Veritas™ Cluster Server Release Notes

Linux

5.0 Maintenance Pack 1

Veritas Cluster Server Release Notes

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
www.symantec.com

Third-party legal notices

Third-party software may be recommended, distributed, embedded, or bundled with this Veritas product. Such third-party software is licensed separately by its copyright holder. All third-party copyrights associated with this product are listed in the Veritas Cluster Server 5.0 Release Notes.

The Veritas Cluster Server 5.0 Release Notes can be viewed at the following URL:
http://support.veritas.com/docs/283850

Licensing and registration

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

Technical support

For technical assistance, visit:
http://www.symantec.com/enterprise/support/assistance_care.jsp.

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.

Veritas Cluster Server Release Notes

Introduction

This document provides important information regarding Veritas Cluster Server (VCS) version 5.0 MP1 for Linux. Please review this entire document before installing VCS.

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

http://entsupport.symantec.com/docs/281993

Changes in this release

This section lists the changes in this release of VCS.

Change in string size for some attribute values

For group name, resource name, attribute name, type name, and VCS username and password, the string size is limited to 1024 characters.

Support dropped for SANVolume agent

This release of VCS does not support the SANVolume agent that was shipped with VCS 5.0.

Campus cluster support

You can configure a campus cluster using functionality provided by Veritas Volume Manager.

To set up a campus cluster, make sure the disk group contains mirrored volumes. The mirrors must be on separate storage at different sites. Use site tags to distinguish between mirrors located at different sites. You could also use enclosure-based naming. See the *Veritas Volume Manager Administrator's Guide* for detailed instructions.

Symantec recommends using I/O fencing in campus clusters.

Change in behavior: hastop command

VCS ignores the value of the cluster-level attribute EngineShutdown while the system is shutting down. [702597]

Change in behavior: BrokerIP attribute of the RemoteGroup agent

The BrokerIP attribute now requires only the IP address. Do not include the port number when you configure the attribute. [789878]

For a secure remote cluster only, if you need the RemoteGroup agent to communicate to a specific authentication broker, then set this attribute.

Type: string-scalar

Example: "128.11.245.51"

Fire drill support in Veritas Cluster Management Console

Veritas Cluster Management Console adds support for fire drills. The console lets you run fire drills and displays the status of the last fire drill.

- Viewing the status of the last fire drill—The service group listing tables display a column for the Physical Fire Drill Status, which indicates the results of the last fire drill.
- Running a fire drill.
  - Verify that replication for an application is working correctly
  - Verify that a secondary disaster recovery (DR) application service group can be brought online successfully.
- Viewing fire drill logs—If a service group is configured with a physical fire drill group, a tab labelled Fire Drill Logs appears on the secondary tab bar in the Group:Summary view. Click this tab to view the VCS log messages about the fire drill group on the remote cluster and the resources that belong to it.

See the *Veritas Cluster Server User's Guide* for information about fire drills.

Viewing the status of the last fire drill

The column Fire Drill Status has been added to service group listing tables. A service group listing table is on the Cluster:Groups view.

For VCS global service groups that are configured with a fire drill group, this column indicates the results of the most recently run fire drill. The following are the possible states:

UNKNOWN	No fire drill has been run or the Cluster Management Console has come online after the most recent fire drill
RUNNING	Fire drill in progress
PASSED	Fire drill group came online on the secondary cluster
FAILED	Fire drill group did not come online on the secondary cluster

If multiple management servers are connected to the global cluster that contains the primary global group, the table does not show fire drill status for that group.

Running a fire drill

The Cluster Management Console supports fire drills in multi-cluster mode only. Before you run a fire drill, you must do the following:

- Configure the local (primary) and remote (secondary) global groups
- Set up the replication for the storage at the primary and secondary sites
- Configure the fire drill group using the FDSETUP command line wizard.

To run a fire drill from the Cluster Management Console

1. On the navigation bar, click **Home**.
2. On the secondary tab bar, click **Clusters**.
3. In the Home:Clusters view, in the Clusters Listing table, click the name of the primary global cluster.
4. On the secondary tab bar, click **Groups**.
5. In the Cluster:Groups view, in the Groups Listing table, click the name of the primary global group.
6. In the Group:Summary view, in the Remote Operations task panel, click **Run fire drill**.
   You can view results of the fire drill in the Cluster:Groups view, the Group:Summary view, and in the Group:Fire Drill Logs view.

Viewing fire drill logs

Running a fire drill creates fire drill logs. If a service group is configured with a fire drill group, a tab labeled Fire Drill Logs appears on the secondary tab bar in the Group:Summary view.

To view fire drill logs

1. On the navigation bar, click **Home**.
2. On the secondary tab bar, click **Clusters**.
3. In the Home:Clusters view, in the Clusters Listing table, click the name of a VCS global cluster.
   The global cluster must contain a global service group (primary group) that is configured with a fire drill group at a secondary location.
4. On the secondary tab bar, click **Groups**.

5 In the Cluster:Groups view, in the Groups Listing table, click the name of the primary global group.

6 In the Group:Summary view, on the secondary tab bar, click **Fire Drill Logs**. This tab contains VCS log messages about the fire drill group on the remote (secondary) cluster and the resources that belong to it.

Features introduced in VCS 5.0

See the *Veritas Cluster Server User's Guide* for details.

Cluster Management Console

The new Cluster Management Console replaces Cluster Manager (Web Console) and CommandCentral Availability.

Cluster Management Console enables administration and analysis for VCS clusters in your enterprise from a single console. You can install Cluster Management Console on a stand-alone system to manage multiple clusters or you can install the console on cluster nodes to manage a local cluster. When installed to manage a local cluster, the console is configured as part of the ClusterService group and the AppName attribute is set to `cmc`.

Cluster Monitor is now called Cluster Connector

CommandCentral Availability installed a component called Cluster Monitor on cluster nodes. The updated component is called Cluster Connector.

VCS privileges for operating system user groups

VCS 5.0 lets you assign VCS privileges to native users at an operating system (OS) user group level in secure clusters.

Assigning a VCS role to a user group assigns the same VCS privileges to all members of the user group, unless you specifically exclude individual users from those privileges.

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

Five levels of service group dependencies

VCS now supports configuring up to five levels of service group dependencies. The exception is the online local hard dependency, for which only two levels are supported.

New RemoteGroup agent to monitor service groups in remote clusters

The new RemoteGroup agent monitors and manages service groups in a remote cluster. See the *Veritas Cluster Server Bundled Agents Reference Guide* for more information about the agent.

