Veritas™ Cluster Server Release Notes

Windows Server 2012 (x64)

6.0.2

January 2013

Symantec

Veritas Cluster Server 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.

Product version: 6.0.2

Document version: 6.0.2 Rev 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 website at the following URL:

www.symantec.com/business/support/index.jsp

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/contact_techsupp_static.jsp

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

Documentation

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com

For information regarding the latest HOWTO articles, documentation updates, or to ask a question regarding product documentation, visit the Storage and Clustering Documentation forum on Symantec Connect.

https://www-secure.symantec.com/connect/storage-management/forums/storage-and-clustering-documentation

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.

http://www.symantec.com/connect/storage-management

Veritas Cluster Server for Windows Release Notes

This document includes the following topics:

Introduction

This document provides important information regarding Veritas Cluster Server (VCS) for Windows, VCS enterprise agents for NetApp SnapMirror and VCS database agent for Microsoft SQL. Please review this entire document before using this product.

The information in the Release Notes supersedes the information provided in the product documents.

You can download the latest version of this document from the Symantec SORT website.

https://sort.symantec.com

For the latest information on updates, patches, and software issues regarding this release, see the following Late Breaking News (LBN):

http://www.symantec.com/docs/TECH161556

For general information about VCS for Windows and Veritas Storage Foundation and High Availability Solutions for Windows, see the following Web site:

http://www.symantec.com

For any install/upgrade failures refer to following technote for information on how to recover from failures.

http://www.symantec.com/docs/TECH76129

Requirements

For information about the operating system, hardware, and other general requirements of Veritas Cluster Server for Windows, see the *Veritas™ Cluster Server Installation and Upgrade Guide*.

For the latest information on supported hardware, see the Hardware Compatibility List (HCL) at:

http://www.symantec.com/docs/TECH152806

For the latest information on supported software, see the Software Compatibility List (SCL) at:

http://www.symantec.com/docs/TECH201485

About Symantec Operations Readiness Tools

Symantec Operations Readiness Tools (SORT) is a website that automates and simplifies some of the most time-consuming administrative tasks. SORT helps you manage your datacenter more efficiently and get the most out of your Symantec products.

SORT can help you do the following:

Prepare for your next installation or upgrade	■ List product installation and upgrade requirements, including operating system versions, memory, disk space, and architecture. ■ Analyze systems to determine if they are ready to install or upgrade Symantec products. ■ Download the latest patches, documentation, and high availability agents from a central repository. ■ Access up-to-date compatibility lists for hardware, software, databases, and operating systems.
Manage risks	■ Get automatic email notifications about changes to patches, array-specific modules (ASLs/APMs/DDIs/DDLs), and high availability agents from a central repository. ■ Identify and mitigate system and environmental risks. ■ Display descriptions and solutions for hundreds of Symantec error codes.
Improve efficiency	■ Find and download patches based on product version and platform. ■ List installed Symantec products and license keys. ■ Tune and optimize your environment.

Note: Certain features of SORT are not available for all products. Access to SORT is available at no extra cost.

To access SORT, go to:

https://sort.symantec.com

New features and changes

This section describes the new features and changes introduced in Veritas Cluster Server for Windows (VCSW) 6.0.2.

Windows Server 2012 support

VCSW introduces support for the following Windows operating systems:

- Windows Server 2012 64-bit (Full/Core): Standard Edition, Datacenter Edition, and Hyper-V Edition

The following enhancements have been introduced as a part of this support in this release:

- The vSphere integrated option that is available to install the Symantec High Availability guest components now enables you to install the Symantec High Availability guest components on a system running Windows Server 2012 operating system.

Client support on Windows 8

SFW and SFW HA introduce support for the client components on Windows 8. The supported Windows 8 editions are as follows:

- Windows 8 Pro
- Windows 8 Enterprise

No longer supported

This section lists the features deprecated in this release.

Windows Server 2003 (x86 and x64) and Windows Server 2008 (x86)

VCS Server and Client components are no longer supported on Windows Server 2003 (x86 and x64) and Windows Server 2008 (x86).

Microsoft Exchange 2003 and Microsoft SQL Server 2000

VCS does not support Windows Server 2003 (x86 and x64) in this release. Hence Microsoft Exchange 2003 and Microsoft SQL Server 2000 are also no longer supported. The VCS agents for Exchange 2003 (ExchService, ExchProtocol) and SQL Server 2000 (SQLServer2000, MSSearch) are no longer available.

Microsoft Operations Manager (MOM) 2005

Microsoft Operations Manager (MOM) 2005 is no longer supported in this release.

The hasnap command

The hasnap command has been deprecated in this release.

The hasnap command can be used to take snapshots of the VCS configuration files on cluster nodes. The command can also be used to back up, restore, compare, and export the VCS configuration files.

Software limitations

This section covers Veritas Cluster Server limitations.

Unable to monitor resources on Windows Server 2012 if Switch Independent NIC teaming mode is used

On Windows Server 2012, VCS requires the MAC address of the team NIC to be static. In the default NIC teaming mode (Switch Independent), a static MAC address is not assigned to the team NIC. Therefore, if you plan to use NIC teaming on Windows Server 2012, make sure that the Static Teaming mode is enabled. Otherwise, VCS will not be able to successfully monitor resources. The VCS agent will fail to identify the resources for which they are configured, and report the UNKNOWN state.

Cluster operations performed using the Symantec High Availability dashboard may fail

This issue occurs while performing the cluster operations in a multi-system VCS cluster that is configured in a VMware virtual environment. The cluster configuration is such that a single system belongs to one datacenter or ESX, and all the other systems belong to another datacenter or ESX. (2851434)

In such a cluster configuration, the operations initiated from the dashboard that is available from the datacenter or ESX to which the single cluster system belongs, may fail on the systems that belong to the other datacenter.

This situation arises if the following changes have occurred with the system:

- The system has lost its network connectivity
- The SSO configuration has become corrupt

This occurs because the operations are performed using the network details of the system that belongs to the datacenter or ESX from where they are initiated.

NBU restore changes the disk path and UUID due to which VMwareDisks resource reports an unknown state

When you restore a VMware virtual machine using NetBackup (NBU), it changes the path and UUID of disks because of which the VMwareDisks agent resource goes into an unknown state as it has the old path and UUID configured in its “DiskPaths” attribute. As a workaround, you need to manually provide the new disk path in the “DiskPaths” attribute of the affected VMwareDisks resource and delete the incorrect UUID (and the colon after it) from the attribute. (2913645)

SQL service group configuration wizards fail to discover SQL databases that contain certain characters

The VCS SQL service group configuration wizards fail to discover SQL databases if the database name contains any of the following characters:

- " (inverted commas)
- , (comma)
- [ ] (square brackets)

Unable to restore user database using SnapManager for SQL

While restoring the user database using SnapManager, user needs to select the checkbox which specifies that the snapshot was taken on other machine. The user is also required to select the system name. When this option is selected, it is possible to restore the database.

SnapDrive service fails to start after uninstalling VCS

When VCS is uninstalled and the system is rebooted, the SnapDrive service fails to start with a logon failure.

Workaround: Reset the password for the SnapDrive service account and then start the SnapDrive service.

Undocumented commands and command options

VCS contains undocumented commands and command options intended for development use only. Undocumented commands are not supported for external use.

Windows Safe Mode boot options not supported

The Windows Safe Mode boot options are not supported. VCS services and wizards fail to run if Windows is running in Safe Mode.(1234512)

Security issue when using Java-GUI and default cluster admin credentials

While configuring the cluster using the VCS Cluster Configuration Wizard (VCW) if you do not choose the secure mode (Use Single Sign-on option) on the **Configure Security Service Option** panel, VCW creates a user with user name as admin and

password as password. The user credentials are auto-populated in the respective fields, by default. This user has administrative privileges to the cluster.

Symantec recommends that you create a different user instead of accepting the default values.(1188218)

VCW does not support configuring broadcasting for UDP

VCW does not provide options to configure broadcasting information for UDP. You can configure broadcasting for UDP by manually editing the `llttab` file. Refer to the *Veritas Cluster Server Administrator's Guide* for more information.

Solutions wizard support in a 64-bit VMware environment

In a 64-bit VMware virtual machine environment, the Disaster Recovery, Quick Recovery, and Fire Drill wizards are supported on VMware ESX 3.5 and above. No support is provided for VMware Workstation version.

