Veritas™ Cluster Server Release Notes

Windows Server 2003

5.1

symantec™

Veritas Cluster Server for NetApp SnapMirror Release Notes

Third-party legal notices

Third-party software may be recommended, distributed, embedded, or bundled with this Symantec product. Such third-party software is licensed separately by its copyright holder. All third-party copyrights associated with this product are listed in the accompanying release notes.

Windows is a registered trademark of Microsoft Corporation.

Licensing and registration

Veritas Cluster Server is a licensed product. See the *Veritas Cluster Server Installation and Upgrade Guide* for license installation instructions.

Technical support

For technical assistance, visit http://www.symantec.com/business/support/index.jsp and select phone or email support. Use the Knowledge Base search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and our customer email notification service.

Contents

Veritas Cluster Server Release Notes

Introduction

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

For general information on regarding Veritas Storage Foundation and High Availability Solutions for Windows, see the following Web site:
http://www.symantec.com

For the latest information on updates, patches, and software issues regarding this release, see the following TechNote:
http://entsupport.symantec.com/docs/303042

This release also supports Veritas Cluster Server Management Console. Release Notes for Veritas Cluster Server Management Console are located on the software discs for that product.

Features and updates

The features and updates described below are introduced in Veritas Cluster Server version 5.1.

Veritas Cluster Server Management Console 5.1 available

The Veritas Cluster Server Management Console 5.1 software disc is included with this release of VCS.

Refer to the VCS Management Console Implementation Guide for installation, upgrade, and configuration instructions.

See the Symantec Support website for information on platform updates and future releases of VCS Management Console.

Client support on Windows Vista

VCS introduces support for client components on Windows Vista, including Vista SP1.

BlackBerry Enterprise Server support

You can configure BlackBerry Enterprise Server 4.1.5 (BES) in a VCS environment using the VCS GenericService agent. In this release, support for BES is limited to the following:

■ BES can be set up in an active-passive configuration only. In an active-passive configuration, the active node hosts the configured BlackBerry server. The second node is a dedicated redundant server able to take over the configured server if the active node fails.

■ BES can be configured only with a SQL database. There is no support for BES with a Microsoft Database Engine (MSDE) database.

See the *Veritas Cluster Server Administrator's Guide* for configuration instructions.

VCW support for configuring VCS LLT over UDP

You can configure LLT over the User Datagram Protocol (UDP) layer while configuring the cluster using the VCS Cluster Configuration Wizard (VCW). VCW provides the necessary configuration options required for using LLT over UDP.

See the *Veritas Cluster Server Administrator's Guide* for more information.

Support for Oracle on 64-bit Windows servers

This release supports Oracle on 64-bit Windows Server operating systems.

Configuration Checker enhancements

The following are Configuration Checker enhancements:

■ Better differentiation between pre-installation and post-installation checks

■ Improved check descriptions and reports

License policy

Each copy of Veritas Cluster Server including all options and agents, whether used on a physical Server or within a virtual machine, must be licensed according to the conditions set forth in the sections below. Each Licensed Software license specifies the number of instances of the Licensed Software you may run on a particular Server at one time.

Table 1-1 lists VCS editions and the additional licensing terms that apply.

Table 1-1   VCS licensing terms

Microsoft Operating System Edition	VCS licensing terms
■ Server Edition ■ Standard Edition ■ Web Edition	A separate license for the licensed software is required for each virtual or physical server, where the software is installed.
■ Advanced Edition ■ Enterprise Edition	For each license, you may run one instance of the licensed software on one physical server and up to four simultaneous instances of the licensed software on virtual servers located on the physical server.
Datacenter Edition	For each license, you may run one instance of the licensed software on one physical server and an unlimited number of virtual servers located on the physical server.

No longer supported

Veritas Cluster Server 5.1 does not support Windows Server 2000

Veritas Cluster Server 5.1 no longer supports Windows Server 2000. Therefore Exchange Server 2000 and Microsoft Operations Manager (MOM) 2000 are also no longer supported.

VCS no longer includes agents and configuration wizards for NetBackup

VCS does not include agents and configuration wizards for NetBackup. Refer to the NetBackup documentation for information on clustering support for NetBackup.