Enhancements to the hastop command

You can customize the behavior of the hastop command by configuring the new EngineShutdown attribute for the cluster.

EngineShutdown Value	Description
Enable	Process all hastop commands. This is the default behavior.
Disable	Reject all hastop commands.
DisableClusStop	Do not process the hastop -all command; process all other hastop commands.
PromptClusStop	Prompt for user confirmation before running the hastop -all command; process all other hastop commands.
PromptLocal	Prompt for user confirmation before running the hastop -local command; reject all other hastop commands.
PromptAlways	Prompt for user confirmation before running any hastop command.

Simulator supports deleting simulated clusters

VCS Simulator now supports deleting simulated clusters.

Symantec recommends using the same tool (command line or Java Console) to create and delete a cluster. For example, if you created the cluster from the Java Console, delete the cluster from the Java Console.

Fencing updates: DMP support

Dynamic multi-pathing (DMP) allows coordinator disks to take advantage of the path failover and the dynamic adding and removal capabilities of DMP. You can configure coordinator disks to use Veritas Volume Manager DMP feature.

You can set the coordinator disks to use either raw or DMP as the hardware path to a drive. See the *Veritas Cluster Server Installation Guide* for more information.

Minimal downtime upgrade to VCS 5.0

See the *Veritas Cluster Server Installation Guide* for a strategy on upgrading to VCS 5.0 while ensuring a minimal downtime for your applications.

Backup of VCS configuration files

VCS backs up all configuration files (<config>.cf) including main.cf and types.cf to <config>.cf.autobackup. The configuration is backed up only if the BackupInterval is set and the configuration is writable.

When you save a configuration, VCS saves the running configuration to the actual configuration file (i.e. <config>.cf) and removes all autobackup files. This does away with the VCS behavior of creating .stale files

If you do not configure the BackupInterval attribute, VCS does not save the running configuration automatically.

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

Support for security services

VCS 5.0 uses the Symantec Product Authentication Service to provide secure communication between cluster nodes and clients, including the Java and the Web consoles. VCS uses digital certificates for authentication and uses SSL to encrypt communication over the public network.

Separate logger thread for HAD

The VCS engine, HAD, runs as a high-priority process to send heartbeats to kernel components and to respond quickly to failures. In VCS 5.0, HAD runs logging activities in a separate thread to reduce the performance impact on the engine due to logging.

Enhanced NFS lock failover

The new NFSRestart agent provides high availability to NFS locks. Use the agent in conjunction with the NFS agent. See the *Veritas Cluster Server Bundled Agents Reference Guide* for more information.

Support for VLAN interfaces

NIC and MultiNICA agents now support VLAN interfaces. The agents do not configure the NICs, but can monitor them.

See the OS vendor's documentation on how to configure VLAN on your host, and ensure that the switch or router connected to such an interface is compatible with your configuration. Both server-side and switch-side VLAN configurations are supported.

Virtual fire drill

VCS supports a virtual fire drill capability that lets you test whether a resource can fail over to another node in the cluster. Virtual fire drills detect discrepancies between the VCS configuration and the underlying infrastructure on a node; discrepancies that might prevent a service group from going online on a specific node. See the *Veritas Cluster Server User's Guide* for more information on running virtual fire drills.

New term: Daemon Down Node Alive (DDNA)

Daemon Down Node Alive (DDNA) is a condition in which the VCS high availability daemon (HAD) on a node fails, but the node is running. When HAD fails, the hashadow process tries to bring HAD up again. If the hashadow process succeeds in bringing HAD up, the system leaves the DDNA membership and joins the regular membership. See the *Veritas Cluster Server User's Guide* for more information.

Change in behavior: Use comma or semicolon as delimiter

VCS 5.0 does not support using spaces as delimiters to separate vector, association, or keylist values. You must use a comma or a semicolon as a delimiter.

Change in behavior: New format for engine version

The new EngineVersion attribute replaces the MajorVersion and MinorVersion attributes. VCS stores version information in the following format:
`<major>.<minor>.<maintenance_patch_num>.<point_patch_num>`

Change in behavior for the resfault trigger

VCS now provides finer control over the resfault trigger. The resfault trigger is now invoked if the TriggerResFault attribute is set to 1.

Change in behavior: New location for enterprise agents

VCS enterprise agents are now installed in the /opt/VRTSagents/ha/bin directory.

The <agent>Types.cf files are now located at /etc/VRTSagents/ha/conf/<agent>.

Change in behavior: New location of message catalogs and attribute pools

VCS stores binary message catalogs (BMCs) at the following location:

/opt/VRTS/messages/*language*/module_name

The variable *language* represents a two-letter abbreviation.

The attribute pools also move from /var to /opt.

Change in behavior: New option for the hastart and had commands

Use the -v option to retrieve concise information about the VCS version. Use the -version option to get verbose information.

Changes to bundled agents

VCS introduces the following new agents:

- NFSRestart—Provides high availability for NFS record locks.
- RemoteGroup—Monitors and manages a service group on another system.
- SANVolume—Monitors volumes in a SAN environment managed using Storage Foundation Volume Server.
- Apache (now bundled on all platforms)—Provides high availability to an Apache Web server.

See "No longer supported" on page 25.

Changes to licensing for VCS

VCS now follows the licensing scheme that is described below:

License	What's included
VCS	■ VCS ■ Cluster Management Console ■ Database agents ■ Application agents ■ Virtual fire drill support
VCS HA/DR	■ VCS ■ Cluster Management Console ■ Database agents ■ Application agents ■ Replication agents ■ Global clustering ■ Fire drill support

Note: Database agents are included on the VCS 5.0 disc. The replication and application agents are available via the Veritas Cluster Agent Pack.

New attributes

VCS 5.0 introduces the following new attributes. See the *Veritas Cluster Server User's Guide* for more information.

Resource type attributes

- AgentFile—Complete name and path of the binary for an agent. Use when the agent binaries are not installed at their default locations.
- AgentDirectory—Complete path of the directory in which the agent binary and scripts are located. Use when the agent binaries are not installed at their default locations.

Cluster attributes

- EngineShutdown—Provides finer control over the hastop command.
- BackupInterval—Time period in minutes after which VCS backs up configuration files.
- OperatorGroups—List of operating system user account groups that have Operator privileges on the cluster.
- AdministratorGroups—List of operating system user account groups that have administrative privileges on the cluster.
- Guests—List of users that have Guest privileges on the cluster.