Cluster Manager (Java Console)

The following are Cluster Manager (Java Console) software limitations.

Latest version of Java Console for VCS is required

Cluster Manager (Java Console) from previous VCS versions cannot be used to manage VCS 6.0.2 clusters. Symantec recommends always using the latest version of Cluster Manager.

Running Java Console on a non-cluster system is recommended

Symantec recommends not running Cluster Manager (Java Console) for an extended period on a system in the cluster.

All servers in a cluster must run the same operating system

All servers in a cluster must run the same operating system. You cannot mix the following Windows operating systems within a cluster:

- Windows Server 2012 (full install) systems and Windows Server 2012 Server Core

Service group dependency limitations

The following are Service group dependency software limitations.

No failover for some instances of parent group

In service groups in which the group dependency is configured as parallel parent/failover child, online global, remote soft or firm, the parent group may not online on all nodes after a child group faults.

System names must not include periods

The name of a system specified in the VCS configuration file, `main.cf`, must not be in the fully qualified form; that is, the name must not include periods. The name in main.cf must be consistent with the name used in the `llthosts.txt` file.

Incorrect updates to path and name of types.cf with spaces

The path of the `types.cf` file, as referenced in the `main.cf`, updates incorrectly if the path contains spaces. For example, C:\Program Files\, would update incorrectly. Running a combination of the `hacf` commands `hacf -cmdtocf` and `hacf -cftocmd` truncates the path of the `types.cf` file and updates the `main.cf` file with the truncated path.

Lock by third-party monitoring tools on shared volumes

Some third-party monitoring tools (such as Compaq Insight Manager) hold an exclusive lock or have an open file handle on the shared volumes they monitor. This lock may prevent VCS from offlining a service group that includes the volume as a resource. VCS requires a lock on resource in a service group when taking the group offline.

Workaround: Symantec recommends adding a custom resource as the topmost parent for an affected service group. Use the custom resource to manage onlining, monitoring, and offlining of the third-party monitoring tool.

Undefined behavior when using VCS wizards for modifying incorrectly configured service groups

If you use the VCS wizards to modify service groups that are incorrectly configured through the VCS Cluster Manager (Java Console), the wizards fail to modify the service groups. This may also result in undefined behaviors in the wizards.(253007)

MirrorView agent resource faults when agent is killed

If all of the parent resources of the MirrorView Agent are offline when the MirrorView Agent is killed, or has crashed, then the resource will fault once the MirrorView Agent has automatically restarted. This behavior only occurs if all of

the parent resources of the MirrorView agent are offline before the MirrorView Agent being killed, or crashing. (508066)

Cluster address for global cluster requires resolved virtual IP

The virtual IP address must have a DNS entry if virtual IP is used for heartbeat agents.

Systems in a cluster must have same system locale setting

VCS does not support clustering of systems with different system locales. All systems in a cluster must be set to the same locale.

Virtual fire drill not supported in Windows environments

The virtual fire drill feature available from the VCS command line and the Cluster Manager (Java console) is not supported in Windows environments.

Cluster Manager consoles do not update GlobalCounter

To avoid updating Cluster Manager views with unnecessary frequency, the Java and Web Console do not increment the GlobalCounter attribute of the cluster.

Symantec Product Authentication Service does not support node renaming

Symantec Product Authentication Service (earlier known as Veritas Security Services) does not support renaming nodes.

WAN cards are not supported

The VCS Configuration Wizard (VCW) does not proceed with network card discovery if it detects a WAN card.

Known issues

This section lists the known issues that are applicable in this release of the product.

For the latest information on updates, patches, and software issues regarding this release, see the following TechNote:

http://www.symantec.com/docs/TECH59755

Issues relating to installing, upgrading and licensing

This section provides information on the issues you may face during the product installation, upgrade or during managing the licenses.

The installation may fail with "The system cannot find the file specified" error

This issue occurs if the vxinstaller service is in a failed state during the product installation. (2560071)

Workaround: Delete the vxinstaller service and then run the installation wizard again.

Installation may fail with "Unspecified error" on a remote system

The product installation wizard may fail to install VCS on a remote system with "Unspecified error".

This issue occurs if the vxInstaller service does not start on the remote node to begin the installation. (2429526)

Workaround: Run the installation locally on the system where the installation has failed.

Installation may fail with a fatal error for VCS msi

The product installation wizard may fail to install VCS with a fatal error for installing the VCS msi. This error occurs on the Installation panel of the product installation wizard.

During the installation the product installer accesses the user profile folder and the SID path for the logged on user. While logging in to the system, if the user profile does not load properly or if the logged on user profile is corrupt, the product installer fails to perform the required installation task. This causes the installation to fail with a fatal error. (2515584)

Workaround: Reboot the system and run the installation again. If the problem persists, contact your system administrator.

Delayed installation on certain systems

You may experience a slower installation on certain systems.

This issue occurs, if you have configured any software restriction policies on the system. During the installation the restriction policies increases the package verification time and thus the over all installation time is increased. (2516062)

VCS uninstallation halts and displays an error message; uninstall continues after clearing the message

During VCS for Windows uninstallation, the installer halts while uninstalling the Symantec Service Management Framework component and displays the following error message:

```
Shell error: not found
```

Uninstallation continues after clearing the error message.

Installation may fail with the "Windows Installer Service could not be accessed" error

This issue occurs if the Windows Installer Service is not accessible during the installation. Since the service is not accessible, the installer fails to proceed with the installation. (2497344)

Workaround: The Windows Installer Service is a native component of an operating system. Typically, the Installer Service inaccessible issue occurs, if the service is damaged or unregistered and thus repairing the operating system installation serves as a workaround.

For more details on the workaround, refer to the following Microsoft knowledge base articles.

http://support.microsoft.com/kb/315353

http://support.microsoft.com/kb/315346

Uninstallation may fail to remove certain folders

After a successful uninstallation, the product installer may fail to remove the following folders:

- VERITAS Object Bus
- Veritas Shared
- Veritas Volume Manager

These folders contain application logs. The reinstallation of the product will not be affected if these folders are not deleted. (2591541, 2654871)

Workaround: You can safely delete these folders manually.

VMware virtual environment specific issues

This section provides information on the known issues specific to the VMware virtual environment. Review these details if you plan to configure application monitoring in a VMware virtual environment.

Storage agent issues and limitations

The following limitations and configuration issues apply for non-shared storage configured using NativeDisks, VMNSDg, and VMwareDisks agents in a VMware virtual environment:

- In case the VMwareDisks agent resource is configured manually, care should be taken not to add the operating system disk in the configuration. The VMwareDisks agent does not block this operation. This might lead to a system crash during failover. (2843813)
- Non-shared disks partitioned using GUID Partition Table (GPT) are not supported. Currently only Master Boot Record (MBR) partition is supported. (2861160)
- VMwareDisks agent does not support disks attached to the virtual machine using IDE controllers. The agent resource reports an unknown if IDE type of disks are configured. (2844255)
- Application may fail to start or report an unknown state if VMware vMotion and application failover is triggered simultaneously.
  If VMware vMotion is triggered for the failover target system at the same time as the application is failed over or switched over to the same failover target system, the application successfully stops on the current system, but may fail to start on the target system or report an unknown state. (2861106, 2874316)
  This issue occurs because as a part of the switch over operation the data disk are successfully detached from the current virtual machine but they cannot be attached to the failover target system since the VMware vMotion is in progress for the target system.
  The application agent tries to start the application on the target system for the configured number of attempts. During this operation the application may report an unknown state and eventually start if the time taken for the VMware vMotion to complete does not exceed the time taken for restarting the application for the configured number of attempts. However, if the time taken for VMware vMotion exceeds the application online retry limit, then the application fails to start on the target system.
  Workaround: Ensure that you do not switch the application to a system for which the VMware vMotion is in progress. However, if you happen to do so and the application fails to start on the target system, you must manually start

the application, using the “Start Application” operation from the Symantec High Availability tab.

- VMware snapshot operations may fail if VMwareDisks agent is configured for a physical RDM type of disk. Currently only virtual RDM disks are supported. (2856068)

  This is a limitation from VMware.