Symantec License Inventory Management (SLIM)

The Symantec License Inventory Management (SLIM) agent is no longer shipped with VCS. The SLIM agent is removed automatically during upgrades from 5.0.

Installation requirements

VCS is supported on Windows-certified network servers containing one or more processors. VCS 5.1 supports clusters of up to 32 nodes.

Supported hardware

Refer to the Hardware Compatibility List on the Symantec Support Web site at http://www.symantec.com/business/support/index.jsp to determine the approved hardware. The compatibility list contains information about supported hardware and is updated regularly. Before installing or upgrading VCS, review the current compatibility list to confirm the compatibility of your hardware and software.

Supported software

The requirements for operating system and application support shown below supersede those requirements listed in the product documentation. For updates on software supported by this product, see http://entsupport.symantec.com/docs/303042

- Veritas Cluster Server (VCS) 5.1 for Windows including the VCS Application Agent for Microsoft Exchange or the VCS Database Agent for Microsoft SQL.

Note: All VCS nodes must run the same Windows operating system and service pack level as well as the same VCS version and service pack level.

- Microsoft Exchange servers and their operating systems:
  - Microsoft Exchange Server 2003 Standard Edition or Enterprise Edition (SP2 supported)
    with
    Windows Server 2003 (Standard Edition, Enterprise Edition, or Datacenter Edition) (SP2 required for all editions)
  - *or*
  - Microsoft Exchange Server 2007 (SP1 supported)
    with
    Windows Server 2003 (64-bit) Standard Edition and Enterprise Edition

Or

- Microsoft SQL servers and their operating systems:
  - Microsoft SQL Server 2000 (32-bit) Standard Edition or Enterprise Edition (all require SP4)

with

Windows Server 2003 (32-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions)

■ Microsoft SQL Server 2000 (64-bit) Standard Edition or Enterprise Edition (all require SP4)

with

Windows Server 2003 (32-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions)

■ Microsoft SQL Server 2005 (32-bit) Standard Edition or Enterprise Edition

with

Windows Server 2003 (32-bit) Standard Edition, Enterprise Edition or Datacenter Edition (SP2 required)

■ Microsoft SQL Server 2005 (64-bit) Standard Edition or Enterprise Edition

with

Windows Server 2003 (32-bit) Standard Edition, Enterprise Edition or Datacenter Edition (SP2 required)

Note: Microsoft SQL Server 2000 and Microsoft SQL Server 2005 can exist in the same cluster but cannot operate on or fail over to the same system. If you use both applications in a cluster, select a distinct set of systems for the SystemList attribute of each application's service group.

■ Network Appliance Data ONTAP 7.2

■ Network Appliance SnapDrive 4.1, 4.2, 5.0

■ Network Appliance SnapManager for SQL 2.0

■ Network Appliance SnapManager for Exchange version 3.1

■ Microsoft iSCSI software initiator version 2.0 or later versions

Hardware requirements

Memory

- Minimum required: 512 MB

- Recommended: 1GB

System processor

- Minimum required: 300 MHz Pentium II

- Recommended: 550 MHz Pentium III or higher

Display resolution

- Minimum resolution: 1024 x 768 pixels or higher

- VCS Cluster Manager (Java Console and Web Console) requires an 8-bit (256 color) display and a graphics card able to render 2D images.

Supported browsers

Veritas Cluster Management Console is supported on the following browsers:

- Microsoft Internet Explorer 6.0 with SP2 or newer

- Firefox 1.5 or newer

Veritas Cluster Management Console requires the Macromedia Flash Plugin v8.0.

Supported client operating systems

The following client operating systems are supported:

- Windows XP Professional (SP 2 or higher required)

- Windows Vista (32-bit) (SP1 supported): Business, Enterprise, and Ultimate editions

- Windows Vista (64-bit) (SP1 supported): Business, Enterprise, and Ultimate editions

VMware ESX server support

VMware ESX 3.0 or higher is required for installing and configuring VCS on VMware virtual machines.

Firewall and anti-spyware considerations

Disable spyware monitoring and removal software before installing this product. You must disable firewalls to enable discovery of the local client. On systems running Windows Server 2003 SP1, you must disable the Windows Firewall or configure it to allow exceptions to the Remote Administration and File and Printer Sharing services.