System attributes

- EngineVersion—Specifies the major, minor, maintenance-patch, and point-patch version of VCS.

Service group attributes

- TriggerResFault—Defines whether VCS invokes the resfault trigger when a resource faults.
- AdministratorGroups—List of operating system user account groups that have administrative privileges on the service group.
- OperatorGroups—List of operating system user account groups that have Operator privileges on the service group.
- Guests—List of users that have Guest privileges on the service group.

Removed attributes

- DiskHbStatus—Deprecated. This release does not support disk heartbeats. Symantec recommends using I/O fencing.
- MajorVersion—The EngineVersion attribute provides information about the VCS version.
- MinorVersion—The EngineVersion attribute provides information about the VCS version.

Updates to the DB2 agent

The Veritas High Availability Agent for DB2 introduces the following changes:

- The attributes StartUpOpt and ShutDownOpt provide new start up and shut down options. Using the StartUpOpt attribute, you can start the instance or partition, activate database commands after processes start, or create customized start up sequences. Using the ShutDownOpt attribute, you can perform a normal stop or customize your shut down sequence.
- In previous releases when you enabled in-depth monitoring (IndepthMonitor=1), it executed a default SQL query. The in-depth monitor now allows you to classify actions for DB2 errors according to their severity. You can associate predefined actions with each error code with a monitoring script that you can customize. You can find a sample of in-depth monitoring script in the following directory: /etc/VRTSagents/ha/conf/Db2udb/sample_db2udb.
  You must install the custom script in the /opt/VRTSagents/ha/bin/Db2udb directory to enable indepth monitoring.
- You can enable the AgentDebug attribute to get more debugging information from the agent and the database.

Updates to the Sybase agent

The Veritas High Availability Agent for Sybase agent supports Sybase ASE 12.5.x and 15 on AIX, HP-UX, Linux, and Solaris.

Updates to the Oracle agent

- New monitoring option—The basic monitoring option of the Oracle agent now allows health check monitoring in addition to the process check monitoring. You can choose the health check monitoring option for Oracle 10g and later.
- Support for virtual fire drills—VCS requires you to keep the configurations in sync with the underlying infrastructure on a cluster node. Virtual fire drills detect such discrepancies that prevent a service group from going online on a specific system. Refer to the *Veritas Cluster Server User's Guide* for more information.
  The agent uses the Action entry point to support the virtual fire drill functionality.

Veritas agents

VCS bundles agents to manage key resources used in the cluster. The implementation and configuration of bundled agents vary by platform.

See the *Veritas Cluster Server Bundled Agent Reference Guide*.

VCS also provides agents for the management of key enterprise applications. This section lists the agents for enterprise applications and the software the agents support.

In addition to the agents for enterprise applications provided with VCS, other agents are available through an independent Symantec offering called the Veritas Cluster Server Agent Pack. The agent pack includes the currently shipping agents and is re-released regularly to add new agents that are now under development. Contact your Symantec sales representative for information about agents included in the agent pack, agents under development, and agents available through Symantec consulting services.

Note: Before configuring an enterprise agent with VCS, verify that you have a supported version of the agent.

Veritas agents support a specified application version on Linux if the application vendor supports that version on Linux.

Agent	Agent version	VCS version			Application		OS	
		4.0	4.1	5.0			RHEL 4.0	SLES 9
DB2	5.0	p	p	s	DB2 Enterprise Server Edition	8.1, 8.2, 9.1	s	s
Oracle	5.0	p	p	s	Oracle	9*i*, 10g R1, 10g R2	s	s
Sybase	5.0	p	p	s	Sybase Adaptive Server Enterprise	12.5.x, 15	s	s

s – supported configuration p – supported by previous version of the agent

System requirements

System requirements for VCS are as follows.

Supported hardware

The compatibility list contains information about supported hardware and is updated regularly. For the latest information on supported hardware visit the following URL:

http://support.veritas.com/docs/283161

Before installing or upgrading Veritas Cluster Server, review the current compatibility list to confirm the compatibility of your hardware and software.

Supported software for VCS cluster nodes

VCS operates on the following architectures and operating systems. Symantec supports only those kernel binaries distributed by Red Hat and SUSE.

Operating System	Kernel	Architecture
Red Hat Enterprise Linux 4 (RHEL 4) Update 3	2.6.9-34.EL 2.6.9-34.smp 2.6.9-34.hugemem	x86 (32-bit) Intel Xeon (32-bit, 64-bit) AMD Opteron (32-bit, 64-bit)
SUSE Linux Enterprise Server 9 (SLES 9) with SP3	2.6.5-7.244 2.6.5-7.244-smp 2.6.5-7.244-bigsmp	x86 (32-bit) Intel Xeon (32-bit, 64-bit) AMD Opteron (32-bit, 64-bit)

- ext2, ext3, reiserfs, NFS, and bind on LVM2, Veritas Volume Manager (VxVM) 4.1 and 5.0, and raw disks
- Veritas Volume Manager (VxVM) 4.1 with Veritas File System (VxFS) 4.1
- Veritas Volume Manager (VxVM) 5.0 with Veritas File System (VxFS) 5.0

Supported Linux operating system updates

Symantec products will operate on subsequent kernel and patch releases provided the operating systems maintain kernel ABI (application binary interface) compatibility.

Information about the latest supported Red Hat erratas and updates and SUSE service packs is available in the following TechNote. Read this TechNote *before* installing any Veritas product.

http://entsupport.symantec.com/docs/281993

Supported software for Cluster Management Console

You can install Cluster Management Console on a standalone system to manage multiple clusters or you can install the console on cluster nodes to manage a local cluster.

When you set up a management server to manage multiple clusters, you can connect to the clusters directly or install the cluster connector on cluster nodes to enable connection across firewalls.

Install Mode	Supported software
Multi-cluster mode.To manage multiple clusters. Installed on a standalone system designated the *management server*.	■ Solaris 8, 9, and 10, with patches indicated by Sun. ■ Windows 2000 Server, Advanced Server, and Datacenter, with SP4 or patches as indicated by Microsoft. ■ Windows Server 2003 Standard Edition, Datacenter Edition, Enterprise Edition, and Web Edition, with patches as indicated by Microsoft. **Note:** Windows Management Instrumentation (WMI) must be installed on Windows 2003 systems prior to installing Cluster Management Console.
Single cluster mode. To manage a single cluster. Installed on cluster nodes.	You can install Cluster Management Console in this mode only with VCS 5.0 in a fresh install or upgrade scenario. See “Supported software for VCS cluster nodes” on page 20.