- In case VMware HA is disabled and the ESX itself faults. VCS moves the service group to the target failover system on another ESX host. VMwareDisks agent registers the faulted virtual machine on the new ESX host. When you try to power on the faulted system, you may see the following message in the vSphere Client:

  ```
  This virtual machine might have been moved or copied. In order to configure certain management and networking features, VMware ESX needs to know if this virtual machine was moved or copied. If you don't know, answer "I copied it".
  ```

  You must select “I moved it” (instead of the default “I copied it”) on this message prompt. (2853873)

- The VMwareDisks agent updates its attributes, saves the configuration, and makes it read-only during the monitor cycle in the following scenarios:

  - Successfully performing Storage vMotion.
  - Not specifying UUID in the DiskPaths attribute of the resource.

  Before performing the following tasks, discard any changes to the configuration that you do not wish to retain:

  - Performing Storage vMotion.
  - Adding, enabling, or probing a resource that does not have a UUID specified in its DiskPaths attribute. (2865463)

Wizard, Dashboard, and Symantec High Availability tab specific issues

Symantec ApplicationHA tab and the Symantec ApplicationHA Dashboard fails to display the application status

Symantec ApplicationHA tab and the Symantec ApplicationHA Dashboard may fail to display the application status. (2988071)

After applying a Microsoft security advisory patch on the systems, you may experience that the Symantec ApplicationHA tab and the Symantec ApplicationHA Dashboard fails to display the application status.

This issue occurs due to the difference in the key length of the authentication certificate issued by ApplicationHA Console Server and the key length desired by Microsoft Windows.

Older browsers accepted the 512 bits certificate. However, the newer browsers now require a certificate of minimum 1024 bits.

Workaround:

Close the vSphere Client and perform the following steps on the Symantec High Availability Console Server:

1. Navigate to the following path:

   ```
   C:\Program Files\Veritas\ApplicationHA\tomcat\conf
   ```

2. Using a text editor tool, open the server.xml file and search for the string "KeystorePass".

   The “KeystorePass” represents the Keystore Password.

3. Note down the password mentioned.

4. Using the command prompt navigate to the following path:

   ```
   C:\Program Files\Veritas\ApplicationHA\JRE\bin
   ```

5. Copy the password that you had noted down in step 3.

6. Execute the keytool.exe and provide the following argument:

   ```
   -genkey -alias tomcat -keyalg RSA -validity 3650
   -keypass password -keystore .keystore -storepass <password>
   -dname "CN=Symantec ApplicationHA Console, O=Symantec, L=MountainView,
   S=CA, C=US" -keysize 2048
   ```

7. Navigate to the following location:

   ```
   C:\Program Files\Veritas\ApplicationHA\JRE\bin
   ```

8. Copy the ".keystore" file.

9. From services.msc stop the Symantec ApplicationHA Service.

10. Navigate to the following path, take a back up of the existing “.keystore” and replace the ".keystore" file with the one copied in step 8.

    ```
    C:\Program Files\Veritas\ApplicationHA\Tomcat\cert
    ```

Note: Do not rename the ".keystore" when you save the backup copy. You must save it using the same name.

---

11 Start the Symantec ApplicationHA Service.

12 Re-launch the vSphere Client.

Error while unconfiguring the VCS cluster from the Symantec High Availability tab

This issue may occur if you try to unconfigure the VCS cluster from the Symantec High Availability tab in VMware vSphere Client. (3011461, 3019671)

The unconfiguration task fails with the following error:

```
Failed to stop the HAD service. Node='systemname',
Error=00000425."
```

This issue typically occurs in case of a secure VCS cluster containing a single system.

Workaround: Perform the following steps to resolve this error:

1. Forcefully stop the VCS High Availability Daemon (HAD) process on the system using the following command:

   ```
   taskkill /f /im had.exe
   ```

2. If HAD starts again, stop HAD using the following command:

   ```
   hastop -local
   ```

3. Ensure that the HAD process is in the stopped state.
4. Launch the VCS Cluster Configuration Wizard (VCW) and then delete the cluster using the VCW wizard flow.

Symantec High Availability tab does not provide an option to remove a node from a VCS cluster [2944997]

The **Symantec High Availability** tab does not support removal of a system from a VCS cluster.

Workaround: You can use VCS commands to remove the system from the VCS cluster. You can also unconfigure the entire VCS cluster from the **Symantec High Availability** tab.

SSO configuration fails if the system name contains non-English locale characters

If you install the Symantec High Availability guest components on a system that has non-English locale characters in its name, then the SSO configuration between such a system and the Symantec High Availability Console host fails. (2910613)

Workaround: Ensure that the system name does not contain any non-English locale characters.

The Symantec High Availability Configuration Wizard gives an error for invalid user account details if the system password contains double quotes (")

This issue occurs while configuring application monitoring using the Symantec High Availability Configuration Wizard.

On the Configuration Inputs panel, if the specified the user account password for the selected systems contains double quotes ("), then the wizard fails to proceed. Even though the user account details entered are correct, it displays an invalid user account details error.(2937186)

Workaround: Ensure that the user account password for the systems which you want add to the VCS cluster systems list do not include the double quotes.

The vCenter Server tasks shown in the vSphere Client may fail to display the correct status if the Symantec High Availability Guest Components installation fails

This issue occurs in case of VMware vCenter Server version 5.1.

If you choose to install the Symantec High Availability Guest Components using the vSphere Client menu and if the installation fails, then the vCenter Server task shown in the vSphere Client gets held-up at 10%. It however, does not display that the installation has failed. (2824900)

Workaround:

Refer to the installer logs at the following locations on the Symantec High Availability Console server. Rectify the cause and re-run the wizard.

```
% ALLUSERSPROFILE %\Symantec\ApplicationHA\Logs\ApplicationHA.log

% ALLUSERSPROFILE %\Symantec\ApplicationHA\Logs\VII\
```

You can also refer to logs on the system at the following location:

```
%ALLUSERSPROFILE %\Veritas\
```

Alternatively, choose to install the guest components using the product installer or the CLI. For details refer to the product-specific installation and upgrade guide.

The Symantec High Availability view does not display any sign for the concurrency violation

In a failover type of VCS cluster configuration the application must be online on one cluster system at any point of time. However, if the application is online on more than one cluster system, then the VCS cluster is in a state of concurrency violation.

The Symantec High Availability view shows that the application is online on more than one cluster system. However, it does not indicate the state as a concurrency violation. On the contrary the concurrency violation is indicated using a red icon in the VCS Java GUI, VOM and the CLI output. (2924826)

The Symantec High Availability installer may fail to block the installation of unrelated license keys

This issue occurs when you initiate to manage the licenses from the Symantec High Availability home view, that is available under the Solutions and Applications menu in the vCenter Server.

The Symantec High Availability installer may fail to validate if the entered license key is applicable to the selected product and may proceed to install the key even if it is applicable to a different product.(2924831)

Even though the installer shows that the validation is successful and installs the license key, you may face unknown issues later.

Workaround: Manage the licenses using the Windows Add or Remove Programs.

For more details refer to the product installation and upgrade guide.

The Symantec High Availability Guest Components Installer does not block the installation of ApplicationHA 6.0 over VCS 6.0.2

If you initiate the installation of ApplicationHA 6.0 through the vSphere Client menu on a system where VCS 6.0.2 is installed, then the installer does not block the installation.(2922421)

However, VCS 6.0.2 and ApplicationHA 6.0 are incompatible products. Do not install ApplicationHA 6.0 on the systems where VCS 6.0.2 is installed.

Symantec High Availability Dashboard fails to differentiate the VCS clusters

While configuring application monitoring using the Symantec High Availability wizard, the wizard generates a unique ID for the VCS cluster after verifying its uniqueness in the network. If the network contains multiple clusters, the wizard verifies the generated ID with the IDs assigned to all the accessible clusters. The wizard does not verify the ID with the clusters that are not accessible during the verification. (2908536)

After the cluster configuration is complete, if any of the inaccessible cluster starts running and its cluster ID matches to the one assigned to this new cluster, then the Symantec High Availability Dashboard fails to differentiate the VCS clusters and displays them as a single cluster.

Workaround: Edit the VCS cluster ID or the cluster name. For more details on modifying the cluster ID or name, refer to the *VCS Administrator's Guide*.

