensure that the account has visibility into the LPARs and VIO servers for which you need discovery.

Meet the requirements for device handle discovery inside LPARs. For details, see *CommandCentral Hardware and Software Configuration Guide*.

Configuring CommandCentral to discover the Hardware Management Console (HMC)

Configuring CommandCentral to discover the Hardware Management Console (HMC) is required to discover your IBM logical partition (LPAR) environment.

See " IBM logical partition (LPAR) configuration requirements" on page 14.

Before you configure CommandCentral to discover the HMC, review the setup requirements.

See "Setup requirements for IBM logical partitions" on page 18.

To configure CommandCentral to discover the HMC

1. Click **Tools > Configure a New Device**.
2. In the **Configure Device - Select Device Type** panel, select the device category **Virtualization Server** and the device type **Logical partition (LPAR)**. Then, click **Next**.
3. In the **Configure Device - Select Explorer** panel, select the host from which you want to perform discovery. Then, click **Next**.

   This panel displays only if you have more than one host that runs the LPAR explorer.
4. In the **Configure Device - Device Credentials** panel, enter the required information. Then, click **Next**.

   See "Device Credentials panel options for IBM logical partitions" on page 19.
5. In the Configure Device - Status panel, click **Finish**.

Device Credentials panel options for IBM logical partitions

Use this panel to configure CommandCentral to discover information about your IBM logical partition (LPAR) environment through the Hardware Management Console (HMC).

Table 1-5 Configure Device - Device Credentials panel options for LPARs

Field	Description
HMC IP Address or Host name	Enter the IP address or host name of the Hardware Management Console (HMC).
Login	Enter the logon for a user account that is assigned the hmcoperator role or hmcsuperadmin role.
Password	Enter the password for the user.

Table 1-5 Configure Device - Device Credentials panel options for LPARs *(continued)*

Field	Description
Enable Discovery	Check this field to enable discovery of the HMC. This field is checked by default.
Configuration Name	Enter a user-friendly name to identify the HMC. This field defaults to the value that you enter in the **HMC IP Address or Hostname** field.
SSH Timeout (seconds)	Enter the number of seconds in which the ssh commands that are issued from the explorer to the HMC should timeout. The default is 1200 seconds. Click **Advanced Settings** to display this field.
Verify Device Configuration	Check this field to verify that CommandCentral can contact the HMC with the information that you entered in this panel. This field is checked by default.

Tuning the LPAR explorer

You can tune the explorer that discovers logical partitions (LPARs).

To tune the LPAR explorer

1. In the CommandCentral Console, click **Settings > Host Management**.
2. In the **Hosts** table, click the host on which you want to configure the explorer.
3. In the **Explorers** table, check **LPARExplorer**.
4. In the drop-down list, click **Configure Explorer**. Then, click **Go**.
5. In the **Configure Explorers - Explorer Settings** dialog box, modify the explorer's settings. Then, click **Next**.

   See "Explorer Settings dialog options for the LPAR explorer" on page 20.
6. Click **Finish**.

   The explorer updates.

Explorer Settings dialog options for the LPAR explorer

Use the Configure Explorers dialog box to tune the explorer.

Table 1-6 LPAR explorer options

Field	Description
Polling Interval in Minutes	Enter the amount of time that you want the explorer to wait before it repeats discovery. The default is 360 minutes.
Debug Level	Enter the level of verbosity for which the explorer logs messages. The verbosity range is 1-6 where 1 is the least and 6 is the most verbose. Enter 0 to turn the logging off. Click **Advanced Settings** to display this field.

Viewing information about your IBM logical partition (LPAR) environment

After CommandCentral discovers your LPAR environment, you can view information in the Managing and Reporting sections of the Console. This information provides an end-to-end visualization of your LPAR environment and the ability to perform capacity management.

You can view information about the following objects:

Managed systems	See "Viewing managed systems" on page 21.
LPARs	See "Viewing IBM logical partitions" on page 22.
VIO servers	See "Viewing IBM VIO servers" on page 23.

Viewing managed systems

When CommandCentral discovers the Hardware Management Console (HMC), it discovers information about the managed systems (or physical frames) that the HMC manages. CommandCentral identifies the managed system as a virtualization server.

You can view information about managed systems in the Managing view. After you select a managed system, you can view information in the following panes:

Overview	Information about the VIO servers and LPARs that the managed system manages.
Reporting	Links to reports that are scoped to the managed system.
Monitoring	If available for the object, this pane includes associated alerts, collectors, and policies.