Install Mode	Supported software
Cluster Connector. Installed on cluster nodes to enable a management server to manage a cluster across a firewall	**AIX** ■ VCS versions: 4.0, 4.0 MP1, 4.0 MP2, 4.0 MP3, and 5.0 ■ OS versions: AIX 5.2 ML6 (legacy) or later; AIX 5.3 TL4 with SP 3 **Note:** Cluster connector installs are not supported on clusters running on AIX 5.1 systems. Use direct connection to manage clusters running on AIX 5.1 systems. **HP-UX** ■ VCS versions: 4.1 and 5.0 ■ OS versions: HP-UX 11i v2 **Linux** ■ VCS versions: 4.0, 4.0 MP1, 4.0 MP2, 4.1, 4.1 MP1, 4.1 MP2, and 5.0 ■ OS versions: RHEL 4 Update 3, SLES 9. **Note:** Cluster connector installs are not supported on clusters running on RHEL 3.0 systems. Use direct connection to manage clusters running on RHEL 3.0 systems. **Solaris** ■ VCS versions: 4.0, 4.0 MP1, 4.0 MP2, 4.1, 4.1 MP1, and 5.0 ■ OS versions: Solaris 8, 9, and 10 **Note:** Cluster connector installs are not supported on clusters running on Solaris 7 systems. Use direct connection to manage clusters running on Solaris 7 systems. **Windows** ■ VCS versions: 4.1, 4.2, 4.2 RP1, 4.2 RP2, 4.3, 4.3 MP1 ■ OS versions: Windows 2000 Server, Advanced Server, and Datacenter, with SP4 or patches as indicated by ■ Microsoft Windows Server 2003* Standard Edition, Datacenter Edition, Enterprise Edition, and Web Edition, with patches as indicated by Microsoft * Windows Management Instrumentation (WMI) must be installed on Windows 2003 systems prior to installing Cluster Management Console.

Supported browsers

Veritas Cluster Management Console is supported on the following browsers:

- Microsoft Internet Explorer 6.0 with SP2 or later
- Firefox 1.5 or newer

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

Requirements for accessing Cluster Manager (Java Console)

Cluster Manager (Java Console)

The VCS Java Console requires a minimum of 256MB RAM and 1280x1024 display resolution. The color depth of the monitor must be at least 8-bit (256 colors), although 24-bit is recommended.

The minimum requirements for Windows clients are Pentium II, 300MHz, 256MB RAM, and 800x600 display resolution. (Symantec recommends a minimum of Pentium III, 400MHz, and 512MB RAM.) The color depth of the monitor must be at least 8-bit (256 colors), and the graphics card must be able to render 2D images.

No longer supported

Support is no longer provided for:

- CampusCluster agent
- Apache agent configuration wizard
- The updated Oracle agent does not support Oracle 8.0.x and Oracle 8.1.x.
- The updated DB2 Agent does not support DB2 7.2

Installation notes for VCS 5.0

The following information includes guidelines, tips, and other considerations for installing VCS 5.0.

Before upgrading VCS to version 5.0

If you plan to upgrade VCS with NFS configuration from versions earlier than 5.0, you must perform the following pre-upgrade tasks:

1. Take a backup of the main.cf file.
2. Remove the NFS configuration from the main.cf.
3. Upgrade VCS to 5.0.
4. After you upgrade VCS to 5.0, add the NFS configuration in the main.cf file.

Change default password after installing VCS

When you install and configure VCS, if you do not choose the secure mode, the installvcs program creates a user *admin* with the password *password*. The user has administrative privileges to the cluster.

Symantec recommends you change the password of the user after installing and configuring VCS. See the *Veritas Cluster Server User's Guide* for more information.

Network Console and crash dump facility (Netdump)

Symantec recommends installing and configuring the Netdump facility on all Red Hat and SUSE installations. The facility is not specifically for Symantec products, but we recommend it as good systems administration practice.

For information on Netdump installations for Red Hat systems, refer to: http://www.redhat.com/support/wpapers/redhat/netdump/

For information on Netdump installations for SUSE systems, refer to: /usr/share/doc/packages/lkcdutils/README.SuSE

If you used the AllowNativeCliUsers attribute

If you used the AllowNativeCliUsers attribute, see the *Veritas Cluster Server Installation Guide* for information on how to use the halogin utility after upgrading to VCS 5.0.

Installation notes for VCS 5.0 MP1

To install VCS 5.0 MP1, you must have a cluster with VCS 5.0 installed and configured on it.

You can perform a minimal-downtime upgrade to minimize the downtime for your system.

Upgrading to VCS 5.0 MP1

To upgrade to VCS 5.0 MP1, you must have a cluster with VCS 5.0 installed and configured on it. See the *Veritas Cluster Server Installation Guide* for detailed instructions on installing VCS.

Note: Symantec recommends backing up your configuration files (types.cf and main.cf) before upgrading VCS.

To upgrade to VCS 5.0 MP1

1. Log in as superuser on one of the systems for installation.
2. Insert the disc containing the VCS 5.0 MP1 software into the disc drive of one of the cluster nodes.
3. Mount the disc on a suitable mount point.
4. Install VCS 5.0 MP1 using the installmp script:

   ```
   ./installmp [-rsh]
   ```

5. After the initial system checks and the requirements checks are complete, press **`Return`** to start upgrading the RPMs.
6. When the installation is complete, note the locations of the summary, log, and response files indicated by the installer.
7. Update the types.cf file to the new version.

   ```
   cp -p /etc/VRTSvcs/conf/config/types.cf \
   /etc/VRTSvcs/conf/config/types.cf.orig
   cp -p /etc/VRTSvcs/conf/types.cf \
   /etc/VRTSvcs/conf/config/types.cf
   ```

8. If you had added custom type definitions in the original types.cf file, you must add them to the new types.cf file.
9. Update the main.cf file to configure resources affected by the upgrade.
   See “Changes in this release” on page 6.
10. Execute the following command to restart your systems:

    ```
    /sbin/shutdown -r now
    ```

Performing a minimal-downtime upgrade to VCS 5.0 MP1

You can perform a minimal-downtime upgrade in the following phases:

- Select a group of one or more cluster nodes as a standby node to upgrade and leave a group of one or more nodes running.
- Upgrade the standby node as follows:
  - Switch over the service group to the nodes that are running.
  - Freeze service group operations and stop VCS on the standby nodes.
  - Install the maintenance patch.
  - Restart the cluster services.
  - Switch back the service group to the upgraded nodes.
- Upgrade the remaining nodes in the second group.