Software limitations in VCS 5.1

For a complete list of known issues as well as other late-breaking news, see
http://entsupport.symantec.com/docs/303042.

The following limitations apply to VCS version 5.1.

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.

UUID files are always installed to the default installation path

During product installation, you can specify a different installation path than
the default.

However, the installation process installs the UUID files in the following default
path regardless of where the other binaries are installed.

```
C:\Program Files\Veritas\UUID\bin
```

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.

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.

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.

Cluster Manager (Java Console)

Java Console for VCS is required
Cluster Manager (Java Console) from previous VCS versions cannot be used to manage VCS 5.1 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.

Service group dependency 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.

Symantec Product Authentication Service
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.

Incorrect updates to path and name of types.cf
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.

Limitation on SnapManager for Exchange

The Exchange Setup Wizard for VCS supports Network Appliance SnapManager for Microsoft Exchange (SME) with the restriction that MTA data, transaction logs, and registry replication information must be on the same LUN.

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.

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.

Exchange virtual servers are shown as non-reachable in the Exchange Service Manager

In an clustered Exchange 2003 configuration, the following issue is observed:

Exchange virtual servers were displayed as non-reachable in the Exchange Service Manager (ESM) under tools, monitoring, and status, if the Routing Group Master is configured on the Exchange cluster nodes.

Workaround: Symantec recommends that you configure the Routing Group Master on a standalone Exchange Server.

Cannot connect to the other LUNs on the NetApp Filer from the node on which the Exchange service group is online

If an Exchange service group (along with the NetAppFiler and NetAppSnapDrive resources) is online on a node, you will not be able to connect to the other LUNs on the filer using the SnapDrive plugin from the Windows Computer Management console.

You will be able to connect to the other LUNs only if MSExchangeSA and all resources above it are taken offline.

SnapDrive resources fail to offline for a standalone Exchange Server in a VCS environment (797915)

In a standalone Exchange 2003 SP1 cluster configuration, if you take the Exchange service group offline, the NetAppSnapDrive resources fail to go offline.

Workaround: Rename the Microsoft iSCSI Initiator such that the initiator name does not contain any reference to the system name.

Security issue when using Java-GUI and default cluster admin credentials (1188218)

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.

VCWSilent does not support LLT over UDP configuration

VCS provides a silent configuration utility, VCWSilent.exe, that can be used to configure a new cluster. However, the VCWSilent does not support configuring LLT over UDP.

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.

For LLT over UDP, VCW does not support the Low Priority option for a network adapter (1260629)

While configuring LLT over UDP, you cannot set the Low Priority option for a network adapter used for the public network. You can lower the priority of a network adapter only when you are configuring LLT over Ethernet.

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 32-bit (x86), x64, or IA64 Windows operating systems within a cluster.

Schedule backups on online nodes

If you are scheduling backups in a VCS cluster, schedule them on the node on which the service group is online. If the Exchange virtual server fails over to another node, you must set up the backup schedule again on the new node.

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.

Known issues in VCS 5.1

For a complete list of known issues as well as other late-breaking news, see
http://entsupport.symantec.com/docs/303042.

The following issues have been reported for VCS version 5.1.

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

This 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 allow you to remove VCS from those nodes with an error that those nodes are part of a cluster. The VCS Cluster Configuration Wizard (VCW) does not allow you to 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.

Workaround

To get the cluster running, you must manually remove the nodes on which VCS upgrade failed, from the cluster. Then, use the clean up 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:

1   Stop HAD and LLT on all the cluster nodes. Type the following on the command prompt:

    ```
    C:\>net stop had
    C:\>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:

`C:\>`**net start had**

You can remove VCS from the affected nodes using the clean up scripts 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.

Symantec Endpoint Protection security policy may block the VCS Cluster Configuration Wizard (1315813)

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.

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.

Reconfiguring the root broker multiple times may cause issues in a secure cluster (1260632)

If in a secure cluster the root broker is changed multiple times, then the Veritas Cluster Configuration Wizard (VCW) may fail to connect to the cluster with the following error message:

```
Failed to open secure socket connection to port 14141 on host
<hostname>
```

The VCS commands may also fail with the following error:

```
VCS ERROR V-16-1-53006 Unable to connect to VCS engine
securely
```

As a result you may not be able to run VCS commands or modify the cluster using VCW.

