

Veritas CommandCentral™ Release Notes

for Microsoft Windows and UNIX

5.2 RU2



CommandCentral 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 RU2.0

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

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

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

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

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

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
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

Veritas CommandCentral™ Release Notes

This document includes the following topics:

- [Upgrading to CommandCentral 5.2 RU2](#)
- [What's new in CommandCentral 5.2 RU2](#)
- [Issues fixed in CommandCentral 5.2 RU2](#)
- [Known issues in CommandCentral 5.2 RU2](#)

Upgrading to CommandCentral 5.2 RU2

CommandCentral 5.2 RU2 is an update to the CommandCentral 5.2 release. You can upgrade the following CommandCentral components to 5.2 RU2:

Management Server

Control Host

You can upgrade to CommandCentral 5.2 RU2 from version 5.2 or 5.2 RU1.

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 RU2.

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_5.2RU2_Solaris_MS.tar.gz`.

- 3 Type the following commands to uncompress the tar file:

```
gunzip VRTS_CommandCentral_5.2RU2_Solaris_MS.tar.gz
```

```
tar -xf VRTS_CommandCentral_5.2RU2_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_5.2RU2_Windows_MS.zip`.

- 3 Extract `VRTS_CommandCentral_5.2RU2_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 or 5.2 RU1 Control Host to 5.2 RU2.

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_5.2RU2_Solaris_CH.tar.gz`.

- 3 Type the following commands to uncompress the tar file:

```
gunzip VRTS_CommandCentral_5.2RU2_Solaris_CH.tar.gz
```

```
tar -xf VRTS_CommandCentral_5.2RU2_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_5.2RU2_Windows_CH.zip`.

- 3 Extract `VRTS_CommandCentral_5.2RU2_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 RU2

CommandCentral 5.2 RU2 includes the following new features and enhancements.

Note: If you are upgrading to 5.2 RU2 from CommandCentral 5.2, it is recommended that you consult the *Veritas CommandCentral 5.2 RU1 Release Notes*. You can find this document at <https://sort.symantec.com>.

Table 1-1 New features and enhancements

Feature	Description
New default port to connect to the Console	<p>In CommandCentral 5.2 RU2, the default port that you use to connect to the CommandCentral Console changes.</p> <p>When you upgrade to CommandCentral 5.2 RU2 from 5.2 or 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.</p> <p>For example, to connect to CommandCentral Storage, you need to enter the following URL in your Web browser: <code>https://myhost.example.com:14191/cc</code></p> <p>To connect to CommandCentral Storage Change Manager, you need to enter the following URL in your Web browser: <code>https://myhost.example.com:14191/sm</code></p> <p>If you need to, you can change the default port. For example, you can change the default port back to 8443.</p> <p>See “Changing the port for the CommandCentral Console” on page 11.</p> <p>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 RU2, CommandCentral is the only Symantec product that uses the Web server.</p> <p>Note: To start and stop the Web server in 5.2 RU2, you can use the <code>vxccs</code> utility. For Solaris, the process is called <code>esmweb</code>. For Windows, the process is called <code>CCSGUI</code>. 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.</p>

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

Feature	Description
Support for new hardware and software	<p>CommandCentral 5.2 RU2 provides added hardware and software support. For the latest support information, see the <i>CommandCentral Hardware and Software Compatibility List</i>. This document is updated regularly at:</p> <p>http://www.symantec.com/business/support/index?page=content&key=50379&channel=TECHNICAL_SOLUTION&basecat=COMPATIBILITY_LIST&sort=popular</p> <p>CommandCentral 5.2 RU2 now includes support for the following:</p> <ul style="list-style-type: none"> ■ EMC Solutions Enabler, version 7.2.1. ■ DB2 on Linux in a Kerberos environment. ■ Red Hat Enterprise Linux 6 (RHEL 6) for both agent and agentless installations. ■ The Veritas Operations Manager (VOM) 4.0 agent. ■ NetApp ONTAP operating system, version 8 (existing features only, no new ONTAP features). ■ Microsoft Diagnostic and Recovery Toolset (DART) , version 6.0.40.500 and later on EMC NS480, NS120, and NSG. ■ FLARE 30 for EMC CLARiiON CX4 storage platforms. ■ EMC CLARiiON Navisphere Command Line Interface (CLI) 7.30. ■ Hitachi Device Manager 7.1. ■ Brocade Network Advisor 11. ■ EMC UniSphere 1.0.50.1.0326.
Non-root users can start and stop the Web engine	<p>CommandCentral 5.2 RU2 now lets non-root users start and stop the Web Engine.</p> <p>See “Letting non-root users start and stop the Web Engine” on page 12.</p>
Discovery of Brocade switches running in Access Gateway mode	<p>CommandCentral 5.2 RU2 now discovers Brocade switches running in Access Gateway mode.</p> <p>See “Support for Brocade Access Gateways” on page 15.</p>