Alternatively, you may consider to unconfigure the VCS cluster and then reconfigure it again. However, note that unconfiguring the VCS cluster requires you to unconfigure your application monitoring configuration.

VCS cluster may display “stale admin wait” state if the virtual computer name and the VCS cluster name contains non-English locale characters

This issue occurs after configuring application monitoring using the Symantec High Availability Configuration wizard.(2906207)

While configuring application monitoring using the Symantec High Availability Configuration wizard, if you specify non-English characters for any of the following, the wizard successfully configures the VCS cluster and completes the application monitoring configuration. However, after the configuration workflow is complete the VCS cluster fails to start and displays the “stale admin wait” state, in the Symantec High Availability tab and the Symantec High Availability Dashboard.

- Virtual name, on the Virtual Network Settings panel
- VCS cluster name, on the Edit Cluster Details panel

Workaround: Edit the virtual name or the VCS cluster ID/name. For more details on modifying the virtual name or the cluster ID/name, refer to the *VCS Administrator's Guide*.

Alternatively, you may consider to unconfigure the VCS cluster and then reconfigure it again. However, note that unconfiguring the VCS cluster requires you to unconfigure your application monitoring configuration.

Issues faced while configuring application monitoring for a Windows service having non-English locale characters in its name

While configuring application monitoring for a Generic Service, if the service that you select on the Windows Service Selection panel has non-English locale characters in its name, you may face the following issues: (2906275)

- The wizard fails to display the service name correctly
- The wizard successfully configures the VCS cluster and completes the application monitoring configuration. However, the resources configured for the service display “unknown” state
- During the Add Failover System operation, the wizard fails to validate the system that you want add to the VCS cluster or as a Failover target

Workaround: Using the VCS Java Console, modify the "ServiceName" attribute of the GenericService agent.

By default the attribute value is set to "Service Display Name". You must change this to "Service Key Name".

The Symantec High Availability configuration wizard fails to configure the VCS cluster if UAC is enabled

This issue occurs while configuring application monitoring in VMware virtual environment.

The Symantec High Availability configuration wizard fails to configure the VCS cluster if the selected cluster systems have User Access Control (UAC) enabled and the user has logged on to the systems using a non-default administrator user account. (2867609, 2908548)

Workaround:

Perform the following steps:

1. Exit the wizard and disable UAC on the systems where you want to configure application monitoring.
2. Reboot the systems and run the Symantec High Availability configuration wizard again.

Alternatively, configure the VCS cluster using the Veritas Cluster Server configuration wizard and then use the Symantec High Availability Configuration Wizard to configure application monitoring.

Generic issues

This section provides information on some general known issues found while configuring application monitoring in a VMware virtual environment.

VMwareDisks resource is unable to go offline if the disks configured are thin provisioned (TP) disks

This issue occurs if VMwareDisks agent is configured to monitor thin provisioned (TP) disks and VMware snapshots are taken.

When the service group is taken offline or failed over, the VMwareDisks resource is unable to go offline. The VMwareDisks agent is not able to perform the disk detach operation as the size of the TP snapshot disk is different than the base disk size.

The following message is displayed in the agent log:

VCS ERROR V-16-10061-22523 VMwareDisks:<AppResourceName>-SG-VMwareDisks:offline:Failed to detach disks from VM on ESX <ESXIPaddress> with error 'Invalid configuration for device '0'.' (2801599)

Workaround: There is no workaround for this issue at this time.

VMwareDisks resource fails to go offline after taking snapshot of the VMware virtual machine

This issue occurs if a service group consisting a VMwareDisks resource is configured on a VMware virtual machine, and a snapshot is taken of that virtual machine while the service group is online. (3029081)

If a snapshot is taken of the virtual machine, the VMwareDisks agent is not able to perform the disk detach operation. Hence, the VMWareDisks resource cannot go offline and service group is unable to failover.

The following message is displayed in the agent log:

```
Invalid configuration for device 0

Cannot remove virtual disk from the virtual machine because it or
one of its parent disks is part of a snapshot of the virtual machine.
```

Workaround: Delete the snapshot that was taken with the virtual disks.

Guest virtual machines fail to detect the network connectivity loss

In a VCS cluster that is configured in a VMware environment, if the ESX host loses its network connectivity, the guest virtual machines residing on the ESX host fail to detect the network loss. The configured virtual IP address remain online even though the underlying network has disconnected. (2901327)

In case of a failover, the application successfully starts on a virtual machine that resides on another ESX host and the configured virtual IP address is accessible over the network. However, when you attempt to failback the application to the original virtual machine, the application status shows "online" but the configured virtual IP address is not accessible.

Workaround: Using the VCS Java Console, configure the "PingHostList" attribute for the VCS NIC agent. For more details, refer to the Veritas Cluster Server Bundled Agents Reference Guide.

VMware vMotion fails to move a virtual machine back to an ESX host where the application was online

In a VCS cluster configured using VMware non-shared disk, if a virtual machine (VM1) on which the application is online is moved to another ESX host (for example, ESX 1), then the storage disk also relocates along with VM1. (2896662)

Now, if the application is failed over to a virtual machine (VM2) that resides on an alternate target ESX host (for example, ESX 2), then the storage disk relocates to VM2. The application is now online on VM2. VMware vMotion now fails to move VM2 back to ESX 1, because of the earlier data logs.

Workaround:

Perform the following steps, to resolve this issue:

1. Fail over the application to VM1
2. Move VM2 to ESX1
3. Fail back the application to VM2

VCS commands may fail if the snapshot of a system on which the application is configured is reverted

In a VCS cluster, the cluster configuration and application monitoring configuration details are replicated on all the cluster systems.

When the snapshot of a cluster system is reverted, that system reverts back to an earlier state while the remaining cluster systems retain the current state. Because of this mismatch, the communication between the cluster systems fail and thus the VCS commands used for the cluster operations fail. (2884317)

Workaround: Perform the following steps, using the command line:

1. Stop the VCS cluster using the following command:

```
hastop -all -force
```

2. Run the following commands sequentially on each cluster system:

```
net stop vcscomm

net stop gab

net stop llt
```

3. Restart the VCS cluster using the following command:

```
hastart -all
```

The VCS Cluster Configuration Wizard (VCW) supports NIC teaming but the Symantec High Availability Configuration Wizard does not

The VCS Cluster Configuration Wizard (VCW) supports Windows NIC teaming. However, the Symantec High Availability Configuration Wizard does not support NIC teaming. (3048358)

If you wish to use NIC teaming you must use VCW to configure the VCS cluster and then configure the application using the application configuration wizards or the Symantec High Availability Configuration Wizard.

Note: While using Windows NIC teaming you must select the mode as Static Teaming. Only the Static Teaming mode is currently supported.

NetAppSnapDrive resource may fail with access denied error

You may intermittently observe an issue where the NetAppSnapDrive resource faults with the access denied error. This issue typically occurs in a DR environment, due to the network connectivity issues.

Due to the connectivity issue, the NetAppSnapDrive resource fails to connect to the LUN and retrieve the Data ONTAP version running on the storage system.

You may observe that the issue is resolved during the subsequent probe.(2422479)

Delay in refreshing the VCS Java Console

You may observe a delay in refreshing the VCS Java Console, if the cluster is configured for Single Sign-on authentication.

This issue may occur because the Veritas Enterprise Administrator Service (VxSVC) service may sometime consume 100% of the CPU memory.(2570302)

Several issues while you configure VCS on systems where Symantec Endpoint Protection (SEP) version 12.1 is installed

The following issues may occur while you install and configure VCS on systems where Symantec EndPoint Protection (SEP) version 12.1 is installed. (2439737, 2487369, 2574748, 2530343)

- The VCS Cluster Configuration Wizard (VCW) may fail to connect to the systems while configuring the cluster.
  The following error may be displayed:

  ```
  WMI Connection failed. Error=800706BA
  ```

- If LLT is configured over UDP on an IPv6 network, the status of the VCS High Availability Engine (HAD) on all the remote nodes in the cluster remains in the REMOTE_BUILD state.
- If you set up Disaster Recovery using the Global Cluster Option (GCO) in an IPv6 environment, the status of the remote cluster (cluster at the secondary site) shows as “initing”.