Workaround: If root broker changes are required frequently, then Symantec recommends that you configure a root broker that is outside the cluster. The root broker system should not be part of the cluster.

If the root broker is part of the cluster, Symantec recommends that you do not change the root broker after configuring a secure cluster the first time.

Options on the Domain Selection panel in the VCS Cluster Configuration Wizard are disabled (1213943)

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.

Workaround: Exit and launch the wizard again.

Unable to add FileShare or CompositeFileShare resource using the Cluster Management Console (1249373)

You cannot add a FileShare or a CompositeFileShare resource using the Cluster Management Console (CMC). The following error is displayed:

```
-16-1-10584 :Last key is not associated with an element
```

Workaround: Use the Cluster Manager (Java console) or the command line to create the resources.

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

During VCS for NetApp 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.

If the network adapters are unable to ping each other, the cluster nodes may not get GAB membership

While configuring LLT over UDP, if the network adapters selected for the LLT communication are unable to ping each other and you proceed with the cluster configuration, VCW configures the LLT service on the selected network adapters but the cluster nodes may not receive GAB membership and as a result the Veritas High Availability Engine, HAD, may fail to start.

You can confirm the GAB membership by running the following command:

```
C:\gabconfig -a
```

If no port membership information is returned it indicates that GAB is not operating.

This issue can be addressed in either of the following methods:

Method 1:

1   Reboot the cluster nodes that do not have GAB membership.

2   Verify the GAB operation in the cluster. Type the following on the command prompt:

```
C:\gabconfig -a
```

If GAB membership information is displayed for all cluster nodes, GAB is working correctly. However, if the appropriate GAB membership information is not returned for one or more nodes, GAB is not operating correctly. In that case, proceed to the next method.

Method 2:

1   Stop the LLT service in the cluster. Type the following on the command
    prompt:

    `C:\net stop llt`

2   Delete the cluster using VCW.

3   Ensure that the network adapters are able to ping each other and then
    re-create the cluster using VCW.

Saving large configuration results in very large file size for main.cf (616818)

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
cause the configuration file to become excessively large in size and may impact
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, and 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 injeopardy 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 (612268)

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 require
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.

Mount resource fails to bring file share service group online (1266158)

If you are using Windows Logical Disk Manager (LDM) for shared storage, you may encounter problems while bringing service groups online or switching service groups. Create file share service group and try to bring it online. Mount resource fails to bring the file share service group online or switch the service group.

Workaround: Set the attribute AutoFSClean of Mount resource agent to 1. The default value is 0. The agent cleans the file system by running Chkdsk/X on the volume being brought online.

Caution: Cleaning a file system may result in loss of data.

Mount agent may go in unknown state on virtual machines (1262346)

On virtual machines having VCS for Windows installed while configuring the Mount agent, node may go in an unknown state. This happens because the attribute PartitionNo is Global and is seen differently on the shared disks.

Workaround:

1   Take the service group offline.

2   Rescan the disks from all the nodes.

3   To retrieve information about the PartitionNo, type the following at the command prompt:

```
C:\>havol -getdrive -details
```

The information about the disk is retrieved and stored in a text file in the same path from where you executed the command.

4   Edit the attribute PartitionNo from Global to Per System. Assign the value for PartitionNo from the disk details retrieved in the above step.

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 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 below.

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.

Workaround: Enable the Target Reset option in the QLogic adapter BIOS settings as follows.

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.

Issues related 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)

Cluster Manager (Java console) fails to launch if CMC 5.1 is installed (1261117)

If you install the Cluster Management Console 5.1 in a VCS environment, the Cluster Manager (Java GUI) may fail to start.

Cluster connection error while converting local service group to a global service group (1295394)

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 will fail to validate the user credentials even if the logged in user is a cluster administrator. 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.

Exception when selecting preferences (585532)

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.

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.

Repaint feature does not work properly when look and feel preference is set to Java (1082952)

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.

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.

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.