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/VRTScstw/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/VRTS/bin/
Windows	\Program Files\VERITAS\CommandCentral Storage\Support\Tools\Vxccs

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

Solaris	<pre>./vxccs stop esmweb ./vxccs start esmweb</pre>
Windows	<pre>vxccs.bat stop CCSGUI vxccs.bat start CCSGUI</pre>

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

Letting non-root users start and stop the Web Engine

As an administrator, you can run a PERL script to allow local, non-root users to start and stop the CommandCentral Storage Web Engine. You can run another PERL script to revoke privileges for specific non-root users, so they can no longer start and stop the Web Engine. You set up and revoke non-root user privileges separately for your Windows and Solaris servers.

Note: The procedures in this section require each non-root user to have their own unique home directory.

Granting privileges to start and stop the Windows Web engine

If you are an administrator, follow these steps to grant privileges to let local, non-root users start and stop the Web Engine.

To grant privileges for non-root users to start and stop the Windows Web Engine

- 1 Log in to the system as an administrator.
- 2 Run the script for granting privileges to non-root users. Enter the following:

```
Installation Directory\VERITAS\CommandCentral Storage\HAL\bin\perl  
Installation Directory\VERITAS\CommandCentral  
Storage\Support\Tools\NonPrivilegedWebServer  
\WindowsNonRootUserWebServer.pl grant
```

- 3 At the username and password prompts, enter the username and password for the non-root user to whom you want to grant privileges.

After you grant privileges for local, non-root users, ask the users to follow these steps to authenticate themselves.

To authenticate yourself as a non-root user

- 1 Log in as a non-root user for whom privileges are granted.
- 2 Run the script for authenticating yourself. Enter the following:

```
Installation Directory\VERITAS\CommandCentral Storage\HAL\bin\perl  
Installation Directory\VERITAS\CommandCentral  
Storage\Support\Tools\NonPrivilegedWebServer  
\WindowsNonRootUserWebServer.pl authenticate
```

The Web Engine starts.

Granting privileges to start and stop the Solaris Web Engine

If you are an administrator, follow these steps to grant privileges to let local, non-root users start and stop the Solaris Web Engine.

To grant privileges for non-root users to start and stop the Solaris Web Engine

- 1 Log in to the system as an administrator.
- 2 Run the script for granting privileges to non-root users. Enter the following:

```
Installation Directory/VRTScCs/VRTShal/bin/perl
```

```
Installation
```

```
Directory/VRTScCs/VRTScCssts/support/tools/NonPrivilegedWebServer
```

```
/SolarisNonRootUserWebServer.pl grant
```

- 3 At the username and password prompts, enter the username and password for the non-root user to whom you want to grant privileges.

After you grant privileges for local, non-root users, ask the users to follow these steps to authenticate themselves.

To authenticate yourself as a non-root user

- 1 Log in as a non-root user for whom privileges are granted.
- 2 Run the script for authenticating yourself. Enter the following:

```
Installation Directory/VRTScCs/VRTShal/bin/perl
```

```
Installation
```

```
Directory/VRTScCs/VRTScCssts/support/tools/NonPrivilegedWebServer
```

```
/SolarisNonRootUserWebServer.pl authenticate
```

The Web Engine starts.