To perform a minimal downtime upgrade

If you do not have the fencing module configured on your cluster, ignore all commands related to fencing in this procedure.

1. Select a node (or a group of nodes) in the cluster as the standby node.
2. Backup llttab, llthosts, gabtab and main.cf files.

```
cp /etc/llttab /etc/llttab.bkp
cp /etc/llthosts /etc/llthosts.bkp
cp /etc/gabtab /etc/gabtab.bkp
cp /etc/VRTSvcs/conf/config/main.cf \
/etc/VRTSvcs/conf/config/main.cf.bkp
cp /etc/VRTSvcs/conf/config/types.cf \
/etc/VRTSvcs/conf/config/types.cf.bkp
```

3. Run the following command to stop VCS.

```
/etc/init.d/vcs stop
```

4. If fencing is configured, stop fencing using following command:

```
/etc/init.d/vxfen stop
```

5. Stop gab.

```
/etc/init.d/gab stop
```

6. Stop llt.

```
/etc/init.d/llt stop
```

7. Install VCS 5.0 MP1 using the installmp script:

```
./installmp [-rsh]
```

8. Update the types.cf file to the new version.

```
cp -p /etc/VRTSvcs/conf/config/types.cf \
/etc/VRTSvcs/conf/config/types.cf.orig
cp -p /etc/VRTSvcs/conf/types.cf \
/etc/VRTSvcs/conf/config/types.cf
```

9 If you had added custom type definitions in the original types.cf file, you must add them to the new types.cf file.

10 After the initial system checks and the requirements checks are complete, press **Return** to start upgrading the RPMs.

11 When the installation is complete, note the locations of the summary, log, and response files indicated by the installer.
Do not start the GAB and LLT processes. Do not start any VCS processes at this time.

12 Restore the copied llttab, llthosts and gabtab files.

```
cp /etc/llttab.bkp   /etc/llttab
cp /etc/llthosts.bkp /etc/llthosts
cp /etc/gabtab.bkp   /etc/gabtab
cp /etc/VRTSvcs/conf/config/main.cf.bkp \
/etc/VRTSvcs/conf/config/main.cf
```

13 Edit the main.cf file to configure new attributes.

14 Change the cluster ID in /etc/llttab file.
Find the line containing "set-cluster" and change the cluster ID following this keyword. Make sure that the new cluster ID is unique within the LAN.

15 Edit the main.cf file to freeze all the groups.
Add the "Frozen = 1" line to all group definitions.

Example:
If original group definition is

```
Group oracle_sg (
    SystemList = { North = 0, South = 1 }
    AutoStartList = { North, South }
```

The new group definition, after adding "Frozen = 1", should be:

```
Group oracle_sg (
    SystemList = { North = 0, South = 1 }
    AutoStartList = { North, South }
    Frozen = 1
```

16 Start all VCS components:

```
/etc/init.d/llt start
/sbin/gabconfig -cx
/etc/init.d/vxfen start
/etc/init.d/vcs start
```

17 Perform the above procedure on each node (or set of nodes), until you reach the last node (or set of nodes) in the cluster.

18 If you are left with the last node or nodes in the cluster, stop VCS components on that node:

```
/opt/VRTSvcs/bin/hastop -local
/etc/init.d/vxfen stop
/etc/init.d/gab stop
/etc/init.d/llt stop
```

19 Unfreeze and bring all services groups online in the new upgraded cluster. On the upgraded node, run the following commands:

- Open the configuration so that changes can be made to it:

  ```
  /opt/VRTSvcs/bin/haconf -makerw
  ```

- For each group in main.cf, run the following commands:

  ```
  /opt/VRTSvcs/bin/hagrp -unfreeze <groupname> -persistent
  /opt/VRTSvcs/bin/hagrp -online <groupname>
  ```

- Finally, save the configuration using the following command:

  ```
  /opt/VRTSvcs/bin/haconf -dump -makero
  ```

20 Upgrade the last node or group of nodes in the cluster.

21 Modify the `/etc/llttab` file and provide the cluster ID for the new cluster.

22 Start all VCS components on the last nodes that were upgraded.

```
/etc/init.d/llt start
gabconfig -cx
/etc/init.d/vxfen start
/etc/init.d/vcs start
```

Upgrading the VCS Java Console

This release includes updates for Cluster Manager (Java Console)

To upgrade the Java Console on a Windows client

1 Stop Cluster Manager if it is running.

2 Remove Cluster Manager from the system.

3 Insert the software disc into a drive on your Windows system.

4 Start the installer from the following path:
\windows\VCSWindowsInstallers\ClusterManager\EN\setup.exe

5 Follow the wizard instructions to complete the installation.

Upgrading the VCS Simulator

This release includes updates for VCS Simulator.

To upgrade VCS Simulator on a Windows client

1. Stop all instances of VCS Simulator.
2. Stop VCS Simulator, if it is running.
3. Remove VCS Simulator from the system.
4. Insert the software disc into a drive on your Windows system.
5. Start the installer from the following path:
   \windows\VCSWindowsInstallers\Simulator \EN\vrtsvcssim.msi
6. Follow the wizard instructions to complete the installation.

Removing VCS 5.0 MP1

You can manually remove VCS 5.0 MP1 from your cluster using the following procedure.

To manually remove VCS 5.0 MP1

1. Backup current configuration files on each cluster node. For example:

   ```
   mkdir -p /var/vcs50mp1-config-save/etc/VRTSvcs/conf/config
   cp -p /etc/lltab /etc/llthosts /etc/gabtab /etc/vxfendg
   /etc/vxfenmode /var/vcs50mp1-config-save/etc/
   cp -p /etc/VRTSvcs/conf/config/main.cf
   /var/vcs50mp1-config-save/etc/VRTSvcs/conf/config/
   ```

   Note that some of the files mentioned in the example may not exist.