Workaround:

- Ensure that the required ports and services are not blocked by the firewall. Refer to the Installation and Upgrade Guide for list of ports and services used by VCS.
- For the VCW issue, add a custom rule to the SEP firewall policy and define the properties as follows:
  - Rule name: Type **VCS TCP 135** as the name.
  - Action: Select **Allow this traffic**.
  - Protocol: Select **TCP** from the drop-down list.
  - Remote Ports: Type **135** in the field.
- For IPv6 networks, configure the SEP firewall policy to allow IPv6 traffic on the cluster nodes.
  Edit the Firewall Rules table and edit the following settings:
  - **Block IPv6**: Change the Action field value to “Allow”.
  - **Block IPv6 over IPv4 (Teredo)**: Change the Action field value to “Allow”.
  - **Block IPv6 over IPv4 (ISATAP)**: Change the Action field value to “Allow”.
    Refer to the SEP documentation for detailed instructions on how to edit the firewall policy.
- For the LLT over UDP issue on IPv6 network (REMOTE_BUILD issue), perform these steps. Note that the steps require you to stop the Veritas High Availability Engine (HAD).
  - Stop the VCS HAD in the cluster.
    From one of the cluster nodes, type the following on the command prompt:
    `hastop -all -force`
  - Perform the following steps on all the cluster nodes, one node at a time:
    - Stop the LLT service on the cluster node.
      Type the following on the command prompt:
      `net stop llt`
    - Navigate to `%vcs_root%\comms\llt` and open the `llttab.txt` file in a text editor.
      Here, vcs_root typically resolves to `C:\Program Files\Veritas`.
    - Modify all the link entries in the llttab.txt file as follows:
      Change this entry: `link <link#> udp6 - udp6 <udpport#> - <IPv6address> -`
      to this: `link <link#> udp6 - udp6 <udpport#>` **`1380`** `<IPv6address> -`

Note that "1380" is added to the link entry. This defines the MTU (packet size) that LLT uses for its communication.
For example, a sample link entry is as follows: `link Link1 udp6 - udp6 50000 1380 2001:db8:0:11:5c56:6867:e398:6152 -`

- Save and close the llttab.txt file.

- Start the VCS HAD in the cluster.
  From one of the cluster nodes, type the following on the command prompt:
  `hastart -all`

VDS error reported while bringing the NativeDisks and Mount resources online after a failover

This error may occur in a VCS configuration of VMwareDisks, NativeDisks, and Mount resources. (2886291)

While bringing the NativeDisks and Mount resources online after a failover, the following VDS error message may be reported in the Windows Event Viewer:

Unexpected failure. Error code: D@01010004

Workaround: This is an information message and can be safely ignored.

Hyper-V DR attribute settings should be changed in the MonitorVM resource if a monitored VM is migrated to a new volume

In a Hyper-V DR environment, if the storage of a virtual machine is migrated to a new volume, then its configuration path changes. This causes the MonitorVM resource in the VCS configuration to go to the unknown state. Hence the VM is not monitored for disaster recovery.

Workaround: Modify the VMNames attribute in the MonitorVM resource and set it to the new configuration path.

Live migration of a VM, which is part of a VCS cluster where LLT is configured over Ethernet, from one Hyper-V host to another may result in inconsistent HAD state.

Consider the following scenario:

- Two or more Hyper-V hosts are set up, between which live migration can be performed.
- Two or more virtual machines (for example, VM1 and VM2) are configured as nodes of a VCS cluster on one of the hosts.

- In the VCS cluster, LLT is configured over Ethernet.

Perform live migration of one of the virtual machines (say VM1, which may be the active node).

After live migration, the HAD state is reported as follows:

- VM1 shows the HAD state as RUNNING for both the nodes.
- VM2 shows the HAD state as FAULTED for VM1, but RUNNING for VM2.

Events such as the following may be seen in the System Event Viewer for VM1 (one event for each LLT link):

```
LLT ERROR V-14-1-10085 LLT protocol is unbinding from link adapterID
```

This issue does not occur when LLT is configured over UDP. (3053241, 3056450)

Workaround: Perform the following steps to work around this issue:

1. Forcibly stop the VCS High Availability Daemon (HAD) service on the migrated node using the following command:

   ```
   taskkill /f /im had.exe
   ```

2. If the HAD service starts again, stop it using the following command:

   ```
   hastop -local
   ```

3. Verify that the HAD service is in the stopped state.
4. Run the following commands sequentially on the migrated node:

   ```
   net stop vcscomm

   net stop gab

   net stop llt
   ```

5. On the migrated node, restart the VCS cluster using the following command:

   ```
   hastart
   ```

6. Verify that all the cluster nodes report a consistent state for the HAD service using the following command:

   ```
   hasys -state
   ```

Event-viewer error message contents are not displayed for VMwareDisks error messages

Workaround: You can search for the EventID in the VMwareDisks log to get the corresponding error message. (2760545)

'Connection Refused' error while using Remote Cluster Configuration Wizard or Global Group Configuration Wizard from Java console

This error may occur in the following scenarios:

- If you try to delete a remote secure cluster using the Remote Cluster Configuration Wizard from Java console
- If you try to configure a service group as a global service group using the Global Group Cluster Configuration Wizard from Java console

The following error is displayed:

Following clusters had problems while connection:Connection refused.

This error occurs because the VCS Java console requires you to re-enter user credentials, even though it should ideally try the logged-in user first. (2740392, 2859468)

Workaround: Re-enter the user credentials.

VCS engine HAD may not accept client connection requests even after the cluster is configured successfully

This issue may occur after you run the VCS Cluster Configuration Wizard (VCW) to configure a cluster to use single sign-on authentication. Even though VCW indicates that the cluster is configured successfully, the VCS high availability engine (HAD) fails to accept client connection requests. This may happen if VCW fails to configure the VCS authentication service on one or more cluster nodes. (2609395)

You may observe one or more of the following:

- If you try to launch any of the VCS service group configuration wizards, you will see the following error:

```
The VCS engine (HAD) is not running on the cluster nodes.
Failed to get the required cluster information.

The wizard will quit.

Error V-16-13-160
```

- If you run the hasys –display command to check the status of HAD in the cluster, you will see the following error on the command prompt:

```
VCS ERROR V-16-1-53007 Error returned from engine:
HAD on this node not accepting clients.
```

- If you try to connect to the cluster using the Cluster Manager (Java Console), you will see the following error:

```
VCS ERROR V-16-10-106
Could not connect to a live system in the cluster localhost:14141.
Please check the application event log for more details.
Closing all windows.
```

- If you run VCW again to reconfigure the cluster, you will see the following error on the Edit Cluster Options panel:

```
Failed to connect to the cluster.
Error reason: Failed to open socket connection to port 14141 on
host <node_name> (1)
```

Workaround: In the following steps we manually modify the cluster that was configured to use single sign-on authentication to use VCS authentication instead and then reconfigure the cluster using VCS Cluster Configuration Wizard (VCW).

Perform the following steps:

1. Stop the VCS high availability engine (HAD) on all the cluster nodes.

   On each cluster node, type the following on the command prompt:

   ```
   net stop had
   ```

2. Perform the remaining steps on one of the cluster nodes.

   Navigate to `%vcs_home%\conf\config` and locate and delete the **.secure** file from that directory.

   Here, `%vcs_home%` is the installation directory for VCS, typically `C:\Program Files\Veritas\Cluster Server`.

3. From `%vcs_home%\conf\config` directory, locate the configuration file **main.cf** and open it in a text editor.
4. In main.cf, search for the text "**SecureClus=1**" and delete that line altogether.
5. Save the file and close the text editor.

6 Start the VCS engine (HAD) locally on the node where you performed the earlier steps.

Type the following on the command prompt:

```
hastart
```

7 Set the cluster configuration to read/write mode.

Type the following on the command prompt:

```
haconf -makerw
```

8 Add a user to the cluster and assign it with cluster administrator privileges.

Type the following command:

```
hauser -add <username> -priv Administrator
```

9 Enter the password for the user, when prompted.

10 Save and make the cluster configuration read-only.

Type the following on the command prompt:

```
haconf -dump -makero
```

11 Start the VCS high availability engine (HAD) on the remaining cluster nodes.

Type the following on the command prompt:

```
hastart -all
```

Use the cluster user you added in earlier steps to connect to the cluster using Cluster Manager (Java Console). If required, run the VCS Cluster Configuration Wizard (VCW) and reconfigure the cluster to use single sign-on authentication.