Attributes	The managed system's attributes.

To view managed systems

1. Click **Managing > Hosts and HBAs > Virtualization Servers**.
2. In the **Virtualization Servers Summary** table, click the name of a virtualization server whose virtualization technology is identified as **AIX LPAR**.

   The **Overview** pane for the managed system appears.

Viewing IBM logical partitions

You can view information about IBM logical partitions (LPARs) in the Managing view. You can use this information to identify how storage is used in the LPAR. After you select an LPAR, you can view information in the following panes:

Overview	Information about the LPAR, such as the associated virtualization server, the Virtual I/O (VIO) Servers that export storage to the LPAR, and consumed device handles.
Reporting	Reports are not available for LPARs.
Attributes	The LPARs attributes.

To view IBM logical partitions

1. Click **Managing > Hosts and HBAs > Virtual Machines**.
2. In the **Virtual Machines** table, click the name of a virtual machine whose virtualization technology is identified as **AIX LPAR**.

   The **Overview** pane for the LPAR appears.

If the LPAR is configured to be discovered agentlessly, or by the Standard Agent, you can view more information about the LPAR by going to the **Hosts** page.

To view the Hosts page for IBM Logical Partitions

1. Click **Managing > Hosts and HBAs > Hosts**.
2. In the **Hosts** table, click the name of a host whose virtualization technology is identified as **AIX LPAR**.

   The **Overview** pane for the LPAR host appears.

Viewing IBM VIO servers

When CommandCentral discovers your IBM logical partition (LPAR) environment, it can discover information about Virtual I/O Servers (VIO servers). You can view information about VIO servers in the Managing view. A new table in the Host Virtualization Detail report, **VIO Server Storage Usage**, shows all of the VIO servers in your environment. After you select a VIO server, you can view information in the following panes:

Overview	Information such as associated LPARs, HBA port groups, and array virtual ports.
Connectivity	The VIO server's HBAs, HBA ports, and host connections.
Zoning	Any active zone memberships, defined zone memberships, and zone alias memberships.
Storage	Masked LUNs, claimed LUNs and device handles.
Exported Storage	The device handles that are exported from the VIO server to LPARs.
Volumes	Information about physical disk groups, volumes, disks, and LUNs.
Projections	Projected storage consumption for the VIO server.
Reporting	Links to reports that are scoped to the VIO server.
Monitoring	Monitoring is not available for this object.
Attributes	The VIO server's attributes.

To view VIO servers

1. Click **Managing > Hosts and HBAs > Virtualization Servers**.
2. In the **Virtualization Servers Summary** table, click the name of a virtualization server whose virtualization technology is identified as **AIX LPAR**.
3. In the **VIO Servers** table, click the name of a VIO server.

   The **Overview** pane for the VIO server appears.

What CommandCentral can discover with agentless discovery of hosts

Table 1-7 details what CommandCentral can discover from an agentless host by operating system.

Table 1-7 Host level discovery for agentless hosts

Host information	AIX	HP-UX	Linux	Solaris	VMware GOS [1]	Windows
Allocated LUNs	X	X	X	X		X
Claimed LUNs	X	X	X	X		X
Databases (Oracle, Sybase, DB2, MS-SQL)						
Device handles	X	X	X	X	X	X
Dynamic Multipathing	X	X	X	X		X
EMC PowerPath			X	X		X
File systems	X	X	X	X	X	X
HBAs	X	X	X	X		X
Host connectivity and topology	X	X	X	X		X
Microsoft Exchange						
Native volume managers	X	X	X	X	X	X
Solaris zones				X	X	
Veritas Cluster Server	X	X	X	X		X
Veritas Volume Manager	X	X	X	X	X	X
ZFS				X		

[1] VMware guest operating systems include Linux, Solaris x86, and Windows.

Commands that require root access for agentless discovery of UNIX hosts

CommandCentral requires a user account to perform agentless discovery of a remote UNIX host. The minimum requirement is a non-root user account. However, there are a few cases where CommandCentral requires a root user account.

Table 1-8 identifies the commands that require root access.