2. Stop VCS along with all the resources. Then stop remaining resources manually.

   ```
   /etc/init.d/vcs stop
   ```

3. Stop the VCS command server:

   ```
   killall CmdServer
   ```

4. Uninstall VCS.

   ```
   cd /opt/VRTS/install
   ./uninstallvcs
   ```

5. Install VCS 5.0 using -installonly option.

6. Restore the VCS configuration on each cluster node:

   ```
   cd /var/vcs50mp1-config-save/etc
   cp -p lltab llthosts gabtab vxfendg vxfenmode /etc
   cp -p VRTSvcs/conf/config/main.cf
   etc/VRTSvcs/conf/config/
   ```

7. If vxfen was originally configured in enabled mode, type the following on all the nodes:

   ```
   rm /etc/vxfenmode
   ```

8. Reboot all nodes.

Upgrading the Cluster Management Console management server

To upgrade to 5.0 MP1, you must have a system with 5.0 version of the management server installed. See the *Veritas Cluster Server Installation Guide* for instructions on how to install and upgrade to the 5.0 version of the Cluster Management Console management server.

Upgrading the Cluster Management Console management server for Windows

You can upgrade to 5.0 MP1 from the Veritas Cluster Management Console that was released earlier with Veritas Cluster Server 5.0 for UNIX platforms. You cannot upgrade to 5.0 MP1 from the Veritas Cluster Management Console released with Veritas Storage Foundations and High Availability Solutions for Windows.

Note that in these instructions, the local system is the system that runs the upgrade program.

To upgrade the management server on Windows

1. Insert the software disc into the disc drive on the local system.
2. Using Windows Explorer or your browser, navigate to the \windows\cluster_management_console\Installer directory on the disc.
3. Double-click the setup.bat file to start the installation wizard.
4. In the Welcome panel, read the introduction and then click **Next**.
5. In the Installation and Configuration Options panel, click **Upgrade the management server on the local node** and then click **Next**.
6. In the Summary panel, observe the messages as the wizard gathers the information that it requires to perform the upgrade. When available, click **Next**.
7. In the Upgrading panel, observe the status messages as the wizard performs the upgrade.
   The current action being performed is displayed above a progress bar that indicates completion status. A windows below the progress bar contains a list of the actions that have been performed.
   When available, click **Next**.
8. After a successful upgrade, the Completed panel appears with the following message:
   You have upgraded Cluster Management Console.
   Click **Finish**.

Fixed Issues

Issues fixed in VCS 5.0 MP1

The following issues were fixed in this release. For a list of additional issues fixed in this release, see the following TechNote:
http://entsupport.symantec.com/docs/285869

830848	The hawizard command hangs.
784335	The Oracle agent cannot identify the shell when the /etc/passwd file has multiple occurrence of the $Owner string.
702594	The Oracle agent does export SHLIB_PATH and other environment in CSH.
646372	The hatype -modify ... -delete ...command works incorrectly. The command deletes the first element of the keylist attribute.
627647	The Action entry point for Oracle fails because set_environment() function prototype differs.
627568	The STARTUP_FORCE value needs to be added in the drop-down list of StartUpOpt values in the Oracle and RAC wizards as the default value for StartUpOpt.
625490	For the agent framework module, ag_i18n_inc.sh does not invoke halog when script entry points use the VCSAG_LOGDBG_MSG API, even if the debug tag is enabled.
620529	Cluster Management Console does not display localized logs. If you installed language packs on the management server and on VCS 5.0 cluster nodes, Cluster Management Console did not initially show localized logs.
619770	The IcmpAgent crashes intermittently.
619219	Running the hastart command twice causes an assertion to be displayed.
616964	In a secure environment, the RemoteGroup agent does not authenticate on a remote host for the first time.
616580	Importing resource types fails on Simulator on Windows systems.
609555	The Remote Group Agent wizard in the Java GUI rejects the connection information for the remote cluster with the domain type other than the local cluster. Fix: The RGA Wizard can now connect to all supported domain types irrespective of the domain type of local cluster.

608926	The template file for the DB2 agent does not contain the complete information for building a DB2 MPP configuration. The template does not include a service group required in the configuration.
598476	If you have a service group with the name ClusterService online on the last running node on the cluster, the hasim -stop command appears to hang.
570992	Cluster Management Console does not display some icons properly.
545469	The Monitor entry point does not detect an online when the Oracle instance is not started by the user defined in the Owner attribute.
244988	Very large login name and password takes all the service groups offline. Fix: For group name, resource name, attribute name, type name, and VCS username and password, the string size is limited to 1024 characters.
243186	Assertion in VCS engine.

Issues fixed in VCS 5.0

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.

Web server configuration page offers two locale options

The configuration page for the Symantec Web server (VRTSWeb) offered two Japanese locale options. Both options had UTF-8 encoding, and there were no functional difference between the two.

Oracle agent uses pfile for initialization

The agent for Oracle obtained its initialization parameters from the pfile. VCS could not monitor Oracle instances created from the spfile.

Cluster Manager installation on Windows XP

When installing Cluster Manager on a Windows XP system, the following error appeared: “The installer has insufficient privileges to access this directory: C:\Config.Msi.”

Unmount failed while taking service group offline

A known issue in Red Hat Enterprise Linux 4 could cause unmount to fail. When an NFS client does some heavy I/O, unmounting a resource in the NFS service group may fail while taking the service group offline. Refer to bugzilla id 154387 for more information.

Other fixed issues

The following issues were fixed in this release.

247698	Need to move logging activities out of single-threaded HAD.
248069	Commands do not close socket after successful termination.
620378	Complex group dependencies and timing issues leads to different failovers.
584243	hares options do not filter correctly.
515644	hacf does not handle MAXARG values of vector/associative attributes in the main.cf.

426932	Indeterministic service thread cancellation.
418971	Cannot configure multiple Sybase servers with VCS.
393849	Performance issues with the Mount agent.
271167	Provide finer control over the hastop -all command.
254947	GAB and LLT device files have open permissions.
252347	Behavior of parent group is incorrect when groups are linked with online global firm and child group faults.
246238	Information required when had is restarted either by hashadow or gab.

Known issues

The following issues are open for this version of VCS.

Operational issues for VCS

Partial groups go online after restart

Partial groups go online erroneously if you kill and restart the VCS engine. [821454]

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 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.

Issue with offline local group dependencies

This issue occurs with offline local group dependencies, when the parent service group has the AutoFailover attribute set to 0. When the child group faults, it does not fail over to system where parent is online, even though that is the only system available for failover. [777928]

The hagetcf script reports an error

Running the hagetcf script to gather information about the VCS cluster generates the following error:

```
tar: cannot stat ./var/VRTSvcs/log/.*A.log.  Not dumped.
```

Workaround: This message may be safely ignored.