Agent logs may not be displayed (643753)

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. Typically, this may happen with Japanese locales.

Workaround: Copy the bmc and bmcmap files to the location specified in Table 1-2:

Table 1-2   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`.

Table 1-2   bmc and bmcmap file location

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

Issues related to global service groups

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 in 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.

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, do one of the following:

- 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.

- From the Web Console, use the Operations links available on the Service Groups page to bring the global group online on a remote cluster.

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.

Changes to referenced attributes do not propagate

This behavior applies to resources referencing attributes of other resources; that is, the ArgList of one resource (A) passes an attribute of another resource (B). If resource B is deleted from the group, or if the SystemList of the group containing resource B does not contain a system defined in the SystemList of the group containing resource A, the VCS engine does not propagate these changes to the agent monitoring resource A. This may cause resource A to fault because it does not receive the appropriate attribute values from resource B.

In such situations, you must reset the value of resource B in the attribute definition of resource A or restart the agent managing resource A.

ArgListValue attribute may not display updated values

When you modify a resource type that has localizable attributes, the agent log warns that ArgListValues cannot be localized. You can safely ignore the warning message about ArgListValues.

After you modify values for a resource that has localizable attributes, the command
`hares -display` does not display the updated ArgListValues.

Resource fails to online after failover on secondary

During a migrate or failover on the secondary, the NetAppSnapDrive resources fail to come online.
Workaround: Mount the LUNs manually using the SnapDrive GUI or CLI and then probe the resources.

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, and 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.

VCS Simulator installation may require a reboot

While installing the VCS Simulator, the installer may display a message requesting you to reboot the computer to complete the installation. Typically, a reboot is required only in cases where you are re-installing the VCS Simulator.

Issues related to secure clusters

Upgrading a secure cluster may require HAD restart (849401, 1264386)

After upgrading a secure cluster, you may not be able to connect to the Cluster Manager Console (Java GUI) and may observe the following error in the VCS engine log:

```
VCS ERROR V-16-1-50306 Failed to get credentials for VCS
Engine(24582).
```

The following error is displayed if you run any VCS commands from the command line:

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

Workaround:

1 Restart the Veritas High Availability Engine (HAD). Type the following at the command prompt:

```
C:\> net stop had
C:\> net start had
```

2 Verify that HAD is running. Type the following at the command prompt:

`C:\> hasys -state`

The state should display as RUNNING.

New user does not have administrator rights in Java GUI (614323)

In a secure cluster, add a new domain user to the cluster from the command line with Cluster Administrator privileges. Try to login into the Cluster Console (Java GUI) using the newly added user privileges. The new user is logged in as a `guest` instead of an `administrator`.

Workaround: When adding a new user to the cluster, add the user name without the domain extension. For example, if the domain is `vcstest.com` then the user name must be specified as `username@vcstest`.

VCS 5.1 with Microsoft Exchange Server

Mail clients cannot access Exchange front-end/back-end servers configured for RPC over HTTP connections (787278)

Mail clients, such as Microsoft Outlook 2003, configured to use RPC over HTTP may not be able to connect to the Exchange back-end server.

This issue occurs when RPC over HTTP is deployed in an Exchange Server 2003 environment with a front-end/back-end configuration, and the Exchange back-end server is clustered with VCS. The front-end server is Exchange 2003 SP2 and the back-end server is Exchange 2003 SP1.

Workaround : Use Outlook Web Access (OWA) to connect to the Exchange server.

Exchange service group does not fail over after installing ScanMail 8.0 (1054793)

This issue occurs when you try to install ScanMail 8.0 in an Exchange cluster. After installing ScanMail on one node in a cluster, when you switch the service group to another node to install ScanMail, the service group does not come online.

You can complete the ScanMail installation by making changes to the registry keys and bring the Information Store online. But the Exchange services continue to stop intermittently, causing the resources and the service group to fault and fail over.