Revoking privileges to start and stop the Web Engine

Run the Windows or Solaris PERL script for revoking privileges to block local, non-root users from starting and stopping the CommandCentral Storage Web Engine.

Revoking privileges on Windows

- 1 Log on as an administrator.
- 2 Run the Windows script for revoking privileges. Enter the following:

```
Installation Directory\VERITAS\CommandCentral Storage\HAL\bin\perl  
Installation Directory\VERITAS\CommandCentral  
Storage\Support\Tools\NonPrivilegedWebServer  
\WindowsNonRootUserWebServer.pl revoke
```

- 3 At the username and password prompts, enter the username and password for the non-root user to whom you want to revoke privileges.

The Web Engine starts.

Revoking privileges on Solaris

- 1 Log on as the root user.
- 2 Run the Solaris script for revoking privileges. Enter the following:

```
Installation Directory\VRTScs\VRTShal/bin/perl  
Installation  
Directory\VRTScs\VRTScsts/support/tools/NonPrivilegedWebServer  
/SolarisNonRootUserWebServer.pl revoke
```

- 3 At the username and password prompts, enter the username and password for the non-root user to whom you want to revoke privileges.

The Web Engine starts.

Support for Brocade Access Gateways

CommandCentral Storage now supports the ability to run Brocade switches in Access Gateway mode. Servers connected to Brocade switches that run in Access Gateway mode provide server access to the SAN fabric without creating new fabric domains.

If you have installed CommandCentral Storage 5.2 RU1, you do not have to configure CommandCentral Storage to discover Access Gateways. The DCFM agent installed with CommandCentral Storage 5.2 RU1 will start discovering your Access Gateways, and the switches that are connected to the Access Gateways.

If you are running Brocade switches in Access Gateway mode, you see the Access Gateway Summary table on the SAN - Switches page. You can add a hidden Switch Role column to the Access Gateway Summary table. You can also view information about an individual Brocade Access Gateway switch in its Overview pane. The

Overview pane displays the Access Gateway's vendor (manufacturer), model, firmware version, WWN, IP addresses (in IPv6 format), role, object dependency group, and a graph showing port usage. The object dependency group tables also include information about Access Gateways, and Access Gateway ports, where applicable. The Connectivity tab shows the Access Gateway's port connections, port mapping, and a trunk table.

The CommandCentral Storage Access Gateway support comes with the following limitations:

- CommandCentral Storage does not include Failover and Failback attributes for the N ports of an Access Gateway.
- CommandCentral Storage does not support monitoring for Access Gateways.
- CommandCentral Storage does not provide a change history link for Access Gateways.

Issues fixed in CommandCentral 5.2 RU2

CommandCentral 5.2 RU2 includes fixes to the following issues.

For information about additional issues fixed since CommandCentral 5.2, see *CommandCentral 5.2 RU1 Release Notes*.

Table 1-2 Issues that are fixed in CommandCentral 5.2 RU1

Incident	Description
2214716	CommandCentral Storage 5.2 did not show performance values for some IBM SVC LUNs when it used an SMI-S agent. This issue is resolved in CommandCentral Storage 5.2 RU2.
2238171	In previous CommandCentral Storage versions, there was a performance issue in DBCT. A large number of historical records were created, and that slowed down insert and update operations. This issue is resolved in CommandCentral Storage 5.2 RU2.
2242960	In CommandCentral Storage 5.2 RU1, pathnames in the Device Path column are incorrect for agile disks. This issue is resolved in CommandCentral Storage 5.2 RU2.
2244630	In CommandCentral Storage 5.2 RU1, agentless discovery of AIX hosts sometimes failed with <code>Error V-86-18-97</code> . This issue is resolved in CommandCentral Storage 5.2 RU2.