SQL Server service resources do not fault even if detail monitoring fails

This issue may occur when detail monitoring is configured for SQL Server 2008 or SQL Server 2012 and IMF is enabled for SQL Server agents.

If detail monitoring fails (either the database becomes unavailable or there is a failure in the detail monitoring script), the SQL service resource faults and VCS may then fail over the service group if the agent's FaultOnDMFailure attribute is set to 1.

It is observed that when IMF is enabled for SQL agents, the SQL service resource does not fault. Instead, the SQL Agent service resource (SQLServerAgent) faults.

This occurs because when detail monitoring fails, the SQL service agent invokes the clean function and as a result the SQL database engine service goes for a restart. As the SQL Agent service depends on the database service, the database service first stops the SQL Agent service as part of its own restart process. IMF instantly detects that the SQL Agent service has stopped and as a result the SQL Agent resource (SQLServerAgent) in the service group faults. As the SQL Agent resource has faulted, VCS initiates a fail over of the service group. The SQL service resource receives this VCS initiated offline and therefore does not fault in response to the original detail monitoring failure event.

This is applicable to SQL Server 2008, SQL Server 2008 R2, and SQL Server 2012. (2535806)

Workaround: There is no known workaround for this issue at this time.

Cluster node may become unresponsive if you try to modify network properties of adapters assigned to the VCS private network

This issue may occur if after configuring the cluster you try to modify the network properties of the adapters assigned to the VCS private network. After you make changes in the adapter properties dialog box and click OK, the properties dialog may hang and in some cases the cluster node itself may become sluggish or unresponsive. (2408878)

Workaround: To resolve this issue, you must either terminate the network properties dialog from Windows Task Manager or restart the VCS LLT service.

Recommendation: If you want to modify the network properties of the adapters assigned to the VCS private network, Symantec recommends that you perform the following steps in the given order.

To modify the private network adapter properties

1. Stop the Veritas High Availability Engine (HAD) on one of the passive nodes. A passive node is a node where are no service groups online.

   Type the following on the command prompt:

   ```
   hastop -local -force
   ```

2. Stop the VCS LLT service on the node.

   Type the following on the command prompt:

   ```
   net stop llt
   ```

3 Modify the network properties of the network adapters on the node, as desired.

4 Start the Veritas High Availability Engine (HAD) on the node.

Type the following on the command prompt:

```
hastart
```

5 Repeat step 1 to step 4 on all the other passive nodes in the cluster.

6 Switch the online service groups from the active node to another node in the cluster. The active node is the node where the service groups are online.

7 Repeat step 1 to step 4 on the active node.

8 If you have assigned a new IP address to any of the network adapters used in the VCS private network, you must reconfigure the private network in the cluster using the VCS Cluster Configuration Wizard (VCW).

This step is required only if you have configured LLT over UDP in the cluster.

Clustered MSMQ resource fails to come online if system is not rebooted after VCS for Windows installation

A clustered MSMQ resource may fail to come online on a Windows Server 2012 node. (3029056)

The MSMQ agent log may contain the following message:

```
resourceName:online:Failed to initialize Services. Error=3
```

Workaround: Reboot the system and try to bring the MSMQ service group online again.

Normally, you are not required to reboot a system after installing VCS for Windows. However, if you plan to make the MSMQ service highly available, you must reboot a Windows Server 2012 system after installing VCS. Make sure that you do so before running the MSMQ Configuration Wizard to create a service group. Otherwise, the clustered MSMQ service fails to initialize, and therefore, the MSMQ resource fails to come online.

MSMQ resource fails to come online if the MSMQ directory path contains double byte characters

The VCS MSMQ resource may fail to come online and may eventually fault if the MSMQ directory path contains Double Byte Character Set (DBCS) characters. (584162, 2121635)

The MSMQ agent log may contain the following message:

V-16-2-13066 Agent is calling clean for resource (MSMQresourcename) because the resource is not up even after online completed.

The Windows Event Viewer may display the following message:

The logger files cannot be initialized (Error: 0x800700003) The file <filename> in the <MSMQdirectory> folder is corrupted or absent. To start the Message Queuing service without losing consistency, you must correct or recover this file.

Workaround: This is a limitation from Microsoft. Do not use DBCS characters in the MSMQ directory paths.

Error while switching global service groups using Veritas Operations Manager (VOM) 3.0

The following issue may occur if you are using Veritas Operations Manager (VOM) 3.0 for administering VCS global service groups configured in secure clusters. (2084898)

If you try to switch global service groups between clusters, the operation fails with the following error:

```
VCS WARNING V-16-1-50824 Command (hagrp -switch <servicegroupname>
<targetsystemname> <targetclustername>) failed. At least Group
Operator privilege required on remote cluster <targetclustername>.
```

Workaround: VOM uses the Veritas Storage Foundation Messaging Service to run VCS commands. This service runs in the Local System account context. Configure this service to run in the Domain Administrator account context and then perform the switch operation.

Change the service account on each of the managed hosts in the clusters.

Perform the following steps on each of the cluster nodes (managed hosts):

1. Open the Windows Services MMC snap-in.
2. Right-click **Veritas Storage Foundation Messaging Service** and then click **Properties**.
3. Click the **Log On** tab and do the following:
   - Click **This account**, click **Browse**, and in the Select User dialog box specify a user account that has Domain Administrator privileges.
   - Click **OK**.
4. Type the account password in the Password and Confirm password fields and then click **OK**.
5. Proceed with the service group operations.

Global group fails to come online on the DR site with a message that it is in the middle of a group operation

When the node that runs a global group faults, VCS internally sets the MigrateQ attribute for the group and attempts to fail over the global group to another node within the local cluster. The MigrateQ attribute stores the node name on which the group was online. If the failover within the cluster does not succeed, then VCS clears the MigrateQ attribute for the groups. However, if the groups have dependencies which are more than one-level deep, then VCS does not clear the MigrateQ attribute for all the groups.(1795151)

This defect causes VCS to misinterpret that the group is in the middle of a failover operation within the local cluster and prevents the group to come online on the DR site. The following message is displayed:

```
VCS Warning V-16-1-51042 Cannot online group global_group.
Group is in the middle of a group operation in cluster
local_cluster.
```

Workaround: Perform the following steps on a node in the local cluster which is in the running state.

To bring the global group online on the DR site

1. Check whether the MigrateQ attribute is set for the global group that you want to bring online on the remote cluster. Type the following on the command prompt:

   ```
   hagrp -display -all -attribute MigrateQ
   ```

   This command displays the name of the faulted node on which the group was online.

2. Flush the global group that you want to bring online on the remote cluster. Type the following on the command prompt:

   ```
   hagrp -flush global_group -sys faulted_node -clus local_cluster
   ```

   where:

   - *global_group* is the group that you want to bring online on the remote cluster.
   - *faulted_node* is the node in the local cluster that hosted the global group and has faulted.
   - *local_cluster* is the cluster at the local site.

The flush operation clears the node name from the MigrateQ attribute.

3 Bring the service group online on the remote cluster.

Type the following on the command prompt:

```
hagrp -online global_group -any -clus remote_cluster
```

VCS cluster configuration fails if Symantec Endpoint Protection 11.0 MR3 version is installed

The VCS Cluster Configuration Wizard (VCW) fails to configure the cluster on systems where Symantec Endpoint Protection (SEP) 11.0 MR3 version is installed.(1455690)

The following error is displayed:

```
Failed to start the cluster. Error=FFFFFFFF. Failed to start
services on all the nodes.
```

The wizard may also fail to ping systems that are selected to be a part of the cluster. VCW uses Internet Control Message Protocol (ICMP) to ping systems and ICMP traffic is blocked in SEP, by default.

Perform the following workaround to resolve this error.

To resolve error message

1 Create a custom rule in SEP to allow ICMP traffic in both directions.

2 Create a custom rule in the SEP firewall rules table. Specify the following details for the rule:

- Rule type: Application
- Application name: llt.sys
- Action: allow

3 Move this rule to the top of the firewall rules table and then apply the firewall policy again.

4 Ensure that the SEP clients on the systems receive this policy and then proceed with the cluster configuration task.

Refer to the SEP documentation for detailed instructions on creating custom firewall rules.