Table 1-8 Commands that require root access for agentless discovery

Storage resource	Operating system	Command	Purpose	Requirement[1]
Disks	HP-UX	/usr/sbin/diskinfo	Provides device handles for disks.	Mandatory
EMC PowerPath	Linux and Solaris	/sbin/powermt check_registration	Provides license-related information.	Mandatory
		/sbin/powermt display dev=all	Provides the paths and their status details.	Mandatory
HBAs or target ports	Solaris	fcinfo	Provides the Fibre Channel-related details regarding HBA, HBA port WWNs, etc.	Optional
	HP-UX	/opt/fcms/bin/ fcmsutil		Mandatory
Linux LVM	Linux	vgdisplay -version	Determines the version of LVM in use on the host.	Mandatory
		vgdisplay -v --units b	Provides volume-related details for all volumes.	Mandatory
		lvdisplay -m --units b	Provides volume-related details for all volumes.	Mandatory
Non-global zones	Solaris	Zlogin	Discovers how storage is consumed in non-global zones.	Mandatory
		df -glZ	Identifies the file systems that are mounted in non-global zones.	Optional
Solaris Volume Manager	Solaris	/usr/sbin/prtvtoc	Discovers information about disks and disk slices. CommandCentral uses the information to calculate capacities for disk groups.	Mandatory
		/usr/sbin/vxdmpadm	Checks the enabled and disabled states of the DMP path during SUNVM agentless discovery.	Optional
Veritas Volume Manager	AIX, HP-UX, Linux, and Solaris	vxdisk list	Provides information about Veritas DMP-related paths.	Optional

[1] Mandatory indicates that that part of feature discovery fails if you do not provide root access for the command. Optional indicates that most of the feature discovery works even if you do not provide root access for the command.

Installing OpenSSH on HP-UX

HP-UX Secure Shell version A.05.30 is based on OpenSSH 5.3 and supports:

- HP-UX 11i v1
- HP-UX 11i v2
- HP-UX 11i v3

HP-UX Secure Shell version A.05.30 contains the following libraries:

- OpenSSL
- Zlib
- TCP Wrappers

Open SSH 5.3 is linked with OpenSSL A.00.09.81.

To install OpenSSH on HP-UX

1. Download the SSH depot from the following location on the HP Web site:

   https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1471AA

2. Install the OpenSSH depot using the `swinstall` command.

Configuring CommandCentral to discover Brocade and McDATA switches through DCFM 10.4.x

You can configure CommandCentral to discover the Brocade and McDATA switches that the Brocade Data Center Fabric Manager (DCFM) 10.4.x manages. You configure discovery of the DCFM through the BrocadeSwitchExplorer.

If CommandCentral currently discovers your Brocade and McDATA switches through another method, you can unconfigure those configurations and configure discovery through DCFM.

To configure CommandCentral to discover Brocade and McDATA switches through DCFM 10.4.x

1. Click **Tools > Configure a New Device**.
2. In the **Configure Device - Select Device Type** panel, select the device category **Switch** and the device type **Brocade Switch**. Then, click **Next**.

3 In the **Configure Device - Select Explorer** panel, select the host from which you want to perform discovery. The selected host must have a physical connection to the host where DCFM runs. Then, click **Next**.

   This panel displays only if you have more than one host that runs the Brocade switch explorer.

4 In the **Configure Device - Device Credentials** panel, enter the required information. Then, click **Next**.

   See "Device Credentials panel options for Brocade and McDATA switches discovered through DCFM 10.4.x" on page 27.

5 In the **Configure Device - Status** panel, click **Finish**.

Device Credentials panel options for Brocade and McDATA switches discovered through DCFM 10.4.x

Enter information in this panel to discover the Brocade and McDATA switches that a Brocade Data Center Fabric Manager (DCFM) 10.4.x manages.

Table 1-9 Configure Device - Device Credentials panel options for Brocade and McDATA switches discovered through DCFM 10.4.x

Field	Description
SMI-S CIMOM IP Address or Name	Enter the IP address or name of the host where DCFM 10.4.x runs.
Login	Enter a user name for the DCFM's integrated SMI-S Agent. The user name that you enter depends on the authentication method for the SMI-S Agent. In the SMIA Configuration Tool, you can set the CIMOM Server Authentication to one of the following: ■ No Authentication ■ DCFM Authentication If you use No Authentication, you still need to enter a user name and password in the Configure a New Device Tool. You can enter any user name and password. If you use DCFM Authentication, the SMI-S Agent credentials are equal to the DCFM Administrator credentials. Enter those credentials in the Configure a New Device Tool.
Password	Enter the password for the specified user name.
Use SMI-S	This read-only field enables discovery and management through SMI-S.