The hacf -verify command fails if the IP address is specified

The hacf -verify command fails if you specify the IP address instead of the system name. [834496]

Node cannot join cluster because port v is not ready for configuration

This behavior is observed when a node leaves a cluster and another node tries to join the cluster at the same time. If the GAB thread is stuck in another process, the new node cannot join the cluster and GAB logs the following warning:

```
GAB WARNING V-15-1-20126 Port v not ready for reconfiguration, will
retry.
```

The haclus -wait command hangs when cluster name is not specified

If you do not specify the cluster name when running the `haclus -wait` command, the haclus -wait command may hang. [612587]

Using the coordinator attribute

This release contains an attribute for disk groups called coordinator, which configures disks as coordinator disks by the I/O fencing driver. Setting the attribute prevents the coordinator disks from being reassigned to other disk groups. See the Veritas Volume Manager documentation for additional information about the coordinator attribute.

The attribute requires that the disk group contain an odd number of disks. Symantec recommends that you use only three coordinator disks. Using more (five or seven) disks may result in different subclusters.

VCS controlled mount fails, while manual mount of volume succeeds

Security-enhanced Linux must be disabled, because the Security-enhanced (SE) Linux support is provided for evaluation purposes only and the Security policy files are not currently available for the Veritas product stack. Problems such as the mount issue in the subject title can result when Security-enhanced Linux is enabled.

Workaround: To disable SE Linux at boot time on both SLES9 and RHEL4, set the kernel boot parameter selinux to 0 (selinux=0) and reboot the machine. Assuming the system has been configured for booting from the machine machine_name, edit the file /boot/machine_name/menu.lst to include selinux=0 on the kernel line. Then reboot the machine to ensure the setting takes effect.

Network interfaces change their names after reboot

On SUSE systems, network interfaces change their names after reboot even with `HOTPLUG_PCI_QUEUE_NIC_EVENTS=yes` and `MANDATORY_DEVICES="..."` set.

Workaround: Use `PERSISTENT_NAME= eth`*X* where *X* is the interface number for all interfaces.

Problem in RHEL 4 update 1 on 32-bit operating systems

There is a known problem in Red Hat Enterprise Linux 4 Update 1 on 32-bit systems that is unlikely to occur but which may result in a stack overflow. The issue was reported to Red Hat and is documented in Bugzilla incident 162257.

Unloading DiskRes driver requires a reboot on RHEL4

On systems running RHEL4, you must reboot a system after if you are upgrading or replacing the DiskRes driver.

Performance issues with LLT over UDP

Slow performance of LLT over UDP if a link goes down

If LLT is configured over UDP and a link goes down, then you may encounter severe degradation in the performance over the remaining link.

Workaround: On all nodes in the cluster, set the LLT window size to small values. The default value is 400. Setting it to 100 can bring the performance close to normal.

To set window limit add this line in /etc/llttab:

```
set-flow                window:100
```

To change at runtime use `lltconfig`(1m)

```
$ lltconfig -F window:100
```

Slow performance of LLT over UDP on SLES 9

LLT over UDP requires properly assigned IP addresses for the Ethernet interfaces used for the LLT private links. Using `ifconfig` to set up the IP addresses for Ethernet interfaces may not be reliable on SLES 9.
Workaround: The issue is not observed when IP addresses are set using YaST or YaST2.

Note: LLT over UDP might give problems on Red Hat Enterprise Linux. The systems might keep logging warnings, CPU usage might increase and the systems might hang.

Unmount fails while taking service group offline

A known issue in Red Hat Enterprise Linux 4 could cause unmount to fail. When an NFS client does some heavy I/O, unmounting a resource in the NFS service group may fail while taking the service group offline. Refer to bugzilla id 154387 for more information.

Segmentation fault occurs if UTF8 encoding is used

The `halog` command results in a core dump if utf8 encoding is used.

For example, if you issue the command:

```
$VCS_HOME/bin/halog -add "test debug msg" -dbg 1 -sys -msgid
   10000 -encoding utf8 -parameters "test"
```

The following error occurs:

```
Unknown trailer
Segmentation fault (core dumped)
```

Make sure you specify the encoding as utf-8.

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 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.

Issue related to security services with VCS

Security configuration may not work if you use encrypted files

If you choose to configure security using the encrypted file during VCS installation, Authentication Service may not be configured successfully. [621313]

Workaround: To configure the cluster in secure mode using the encrypted files option, do the following:

1 Configure the cluster.

2 Enable security using `installvcs -security` option

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

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 fencing

Preexisting split brain after rebooting nodes

The fencing driver in 5.0 uses Veritas DMP to handle SCSI commands to the disk driver if fencing is configured in *dmp* mode. This allows fencing to use Veritas DMP for access to the coordinator disks. With certain disk arrays, when paths are failed over due to a path failure, the SCSI-3 persistent reservation keys for the previously active paths are not removed. If the nodes in a cluster are all rebooted at the same time, then the cluster will not start due to a "Preexisting split brain" message. [609407]

Workaround: Use the `vxfenclearpre` script to remove the keys from the coordinator disks as well as from the data disks.

Stopping vxfen when the fencing module is being configured

Trying to stop the vxfen driver when the fencing module is being configured results in the following error.

```
VCS FEN vxfenconfig ERROR V-11-2-1013 Unable to unconfigure vxfen
VCS FEN vxfenconfig ERROR V-11-2-1022 Active cluster is currently
fencing.
```

Workaround: This message may be safely ignored.

Fencing configuration fails if fencing module is running on another node

The `vxfenconfig -c` command fails if any of the following commands are running on other nodes in the cluster:

```
vxfenconfig -U
vxfenconfig -c
```

Some vxfenadm options do not work with DMP paths

Some options of the vxfenadm utility do not work well with DMP paths such as /dev/vx/rdmp/sdt3.

Workaround: Use the -a option to register keys instead of -m option for DMP paths.

Issues related to global service groups

Switch across clusters may cause concurrency violation

If you try to switch a global group across clusters while the group is in the process of switching across systems within the local cluster, then the group may go 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.

Using LVM in a GCO environment may cause concurrency violation

Logical Volume Manager (LVM) on Linux operating system is not supported with all replication technologies. Before using LVM with a VCS replication agent, read the documentation for the agent and the late breaking news for the Agent Pack

http://support.veritas.com/docs/282004.