SQL Server Analysis and Agent service resources may go in to an unknown state

The SQL Server Analysis service and SQL Server Agent service resources may go in to an UNKNOWN state when you bring the SQL Server service group online. (1466012)

This issue is applicable to SQL Server 2008 and SQL Server 2012.

The following error is logged on the GenericService agent log:

```
VCS ERROR V-16-10051-6012
GenericService:MSOlap-NEW:online:Failed to wait for the
service 'MSOLAP$NEW' to start. Error = 258
VCS ERROR V-16-10051-6012
GenericService:SQLServerAgent-NEW:online:Failed to wait for
the service 'SQLAgent$NEW' to start. Error = 258
```

Workaround: Probe the resources if they are in the UNKNOWN state.

Symantec Endpoint Protection security policy may block the VCS Cluster Configuration Wizard

While configuring a cluster, the VCS Cluster Configuration Wizard (VCW) may fail to ping systems that are selected to be a part of the cluster. As a result, you cannot configure the cluster. This may happen in case Symantec Endpoint Protection (SEP) client is installed on the selected systems. VCW uses Internet Control Message Protocol (ICMP) to ping systems and ICMP traffic is blocked in SEP, by default.(1315813)

Workaround: Create a custom rule in SEP to allow ICMP traffic in both directions.

Ensure that you create this rule on all the systems that are going to be part of the cluster. Refer to the SEP documentation for instructions.

Saving large configuration results in very large file size for main.cf

If your service groups have a large number resources or resource dependencies, and if the PrintTree attribute is set to 1, saving the configuration may cause the configuration file to become excessively large in size and may affect performance.(616818)

Workaround: Disable printing of resource trees in regenerated configuration files by setting the PrintTree attribute to 0.

AutoStart may violate limits and prerequisites load policy

The load failover policy of Service Group Workload Management may be violated during AutoStart when all of the following conditions are met:

- More than one autostart group uses the same Prerequisites.
- One group, G2, is already online on a node outside of VCS control. The other group, G1, is offline when VCS is started on the node.
- The offline group is probed before the online group is probed.

In this scenario, VCS may choose the node where group G2 is online as the AutoStart node for group G1 even though the Prerequisites load policy for group G1 is not satisfied on that node.

Workaround: Persistently freeze all groups that share the same Prerequisites before using `hastop -force` to stop the cluster or node where any such group is online. This workaround is not required if the cluster or node is stopped without the force option.

Trigger not invoked in REMOTE_BUILD state

In some situations, VCS does not invoke the in jeopardy trigger if the system is a REMOTE_BUILD state. VCS fires the trigger when the system goes to the RUNNING state.

Some alert messages do not display correctly

The following alert messages do not display correctly: (612268)

51030	Unable to find a suitable remote failover target for global group %s. Administrative action is required.
51031	Unable to automatically fail over global group %s remotely because local cluster does not have Authority for the group.
50913	Unable to automatically fail over global group %s remotely because clusters are disconnected and ClusterFailOverPolicy is set to %s. Administrative action is required.
50914	Global group %s is unable to failover within cluster %s and ClusterFailOverPolicy is set to %s. Administrative action is required.
50916	Unable to automatically failover global group %s remotely due to inability to communicate with remote clusters. Please check WAN connection and state of wide area connector.

50761	Unable to automatically fail over global group %s remotely because ClusterList values for the group differ between the clusters. Administrative action is required.
50836	Remote cluster %s has faulted. Administrative action is required.
51032	Parallel global group %s faulted on system %s and is unable to failover within cluster %s. However, group is still online/partial on one or more systems in the cluster
51033	Global group %s is unable to failover within cluster %s and AutoFailOver is %s. Administrative action is required.

NetBackup may fail to back up SQL Server database in VCS cluster environment

In a VCS cluster environment, backup of the SQL database with Symantec NetBackup may fail.

The batch (.bch) file generated by NetBackup for backing up a SQL Server database must contain the following keyword in a VCS cluster environment:

`BROWSECLIENT` *`VirtualServer`*

where *`VirtualServer`* is the SQL Server virtual server name used in the VCS SQL Server service group.

With NetBackup 7.1, the batch file generated for the SQL database has been observed to be missing this keyword, and as a result, the backup fails. (2415667)

Workaround: Manually add the missing `BROWSECLIENT` *`VirtualServer`* keyword to the batch file after it is created.

Issues related to the VCS engine

The following issues relate to the VCS engine.

Engine may hang in LEAVING state

When the command hares -online is issued for a parent resource when a child resource faults, and the `hares -online` command is followed by the command `hastop -local` on the same node, then the engine transitions to the LEAVING state and hangs.

Workaround: Issue the command `hastop -local -force`

Timing issues with AutoStart policy

Consider a case where the service group is offline and engine is not running on node 1. If you restart the engine on node 1 after HAD is killed on node 2 and before the engine is restarted on node 2, then VCS does not initiate the autostart policy of the group.

Issues related to Cluster Manager (Java Console)

The following issues relate the Cluster Manager (Java Console)

Cluster connection error while converting local service group to a global service group

This issue occurs while converting a local service group into a global service group using the Global Group Configuration Wizard from the Cluster Manager (Java Console). While specifying the remote cluster information, if you choose the **Use connected clusters credentials** option for the cluster admin user, the wizard fails to validate the user credentials even if the logged on user is a cluster administrator. (1295394)

The following error is displayed:

```
VCS WARNING V-16-10-73 Following clusters had problems while
connection: Cluster <cluster name>: Connection Refused
```

Workaround: You must select the **Enter new credentials** option and manually specify the cluster administrator credentials.

Repaint feature does not work properly when look and feel preference is set to Java

When a user selects the **Java Look and Feel in the Preferences** dialog box and the look and feel has changed, repainting does not work in that the **Preferences** dialog box does not change as it should and the panel is not clearly visible.(1082952)

Workaround: After selecting the **Java Look and Feel in the Preferences** dialog box, close the Java GUI and then reopen it. You should then be able to select other tabs in the **Preference** dialog box.

Exception when selecting preferences

On Windows systems, selecting the Java (Metal) look and feel of the Java Console may cause a Java exception. (585532)

Workaround: After customizing the look and feel, close restart the Java Console.

Java Console errors in a localized environment

When connected to cluster systems using locales other than English, the Java Console does not allow importing resource types or loading templates from localized directories.

Workaround: Copy the types files or templates to directories with English names and then perform the operation.

Common system names in a global cluster setup

If both local and remote systems have a common system name in a global cluster setup, group operations cannot be performed on those systems using the Java console.

Workaround: Use command-line interface to perform group operations.

Agent logs may not be displayed

If VCS is installed at a different location (at a location other than the default location), the VCS agent logs may not be visible from the Java Console. (643753)

Workaround: Copy the `bmc` and `bmcmap` files to the location specified in Table 1-3:

Table 1-1 bmc and bmcmap file location

Copy from this directory	Copy to this directory
(For English) D:\Program Files\Veritas\messages\en Where, D: is the drive on which VCS is installed.	%VCS_HOME%\messages\en Where, %VCS_HOME% is the default installation directory for VCS, typically C:\Program Files\Veritas\Cluster Server.

Global service groups

The following are global service groups issues.

VCW configures a resource for GCO in a cluster without a valid GCO license

The VCS Configuration Wizard (VCW) enables you to configure a resource for global clustering, even if the cluster does not have a valid license for the Global Cluster Option (GCO). You can successfully bring a GCO resource online, take it offline, or switch it between nodes in a cluster. However, the following message is logged on the engine log if you attempt to connect to a remote cluster:

```
VCS WARNING V-16-3-18000 Global Cluster Option not licensed.
Will not attempt to connect to remote clusters
```

Workaround: Symantec recommends that you do not configure a global cluster resource in a cluster without a valid GCO license.

Group does not go online on AutoStart node

Upon cluster startup, if the last system on which the global group is probed is not part of the group's AutoStartList, then the group will not AutoStart in the cluster. This issue affects only global groups. Local groups do not experience this behavior.

Workaround: Ensure that the last system to join the cluster is a system in the group's AutoStartList.

Cross-cluster switch may cause concurrency violation

If the user tries to switch a global group across clusters while the group is in the process of switching within the local cluster (across systems), then the group will be online on both the local and remote clusters. This issue affects only global groups. Local groups do not experience this behavior.