Table 1-9 Configure Device - Device Credentials panel options for Brocade and McDATA switches discovered through DCFM 10.4.x *(continued)*

Field	Description
Interop Namespace	Enter the interop namespace that the DCFM SMI-S Agent uses. The default is `interop`. See vendor documentation to determine whether this value should be changed.
HTTP Port	Enter the HTTP port to use for clear text HTTP SMI-S messages. The default is 5988. See vendor documentation to determine whether this value should be changed. If you configured the DCFM SMI Agent to use a non-default port, enter that value here.
HTTPS Port	Enter the HTTPS port to use for SSL HTTP SMI-S messages. The default is 5989. See vendor documentation to determine whether this value should be changed. If you configured the DCFM SMI Agent to use a non-default port, enter that value here.
Use SSL encryption	Check to use SSL encryption instead of clear text HTTP for SMI-S messages. Ensure that the SMI Agent is configured for SSL.
Use SSL Mutual Authentication	Check if you want to configure the explorer to attempt mutual authentication. Both the explorer and the SMI-S CIMOM send their respective SSL certificates during the SSL handshake. If you select this option, you must manually install the CommandCentral SMI-S certificate to the SMI-S CIMOM Truststore. Consult your vendor documentation. If you do not select this option, the SSL authentication mode is set to `Client Authentication Only`. In this case, only the SMI-S CIMOM is expected to send its SSL certificate for validation. The option is deselected by default. The default setting is `Client Authentication Only`.

Table 1-9 Configure Device - Device Credentials panel options for Brocade and McDATA switches discovered through DCFM 10.4.x *(continued)*

Field	Description
SSL Trust All Certificates	Check if you want the explorer to trust all SSL certificates. If you enable this option, the explorer accepts any certificate that the CIMOM passes during the SSL handshake. If not selected, the explorer checks the certificate that the CIMOM passes against the installed CIMOM's public certificate. The public certificate is in the CommandCentral SMI-S CIMOM SSL Truststore. If you deselect this option, you must manually install the SMI-S CIMOM certificate to the CommandCentral SMI-S CIMOM SSL Truststore.
Enable Discovery	Check to enable discovery and management of the fabric.
Configuration Name	(Optional) Enter a user-friendly name to identify the switch.
Verify Device Configuration	Check to verify that the DCFM can be contacted using the information that you have entered.

View V_NETAPP_DEDUPLICATION_BASE

The database view, V_NETAPP_DEDUPLICATION_BASE, provides information about the deduplication of NetApp flex volumes with Single Instance Storage (SIS). You can use this information when you create ad hoc reports (SQL queries).

Table 1-10 Columns included in the view

Column	Description
ArrayLink	Unique database number of the NetApp unified storage system.
ArrayName	Name of the NetApp unified storage system.
DBObjectKey	Unique ID of the volume.
DedupState	Whether deduplication is enabled or disabled on the volume.
EffectiveUsed	Used capacity of the volume, if no space was shared. This capacity is calculated as follows: space saved + space used.
Lastsisoperationbegin	Start timestamp of the last SIS operation.
Lastsisoperationend	End timestamp of the last SIS operation.

Table 1-10 Columns included in the view *(continued)*

Column	Description
LogicalUsed	Used capacity of the volume.
SerialNumber	Serial number of the volume.
SpaceSaved	The disk space savings from the shared space.
SpaceSavedPercent	Percentage of space savings from the shared space. This percentage is calculated as follows: SpaceSaved / EffectiveUsed. This information is available if the SIS volume is online.
SpaceShared	Used space of the volume that is shared. This information is available if the SIS volume is online.
SubscribedPercent	Percentage of the space that the volume uses with regards to the logical capacity. The percentage helps to determine whether used storage would outgrow logical storage (over subscription), if no space was shared. This percentage is calculated as follows: (EffectiveUsed / TotalLogicalCapacity) * 100.
TotalLogicalCapacity	Total logical capacity of the volume.
RAIDLevel	RAID level of the volume.
Volume	Name of the volume.
VolumeLink	Unique database number of the volume.

Issues fixed in CommandCentral 5.2 RU1

In addition to the issues fixed in CommandCentral 5.2 , CommandCentral 5.2 RU1 includes fixes to the following issues.