Table 1-2 Issues that are fixed in CommandCentral 5.2 RU1 (*continued*)

Incident	Description
2270756	<p>In CommandCentral Storage 5.1, claimed and unclaimed LUNs were double-counted if they were related to share disks on cluster nodes.</p> <p>This problem is fixed in CommandCentral Storage 5.2.</p>
2270822	<p>In CommandCentral Storage 5.2 RU1, agentless discovery of HPUX hosts sometimes failed.</p> <p>This issue is resolved in CommandCentral Storage 5.2 RU2.</p>
2274717	<p>The CommandCentral Storage 5.2 GUI still shows thin source LUN capacity in the Array Summary table LUNCapacity column, even if you set CommandCentral Storage to exclude thin pool source LUNs.</p> <p>This is fixed in CommandCentral Storage 5.2 RU2.</p>
2279555	<p>CommandCentral Storage 5.2 RU2 adds support for discovering arrays with HP XP CVAE (CLI only) for customers with core licenses.</p>
2280662	<p>In previous CommandCentral Storage versions, there was a performance issue with SAN and NAS waterfall reporting.</p> <p>This issue is resolved in CommandCentral Storage 5.2 RU2.</p>
2286596	<p>In CommandCentral Storage 5.2 RU1, the email reporting feature did not work correctly because the installer installs the mail.jar file in the wrong location.</p> <p>The email reporting feature now works correctly in CommandCentral Storage 5.2 RU2.</p>
2299450	<p>In CommandCentral Storage 5.2, the Symmetrix explorer fails on some control hosts when you try to discover VMAX virtual storage.</p> <p>This issue was fixed in CommandCentral Storage 5.2 RU2.</p>
2319540	<p>In CommandCentral Storage 5.2 RU1, the ZonesExplorer files sometimes grow very large.</p> <p>This issue is resolved in CommandCentral Storage 5.2 RU2.</p>

Table 1-2 Issues that are fixed in CommandCentral 5.2 RU1 (*continued*)

Incident	Description
2319837	<p>The Agile node for HPUX agentless does not get created in CommandCentral Storage 5.2 RU1 if some of the underlying paths are disabled.</p> <p>This issue is resolved in CommandCentral Storage 5.2 RU2.</p>
2321289	<p>Previously disks sometimes did not correlate properly with volumes in some Windows agentless configurations.</p> <p>This issue is resolved in CommandCentral Storage 5.2 RU2.</p>
2323006	<p>In previous CommandCentral Storage versions, there were performance issues with VMware explorer DCT.</p> <p>This issue is resolved in CommandCentral Storage 5.2 RU2.</p>
2328446	<p>CommandCentral Storage 5.2 added the thin source LUN capacity to the Array Summary table's LUNCapacity column , which resulted in double counting.</p> <p>This issue is resolved in CommandCentral Storage 5.2 RU2.</p>
2328885	<p>In CommandCentral Storage 5.2, agentless discovery of hosts didn't succeed if the remote host had a non-English operating system.</p> <p>CommandCentral Storage 5.2 RU2 successfully performs agentless discovery of hosts with non-English operating systems.</p>
2336617	<p>CommandCentral Storage 5.2 had problems discovering HP EVA 4400 arrays.</p> <p>CommandCentral Storage 5.2 RU2 can now reliably discover HP EVA 4400 arrays.</p>
2338228	<p>In 5.2 RU1, the CommandCentral Storage GUI does not discover Netapp Data Ontap 8.x fiber channel adapters and ports.</p> <p>CommandCentral Storage 5.2 RU2 now discovers Netapp Data Ontap 8.x fiber channel adapters and ports.</p>
2338266	<p>In CommandCentral Storage 5.2 RU1, Celerra DART6 discovery fails while discovering the iSCSI targets.</p> <p>This issue is resolved in CommandCentral Storage 5.2 RU2.</p>

Table 1-2 Issues that are fixed in CommandCentral 5.2 RU1 (*continued*)