To make changes in the registry keys

1 Bring the Exchange service group online.

2 Click **Start** and then click **Run**.

3 In the dialog box, enter *regedit* and click **OK**.

4 In the Registry Editor, locate the following subkey in the registry:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSE xchangeIS\VirusScan`

5 In the right pane, double-click **Enabled**.

6 Click **Decimal**, enter **0**, and then click **OK**.

7 On the File menu, click **Exit** to quit Registry Editor.

Error while performing Exchange post-installation steps

After installing Exchange and rebooting the node, the Veritas High Availability Engine (HAD) may fail to start. As a result, while performing the Exchange

post-installation tasks, the Exchange Setup Wizard may either fail to launch or may display the following error message:

```
Failed to get the cluster information. Make sure that VCS
Engine (HAD) is in running state. Start HAD and click Retry
to continue. Click Cancel to exit the wizard.
```

```
Error V-16-13-4207
```

This issue may occur in a secure cluster environment.

Workaround:

1. Restart the Veritas High Availability Engine (HAD). Type the following at the command prompt:

    ```
    C:\> net stop had
    C:\> net start had
    ```

2. Verify that HAD is running. Type the following at the command prompt:

    ```
    C:\> hasys -state
    ```

    The state should display as RUNNING.

3. Click **Retry** on the Exchange Setup Wizard panel and proceed with the Exchange post-installation steps.

Exchange Setup Wizard does not allow a node to be rebuilt and fails during installation (256740)

The Exchange Setup Wizard does not allow a node to be rebuilt, and fails during installation. This is because the wizard stores all the information about the Exchange Virtual servers (EVS) that can failover on a node, in the ExchConfig registry hive. The path in the registry hive is HKLM\SOFTWARE\VERITAS\VCS\EXCHCONFIG. Even if any of the failover nodes die, the corresponding entry still exists in the system list of the EVS. During installation, the Exchange Setup wizard refers to this incorrect registry entry and fails.

Workaround: You will have to manually remove the registry entries of the nodes that are being rebuilt, from the system list of the virtual exchange server on all nodes.

Caution: Incorrectly editing the registry may severely damage your system. Before making changes to the registry, make a backup copy.

---

1. To open the Registry Editor, click **Start > Run**, type **regedit**, and then click **OK**.

2. In the registry tree (on the left), navigate to
    HKLM\SOFTWARE\VERITAS\VCS\ExchConfig

3   From the Exchange Virtual Server keys, delete the keys representing the
     nodes that are being rebuilt.

4   Repeat steps 1 to 3 for the Exchange virtual server on all the nodes in the
     cluster.

5   Exit the Registry Editor.

Metabase update for Exchange may take a longer time

In some failover environments the metabase update for Exchange may take a
longer time. The Exchange agent waits for 10 seconds (default timeout value)
before timing out and faulting the resource.

Workaround: Increase the metabase update timeout value. See Technote 274174
at http://entsupport.symantec.com for more information.

Exchange Setup Wizard messages

During preinstallation steps, the Exchange Setup wizard for VCS renames a
node to the Exchange virtual server name. Installing Microsoft Exchange on the
node then adds the virtual server name to the Exchange Domain Servers group.

During post-installation steps, the setup wizard restores the original name to
the node and removes the Exchange virtual server name from the Exchange
Domain Servers group.

VCS Configuration Wizard may fail to add nodes or reconfigure a cluster with an online Exchange service group (263698)

If an Exchange service group is online in a cluster, the VCS Configuration
Wizard may fail to add a node to the cluster or reconfigure the cluster.
Workaround: Take the Exchange service group offline and run the VCS
configuration Wizard to add the node.

Resource for Exchange Information Store may take time to online

If the Microsoft Exchange database is in an inconsistent state and the enterprise
agent for Exchange attempts to bring the resource for Microsoft Exchange
Information Store (IS) service online, the IS service runs a recovery on the
Exchange database. This recovery may take considerable time, depending on the
number of transaction logs to be replayed.

As a default behavior, the enterprise agent for Exchange waits in the Online
entry point and returns only when the IS resource starts or when the start

operation fails. When IS service is delayed, the enterprise agent for Exchange logs the following message:

```
The Information Store service is not yet started. It
might be running recovery on the database.
```

In some cases, however, the IS service may not be running a recovery.

Workaround: If the IS service is stuck in the STARTING state, you can force the Online entry point to exit without waiting for IS service to start:

1   Open the Registry Editor.

2   From the navigation pane, go to
    \\HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\VCS\
    EXCHCONFIG\PARAMETERS\MSEXCHANGEIS.