For information about the issues fixed in CommandCentral 5.2, see *CommandCentral 5.2 Release Notes*.

Table 1-11 Issues that are fixed in CommandCentral 5.2 RU1

Incident	Description
2129330	In the SAN scope, the Host Storage Assessment report now includes DAS-based data for disk groups when you select the **Include DAS** option.

Table 1-11 Issues that are fixed in CommandCentral 5.2 RU1 *(continued)*

Incident	Description
2133634	In CommandCentral Storage 5.2, the Host Management page sometimes shows the following runtime error: `Exception: Internal error, found multiple copies of table WEBUTIL_STR_MANAGED_HOSTS_TABLE instance` This issue is fixed in CommandCentral Storage 5.2 RU1.
2146974	In CommandCentral Storage 5.2, the disk group capacity on SAN storage showed in the **DiskGroup Capacity DAS** column. In CommandCentral Storage 5.2 RU1, disk group capacity on SAN storage now correctly shows in the **DiskGroup Capacity SAN** column.
2202275	The Online Storage report in CommandCentral Storage 5.2 erroneously showed LUNs that were masked to multiple user-created hosts as **Unclaimed** instead of **Unknown**. As a result of this error, some LUNs appeared in the incorrect slice of the waterfall chart. CommandCentral Storage 5.2 RU1 correctly shows user-created host LUNS as **Unknown**.
2206747	The date column in the CommandCentral Storage 5.2 task tree table did not sort. This issue is fixed in CommandCentral Storage 5.2 RU1.
2227196	In CommandCentral Storage 5.2, the Host Storage Assessment report displayed "N/A" for all file systems used for VMware guests even though CommandCentral Storage 5.2 discovered file system information for those guests. The only way to include information for file systems for VMware guests in CommandCentral Storage 5.2 was to select the **Include DAS** option in the report, thereby including directly-attached storage. However, when CommandCentral Storage 5.2 included information about directly-attached storage, it only considered uncorrelated file systems on SAN storage. It did not consider the uncorrelated file systems on NAS storage. CommandCentral Storage 5.2 RU1 has been updated to consider both SAN and NAS-based uncorrelated file systems.

Table 1-11 Issues that are fixed in CommandCentral 5.2 RU1 *(continued)*

Incident	Description
2230505	The masked LUNs capacity did not show on the **Storage** tab of the CommandCentral Storage 5.2 host view. CommandCentral Storage 5.2 RU1 now shows the masked LUNs capacity on the host view **Storage** tab.
2232853	In CommandCentral Storage 5.2, the **Last Update** column on the **Host Update** page showed incorrect times. The **Last Update** column on the **Host Update** page shows the correct time in CommandCentral Storage 5.2 RU1.
2233664	CommandCentral Storage 5.2 sometimes incorrectly identified the host name for managed virtual machine objects corresponding to virtual machines. CommandCentral Storage 5.2 RU1 uses the virtual machine's name as the hostname for managed virtual machine objects if either of the following is true: ■ The guest machine's network is unreachable from the explorer host ■ The virtual machine IP address is 0.0.0.0.
2234416	When you configure credentials in CommandCentral Storage 5.2, you only see pre-defined explorers in the **Configure Credentials** list. New explorers you define at run time do not appear in the **Configure Credentials** list. CommandCentral Storage 5.2 RU1 shows both new and pre-defined explorers in the **Configure Credentials** list.
2245713	If different users create multiple hosts with the same name in CommandCentral Storage 5.2, you cannot delete the extraneous host entries from the **Agent** table. CommandCentral Storage 5.2 RU1 allows you to delete multiple hosts with the same name from the **Agent** table.
2236870	CommandCentral Storage 5.2 RU1 now reports correct capacities for Symmetrix thin devices.

Known issues in CommandCentral 5.2 RU1

The following known issues are introduced in the 5.2 RU1 release.

LPAR discovery limitations

The following limitations apply to LPAR discovery:

- CommandCentral Storage supports only native device handles as a backing device. We do not support LVM volumes, or DMP devices.
- CommandCentral Storage does not support standard agent or agentless discovery of VIO servers.
- If you configure LPARs agentlessly, you'll need to rediscover those hosts after the upgrade for immediate visibility of correlated data.
- Some reports may be incorrect if you use an unsupported backing device. For example, if you use an LVM volume, in the waterfall report, the totals for **VM Consumption** are greater than the totals for **VM Allocated**.
- In a clustering scenario, when multiple LPARs share the same virtual device, the storage is counted multiple time from an aggregated LPAR capacity perspective. For example, in the waterfall report, the totals for **VM Consumption** are greater than the totals for **VM Allocated**.
- If an LPAR has multiple paths to the same LUN, disabling MPIO on the LPAR results in counting storage more than once. The double counting occurs because multiple device handles are created for the LUN.