Incident	Description
2383113	<p>Auto refresh does not stay enabled in CommandCentral Storage 5.2.</p> <p>This issue is resolved in CommandCentral Storage 5.2 RU2.</p>
2390317	<p>In previous CommandCentral Storage versions, the GUI pages for the Array Summary and Host Summary reports sometimes loaded slowly.</p> <p>The Array Summary and Host Summary GUI pages load more quickly in CommandCentral Storage 5.2 RU2.</p>
2396352	<p>CommandCentral Storage loaded slowly after an upgrade to 5.2 RU1.</p> <p>CommandCentral Storage 5.2 RU2 loads more quickly.</p>
2396526	<p>CommandCentral Storage 5.2RU2 now discovers online shared storage capacity if the MSCS cluster uses Windows LDM as a resource. Install CommandCentral Storage 5.2 RU2 on your Management Server, and install the hotfix <code>ccs-F520002329100.tar.gz</code> on your managed hosts.</p>
2402675	<p>CommandCentral Storage 5.2 RU1 sometimes did not discover LPARs on IBM P570 servers.</p> <p>CommandCentral Storage 5.2 RU2 now reliably discovers LPARs on IBM P570 servers.</p>
2404749	<p>Previous CommandCentral Storage sometimes hang at login time because of a locked vxam.session table.</p> <p>CommandCentral Storage 5.2 RU2 no longer hangs at login because of this issue.</p>
2407056	<p>CommandCentral Storage 5.1 and 5.2 had issues with the Last Update Time column showing future times.</p> <p>This issue is resolved in CommandCentral Storage 5.2 RU2.</p>
2407810	<p>CommandCentral Storage 5.2 RU1 did not correctly discover IBM XIV storage arrays if the cluster names had spaces.</p> <p>This issue is resolved in CommandCentral Storage 5.2 RU2.</p>

Table 1-2 Issues that are fixed in CommandCentral 5.2 RU1 (*continued*)

Incident	Description
2409462	<p>After upgrading to CommandCentral Storage 5.2 RU1, some reports appear in the wrong sort order, and some some attributes are missing.</p> <p>This issue is resolved in CommandCentral Storage 5.2 RU2.</p>
2409468	<p>The CommandCentral Storage GUI reports the 4GB and 8GB online ports for Cisco switches as <i>Unknown</i>.</p> <p>This issue is resolved in CommandCentral Storage 5.2 RU2.</p>
2411510	<p>After upgrading to CommandCentral Storage 5.2 RU1, agentless discovery is incomplete for SUSE 10 hosts that are discovered manually.</p> <p>This issue is resolved in CommandCentral Storage 5.2 RU2.</p>
2426250	<p>When CommandCentral Storage 5.2 is used with a Netapp filer configuration, CommandCentral Storage does not always correlate the source filer name with the destination name for Netapp shares.</p> <p>CommandCentral Storage 5.2 RU2 now correlates the source and destination filer names correctly.</p>
2434722	<p>In CommandCentral Storage 5.2, refreshing an array on a partially discovered Symmetrix array fails.</p> <p>Refreshing an array on a partially-discovered Symmetrix array does not fail in CommandCentral Storage 5.2 RU2.</p>

Known issues in CommandCentral 5.2 RU2

The following known issues are introduced in the 5.2 RU2 release.

Host reboot requirement when you upgrade to CommandCentral Storage 5.2 RU2 on Windows

When you upgrade to CommandCentral Storage 5.2 RU2 on Windows, the installer sometimes asks you to reboot the host after the upgrade completes. The solution is to reboot the host to complete the upgrade process.

Erroneous exception when non-root user stops the Web Engine

CommandCentral Storage lets you grant privileges to non-root users to start and stop the Web Engine. If a non-root user stops the Web Engine using the services panel, CommandCentral Storage may throw an erroneous exception.

Workaround: Non-root users should stop the Web Engine using the `vxccs stop CCSGUI` command instead of using the Windows services panel.

LPAR discovery limitations

The following limitations apply to LPAR discovery:

- CommandCentral Storage supports only native device handles as a backing device. It does 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 HP-UX 11.31 (Agile disks).

For information about supported multipathing software, see the *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 CommandCentral Storage uninstallation failure warning (2231550)

When you uninstall the CommandCentral Storage 5.2RU1 add-on, 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.