Workaround: Ensure that the group is not switching locally before attempting to switch the group remotely.

Declare cluster dialog may not display highest priority cluster as failover target

When a global cluster fault occurs, the **Declare Cluster** dialog enables you to fail groups over to the local cluster. However, the local cluster may not be the cluster assigned highest priority in the cluster list.

Workaround: To bring a global group online on a remote cluster, from the Java Console, right-click the global group in the Cluster Explorer tree or **Service Group View**, and use the Remote Online operation to bring the group online on a remote cluster.

Fibre Channel adapters may require modified settings

The following issues apply to VCS with specific Fibre Channel host bus adapters.

Emulex Fibre Channel adapters

For servers configured with Emulex Fibre Channel host bus adapters, you must modify settings of the adapter. The default settings of the adapter do not ensure proper function of SCSI reserve and release.

Workaround: Be sure that the host bus adapter has the proper drivers installed.

Modify the Topology, ResetFF, and ResetTPRLO drive settings in the Emulex adapter BIOS settings, as instructed in the following workaround.

To workaround this issue

1. Locate and run the `Emulex` utility for changing Miniport driver settings.
2. Select **Configuration Settings**.
3. Select **Adapter Settings**.
4. Set the **Topology** parameters to 1, Permanent, and Global.
5. Set the **ResetFF** parameters to 1, Permanent, and Global.
6. Set the **ResetTPRLO** parameters to 1, Permanent, and Global.
7. Save the configuration.
8. Repeat step1 through step 7 for all Emulex adapters in each system.
9. Reboot the systems.

Note: When using EMC storage, you must make additional changes to Emulex host bus adapter settings. See TechNote 245039 on this topic at,

http://entsupport.symantec.com.

QLogic Fibre Channel adapters

When configured over QLogic Fibre Channel host bus adapters, the DiskReservation agent requires the Target Reset option of the adapter to be enabled. By default, this adapter option is disabled, causing the agent to hang during failover.

To workaround this issue

1. During system startup, press ALT+Q to access the QLogic adapter settings menu.
2. Select **Configuration Settings**.
3. Select **Advanced Adapter Settings**.
4. Set the **Enable Target Reset** option to Yes.
5. Save the configuration.
6. Repeat step 1 through step 5 for all QLogic adapters in each system.
7. Reboot the systems.

If VCS upgrade fails on one or more nodes, HAD fails to start and cluster becomes unusable

This issue may happen in cases where you are upgrading a multi-node VCS cluster. If the upgrade succeeds on at least one node but fails on one or more nodes in the cluster, the VCS High Availability Engine (HAD) may fail to start on the nodes on which the upgrade has failed.

The VCS installer does not let you remove VCS from those nodes with an error that those nodes are part of a cluster. The VCS Cluster Configuration Wizard (VCW) does not let you remove those nodes from the cluster with an error that the nodes have a different version of VCS installed.

As a result, you cannot perform any operations on the cluster. (1251272)

Workaround: To get the cluster running, you must manually remove the nodes on which VCS upgrade failed, from the cluster. Then, use the cleanup scripts to remove VCS from the nodes on which the upgrade failed, reinstall VCS, and add the nodes to the cluster.

Perform the following steps to remove the nodes on which the VCS upgrade failed, from the cluster:

To workaround this issue

1. Stop HAD and LLT on all the cluster nodes.

   Type the following on the command prompt:

   ```
   net stop had
   ```

   ```
   net stop llt
   ```

2. On a node on which VCS was upgraded successfully, open the file `llthosts.txt` and delete the entries of all the cluster nodes on which the upgrade failed.

   For example, consider a cluster with three nodes, N1, N2, and N3.

   The `llthosts.txt` file contains the following entries:

   ```
   # This is program generated file, please do not edit.
   0 N1
   1 N2
   2 N3
   ```

   If the upgrade failed on N3, delete the last entry from the file.

   So the modified `llthosts.txt` file should look like this:

   ```
   # This is program generated file, please do not edit.
   0 N1
   1 N2
   ```

   The `llthosts.txt` file is typically located at `C:\Program Files\VERITAS\comms\llt`.

   Here C:\ is the drive on which VCS is installed.

3 On the node on which you performed step 2, open the `gabtab.txt` file and modify the entry to reflect the exact number of nodes in the cluster.

The `gabtab.txt` file contains the following entry:

```
#This is program generated file, please do not edit.
gabconfig -c -n <number of nodes in the cluster>
```

The *<number of nodes in the cluster>* should be the number of nodes on which VCS was upgraded successfully.

Considering the example in step 2 earlier, the `gabtab.txt` file contains the following entry:

```
#This is program generated file, please do not edit.
gabconfig -c -n 3
```

As the upgrade failed on one out of the total three nodes in the cluster, the entry should look like this:

```
#This is program generated file, please do not edit.
gabconfig -c -n 2
```

The `gabtab.txt` file is typically located at `C:\Program Files\VERITAS\comms\gab`.

Here C:\ is the drive on which VCS is installed.

4 From the Windows Services snap-in, change the startup type of the Veritas High Availability Engine (HAD) service to Manual.

5 Repeat step 2, step 3, and step 4 on all the nodes on which VCS was upgraded successfully.

6 On one of the nodes on which VCS was upgraded successfully, open the VCS configuration file main.cf in a text editor and remove the entries of all the cluster nodes on which the VCS upgrade failed.

The `main.cf` file is located at %VCS_Home%\conf\config.

The variable *%VCS_HOME%* is the default installation directory for VCS, typically C:\Program Files\VERITAS\Cluster Server.

7 Start HAD on the node on which you modified the VCS configuration file in step 6 earlier.

Type the following on the command prompt:

```
net start had
```

You can remove VCS from the affected nodes using the cleanup scripts that are provided with the software. These scripts are .bat files located in the \Tools\vpi

directory on the software DVD. Refer to the `readme.txt` file located in the directory for details on how to use the cleanup scripts. After removing VCS, install VCS using the product installer and then add the nodes to the cluster.

Contact Symantec Technical Support for more information.

Custom settings in the cluster configuration are lost after an upgrade if attribute values contain double quote characters

This issue may occur if attribute or argument values of the configured resources in the cluster contain double quote characters (“ “).

If double quotes are used and you upgrade the cluster, all the custom settings made in the cluster configuration are lost. The upgrade itself is successful and the cluster is able to start. But all the customized settings (custom agents, attributes values, arguments and settings) are lost.

Note that these double quotes are not those added by the VCS wizards or Cluster Manager (Java Console). Here’s an example of an agent attribute value:

```
StartProgram @CLUSSYSTEM1 = "\"C:\\ Windows \\ System32 \\
notepad.exe\""
```

The double quotes at the start and end of the entire path are valid. The double quotes included within the starting and ending double quotes cause this issue. (2837356)

Workaround: Symantec recommends that before you upgrade, you take a backup of the cluster configuration files, main.cf and types.cf. The files are located at:

`%vcs_home%\conf\config`.

Here *%vcs_home%* is the default VCS installation directory, typically `C:\Program Files\Veritas\Cluster Server`.

If there are custom settings made in the cluster configuration, then before upgrading the cluster you modify the resource attributes and argument values to remove the double quotes. If you have already upgraded the cluster, then you will have to modify the cluster again to include all the customizations required in the configuration. For the custom settings, you can refer to the cluster configuration files that you backed up before the upgrade.

Options on the Domain Selection panel in the VCS Cluster Configuration Wizard are disabled

While running the VCS Cluster Configuration Wizard (VCW), the options to retrieve a list of systems and users in the domain on the **Domain Selection** panel are

available only for the first time you run the wizard. If you click **Next** and then click **Back** to go back to the panel, all or some of these options appear disabled. (1213943)

Workaround: Exit and launch the wizard again.

Configuration wizards do not allow modifying IPv4 address to IPv6

The VCS Cluster Configuration Wizard (VCW) and the service group configuration wizards do not allow you to modify IPv4 addresses of resources in an existing service group to IPv6. (2405751)

Workaround: You can work around this issue in one of the following ways.

- Use the appropriate wizard to delete the service group and create it again using resources with IPv6 addresses.
- Use either the Java GUI or CLI to replace the IPv4 resources in the service group with corresponding IPv6 resources.