3   On the Edit menu, select **New**, and then click **DWORD Value**.

4   Name the value *ForceExit*.

5   Right-click the value and select **Modify**.

6   In the Edit DWORD Value dialog box, specify the value data as '1'. Click **OK**.

When the Online routine detects this value in the registry, it exits without waiting for the IS resource to start.

Note: To restore the default behavior of the agent, set the *ForceExit* value to zero.

Error when reconfiguring cluster or creating the ClusterService group if an Exchange 2003 service group is online (1171088)

If an Exchange 2003 service group is online and you run the VCS Cluster Configuration Wizard (VCW) to reconfigure the cluster or create the ClusterService group, VCW may fail to discover the network adapters on the cluster nodes.

Workaround: Perform the following steps:

1   Take all the ExchService resources in the Exchange 2003 service group offline.

2   From the Services MMC snap-in, restart the WMI service.

3   Run VCW to perform the required tasks.

4   Bring the ExchService resources online.

Exchange Best Practices Analyser health check fails with server name mismatch error (1166985)

If you try to use the Exchange Server 2007 Best Practices Analyzer to run a Health Check on a clustered Mailbox server, the test fails with a server name mismatch error, as in the following example:

```
Server name mismatch Server: EVS1
There is a discrepancy with the Exchange server name EVS1 between
the registry and Active Directory. The computer may have been
renamed or third-party clustering software may be running. Host name
in registry: CNODE1.
```

You can ignore this error and proceed with the analysis.

Other issues

Resources in a parent service group may fail to come online if the AutoStart attribute for the resources is set to 0 (1363503)

This issue occurs with service groups in a parent-child relationship linked with online local firm dependency and when the AutoStart attribute for all the resources of the parent service group is set to 0 (false). The AutoStart attribute of the parent service group is set to 1 (true).

If you take the parent service group resources offline and then switch or fail over the child service group to another node in the cluster, the child service group comes online on the node but the parent service group resources do not come online on that node.

The following error is displayed in the parent service group's resource logs:

```
VCS WARNING V-16-1-10285 Cannot online: resource's group is frozen
waiting for dependency to be satisfied
```

Workaround

In such a scenario, while taking the parent service group resources offline, use the following command for the last resource:

```
hagrp –offline service_group -sys system_name -clus
cluster_name
```

Here, *service_group* is the name of the parent service group.

You can also take the resource offline using the Cluster Manager (Java Console). This ensures that the parent service group resources come online on the node on which the child service group is switched or failed over.

VCS wizards may fail to probe resources (1318552)

While creating resources and service groups using VCS wizards, if you choose to bring the resources or service groups online, the wizards may fail to probe the resources.

The following error is displayed:

```
Failed to online <resourcename> on system <nodename> Resource
has not been probed on system <nodename>
```

Workaround

In such cases, complete the wizards and then probe the resource manually from the Cluster Manager (Java console) and then bring it online.

Print Share wizard may fail to discover the PrintSpool resource if NetBIOS over TCP/IP is disabled (1248877)

If NetBIOS over TCP/IP is disabled for the network adapter, the Print Share wizard may fail to discover the PrintSpool resource in a service group. As a result, you cannot add network printers to the virtual computer.

Workaround: Enable NetBIOS over TCP/IP and then add printers to the virtual computer.

Windows Safe Mode boot options not supported (1234512)

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

Service group offline alerts remain unresolved on a MOM 2005 server (1217601)

In a VCS cluster with a MOM 2005 monitoring environment, the VCS state monitoring script logs service group offline alerts. These alerts are logged only if the service group is offline on the cluster node that has highest priority in the SystemList attribute of that service group. However, if the service group is brought online on the node again, the offline alerts logged earlier do not get resolved.

You must manually resolve the service group offline alerts on the MOM 2005 server.

Software fixes and enhancements

Concurrency violation with online firm dependencies

The concurrency violation trigger could not offline a service group if the group had a parent online on the system with local firm dependency. The concurrency violation continued until the parent was manually taken offline.

Table 1-3 describes the other fixed issues and software enhancements and are referenced by the Veritas incident number.