Mixed fabric zoning (Brocade-McData) discovery using DCFM 10.4.x

You can discover fabric zoning information using DCFM 10.4.x for mixed (Brocade-McData interoperability) fabrics and pure EOS (McData) fabrics.

To discover fabric zoning information for mixed (Brocade-McData) and pure EOS fabrics

- Set the **MixedFabric_Management** key to **2**.

  (The default setting is 1).

Missing GUI information due to non-root agentless configuration of Solaris hosts

If a non-root user configures Solaris hosts agentlessly, the following information will be missing from the GUI:

- The Sun disk set capacity is not discovered
- Disk and slice information is not discovered.

If the disk and slice information is not discovered, the following correlations are impacted:

- Volume to LUN
- Soft Partition to LUN

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 Storage to discover the storage arrays from which the multipathing LUNs are allocated to the host. Otherwise, CommandCentral Storage cannot discover the IDs for the LUNs that are allocated to the host. As a result, CommandCentral Storage identifies the device handles for the LUNs as separate disks and capacities are multiplied in the Storage Consumption reports.

This incident applies to EMC PowerPath (emcpower devices) and HPUX 11.31 (Agile disks).

For information about supported multipathing software, see the *CommandCentral Hardware and Software Compatibility List*. This document is updated regularly at:

http://www.symantec.com/docs/TECH148619

The Console lets you configure agentless discovery of the same host multiple times (2229779)

When you configure agentless discovery of remote hosts, you can enter any of the following to identify the host:

- Host name
- Fully-qualified host name
- IP address

You can configure discovery of the same host multiple times if you choose a different identifier each time. For example, you can discover the same host three different times if you separately enter the host name, fully-qualified host name, and then the IP address. As a result, data for that host appears multiple times.

If you mistakenly add the same host multiple times, you can unconfigure the extra hosts.

Erroneous uninstallation failure warning (2231550)

When you uninstall CommandCentral Storage 5.2RU1, you see the following erroneous uninstallation failure warning:

```
WARNING: Failed to remove service VRTSccsweb. Command
C:\PROGRA~2\VERITAS\VRTSweb\bin\install\webappsvc.exe -uninstall VRTSccsweb
returned Error: 1!!!
```

This warning appears even though the service is successfully removed. You can ignore this warning.

Capacity calculation and correlation issues on some SunVM configurations (2246290)

The following issues have been observed in SunVM configurations:

- A Sun Diskset may report incorrect total storage capacities for discovery disks with EFI labels running on Solaris with SunVMs.
- If you configure a Solaris host agentlessly on the Management Server, and the host contains a local zone, the SunVM is missing a local disk set to LUN correlation.

Host Storage Assessment may be over 100% for hosts discovered by the VMware tools VI SDK (2251667)

In CommandCentral Storage 5.2 RU1, in the **Exclude DAS** option, the Host Percentage Utilization in the Host Storage Assessment Report may be over 100% for hosts discovered by the VMware tools VI SDK.

Due to a missing file system to LUN correlation, CommandCentral Storage cannot determine if a file system is on SAN or local, directly-attached storage (DAS). CommandCentral Storage counts the uncorrelated storage as SAN storage. If file systems are on DAS storage, the utilization percentage calculation may be over 100% on some hosts.

Virtualization detail report lists incorrect server types (2255844)

In the Host Virtualization Detail report, Managed Virtual Machine Storage Usage table, the VIO Servers column erroneously lists GZ servers for Solaris Zones and ESX servers for VMWare.

An incorrect error message displays when you configure HMC in LPARExplorer (2258172)

When you configure HMC for IBM LPAR discovery in CommandCentral Storage, you may see an incorrect error message pertaining to configuration errors, such

as invalid HMC IP address, invalid username, or invalid password. The error message contains the words:

```
Failed to execute command. Command may not be valid or system may be
out of resources
```

If you encounter this error message, check the configuration data you entered and try the operation again.