Table 1-3 Fixed issues

Incident Number	Description
506454	VCW configures the cluster with both upper and lower case of the same system name.
864671	A user in a user group does not receive Cluster Administrator rights.
837702	The Fire Drill Wizard does not delete the DCO log volume when deleting a fire drill configuration.
703925	Resync action for MirrorView agent does not resynchronize mirrors in a fractured or consistent state.
894979	Cannot use the same NIC resource to configure Notifier and Web Console using VCW.
493266	Lanman resources fail to come online if multiple Lanman resources depend on the same IP resource.
582351	Error Bringing Mount Points Online After Power-Off
425035	Use a Valid Script File for Detail Monitoring
603211	DNS Scavenging Affects Virtual Servers Configured in VCS
582837	On a Japanese locales, Selection panel of the VCW wizard displays distorted system selection panes
	Concurrency violation with online firm dependencies
765323	AddArrayUser action for the MirrorView agent fails on x64 systems.

Documentation changes

See http://entsupport.symantec.com/docs/303042 for a complete list of changes to the product documentation as well as other late-breaking news.

This section lists the documentation errata in the information provided in the product documentation.

Veritas Cluster Server Installation and Upgrade Guide

The following information about "Installing Sun's Java Access Bridge" should appear on page 28 preceding the section "Configuring Veritas Cluster Server".

Installing Sun's Java Access Bridge

JAWS (Job Access for Windows and Speech) is a screen reader program that allows visually impaired users to gain access to information on their computers. In order to use JAWS with the Java GUI, you need to install Sun Microsystem's Java Access Bridge. This provides access to all Java applications.

To install Java Access Bridge

1   Open a Web browser and go to the Java Access Bridge download page at http://java.sun.com/javase/technologies/accessibility/accessbridge/index.jsp.

2   Click the link **Download Java Access Bridge,** and then select the Access Bridge executable. There is also a manual download option but automatic installation is preferable.

3   Run the installer to install the required dll and jar files in the java installations of the system.

4   Restart your system.

5   Run JAWS and the Java GUI.

Veritas Cluster Server Administrator's Guide

In chapter 22 "Troubleshooting and recovery for VCS", refer to the section Setting the checksum option on page 691.

Replace the 3rd bullet with the following:

2 - checksum calculated for header and message. When set to 2, LLT also checksums the whole data buffer submitted by the client to be verified by the peer before delivering it to peer-client. In case the checksum verification fails on the receiver, LLT drops that packet, causing the sender to retransmit it. A

message containing the number of bad checksum packets sent is logged in the event log.

Documentation

Documentation is included on the Symantec software discs in Adobe Portable Document Format (PDF) in the directory `Docs\Cluster_Server`. To view a document, explore the CD and double-click the file name.

- `VCS_AgentDev.pdf`, *VCS Agent Developer's Guide*

- `VCS_GettingStarted.pdf`, *VCS Getting Started Guide*

- `VCS_Admin.pdf`, *VCS Administrator's Guide*

- `VCS_BundledAgents.pdf`, *VCS Bundled Agents Reference Guide*

- `VCS_NetApp-Exch.pdf`, *Veritas Cluster Server Implementation Guide for Microsoft Exchange*

- `VCS_NetApp-Exch2007.pdf`, *Veritas Cluster Server Implementation Guide for Microsoft Exchange 2007*

- `VCS_NetApp-SQL.pdf`, *Veritas Cluster Server Implementation Guide for Microsoft SQL*

- `VCS_NetApp-Oracle.pdf`, *Veritas Cluster Server Implementation Guide for Oracle*

Release notes for this product bundle are on the Symantec product disc. Copy the release notes from the disc to the directory `C:\Program Files\Veritas\Docs\ENU\VCS` if you want them available on your system for reference.

- `VCS_ReleaseNotes.pdf`, *Veritas Cluster Server Release Notes*

Commenting on documents

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions to sfwha_docs@symantec.com. Include the title and part number of the document (located in the lower left corner of the title page), and chapter and section titles of the text on which you are reporting. Our goal is to ensure customer satisfaction by providing effective, quality documentation. For assistance with topics other than documentation, visit http://www.symantec.com/business/support/index.jsp.