Global service group does not go online on AutoStart node

At cluster startup, if the last system where the global group is probed is not part of the group's AutoStartList, then the group does not AutoStart in the cluster. This issue affects only global groups. Local groups do not display 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.

The gcoconfig command assigns priority 0 to all nodes

If you configure a global cluster using the `/opt/VRTSvcs/bin/gcoconfig` command, the gcoconfig utility assigns the same priority '0' to all the nodes that are in the SystemList of the ClusterService group. [857159]

Workaround: Edit main.cf and assign priority for cluster nodes in the SystemList of the ClusterService group.

Use one of the following approaches to edit the main.cf file:

- Veritas Cluster Server GUI
- VCS commands
- Stop VCS and manually edit the main.cf file
  Note that this approach has HA downtime.

Issues related to VCS bundled agents

Problem in failing over the IP resource

When a system panics, the IP address remains plumbed to the system for a while. In such a case, VCS may not succeed in failing over the IP resource to another system. This can be observed when a system panics during I/O Fencing.

Workaround: Increase the value of the OnlineRetryLimit attribute for the IP resource type.

DiskReservation might fault Mount resources

When the DiskReservation resource is brought online, the agent also does a BLKRRPART ioctl on the disks. This causes the block subsystem to see new block devices. Consequently, the OS launches the block hotplug agent to handle the events. The hotplug agent, as part of its work, unmounts any stale entries.

Because the hotplug agents are asynchronous, it is difficult to find whether all the hotplug agents have finished processing. So, the DiskReservation resource goes ONLINE even while the hotplug agents are running, which is fine with SCSI reservation as the disks are reserved. However, when the DiskReservation resource goes ONLINE, a dependent Mount resource could also come up. And it is possible that the hotplug agent does its unmount *after* the Mount agent does its mount and a monitor cycle. If the Monitor entry point of the Mount resource is called after the unmount, VCS will never see the Mount resource as online. If the Monitor is called before the unmount, the resource goes ONLINE, and then in the next Monitor cycle, goes to FAULTED state.

Workaround: To avoid this, the DiskReservation agent is hard coded so that the Monitor entry point of the DiskReservation resource is called `HOTPLUG_DELAY` seconds after the Online entry point of the DiskReservation resource completes. `HOTPLUG_DELAY` is hard-coded to 5 seconds so that the first monitor happens 5 seconds after the DiskReservation resource is brought online.

If the hotplug agent cannot complete within the default `HOTPLUG_DELAY` time, set the `OnlineRetryLimit` and `RestartLimit` of the Mount type to 1.

NFS Lock recovery is not supported on RHEL4 and SLES9

For more information, refer to the following bugzillas/issues:

- RHEL4: issue 79602
- SLES9: bugzilla 148009

No support for NFSv4 on SLES9

VCS does not support NFS v4 on SLES9.

NFS cannot handle minor number greater than 255

NFS cannot handle minor numbers greater than 255. [143897]

Workaround: Ensure that minor number of the VxVM diskgroup is not greater than 255.

The NFS security feature of RHEL4/SLES9 does not work in a VCS environment.

The NFSSecurity attribute is reserved for future use.

Issues related to the DB2 agent

All partitions fault even if there are errors on only one partition with the IndepthMonitor database

This issue occurs in an MPP environment when multiple partitions use the same database. If the Databasename attribute is changed to an incorrect value, all partitions using the database fault. [568887]

Log message when running DB2 agent

When the Veritas agent for DB2 is run on a VCS system with ja_JP.eucJP locale, VCS logs the message “Failed to open file /opt/VRTSvcs/messages/ja/HAD.bmcmap.” The agent is functioning correctly, and this message can be safely ignored.

between DB2udbAgent and Script50agent files is lost

If you install the VCS 5.0 MP1 DB2 agent using the following command, then the link between Script50agent and DB2udbAgent is removed [832986]:

```
rpm -Uvvh VRTSvcsdb-5.0.10.00-MP1_GENERIC.noarch.rpm
```

Workaround: To retain the link between the files, do one of the following:

- Uninstall the 5.0 agent, and reinstall the 5.0MP1 agent using rpm -i option.
  or
  Use the following command to install the agent:

```
rpm -Uvh --noscripts\
VRTSvcsdb-5.0.10.00-MP1_GENERIC.noarch.rpm
```

Issues related to the Oracle agent

NOFAILOVER action specified for certain Oracle errors

The Veritas High Availability agent for Oracle provides enhanced handling of Oracle errors encountered during detailed monitoring. The agent uses the reference file oraerror.dat, which consists of a list of Oracle errors and the actions to be taken. Refer to the *Veritas High Availability Agent for Oracle Installation and Configuration Guide* for a description of the actions.

Currently, the reference file specifies the NOFAILOVER action when the following Oracle errors are encountered:

ORA-00061, ORA-02726, ORA-6108, ORA-06114

The NOFAILOVER action means that the agent sets the resource's state to OFFLINE and freezes the service group. You may stop the agent, edit the oraerror.dat file, and change the NOFAILOVER action to another action that is appropriate for your environment. The changes go into effect when you restart the agent.

Health check may not work

If you set MonitorOption to 1, health check monitoring may not function when the following message is displayed [589934]:

```
Warning message - Output after executing Oracle Health Check is:
GIM-00105: Shared memory region is corrupted.
```

Workaround: Set MonitorOption to 0 to continue monitoring the resource.

Health check monitoring does not work in csh environment

If you use csh, you must change your shell environment to enable the Health check monitoring option.

Issues related to Cluster Manager (Java Console)

Cluster Manager (Java Console) hangs on Linux

The Cluster Monitor may hang while adding a new cluster panel and may fail to refresh the GUI. [527301]

Workaround: Kill the VCSGui process and restart the Cluster Manager (Java Console).

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. [585532]

Workaround: The workaround is to copy the types files or templates to directories with english names and then perform the operation.

Printing to file from the VCS Java Console throws exception

VCS Java Console and Help throw an exception while printing to a file from a system that does not have a printer configured. Also, the content is not written to the file.

Workaround: Before printing, make sure at least one printer is configured on the system where the VCS Java Console is launched.

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.

Issues related to Cluster Management Console

Warning messages in the log file when running the installmp command

The installmp command logs the following messages. [782798]

```
warning: user vcsbuild does not exist - using root
warning: group fcf does not exist - using root
warning: user vcsbuild does not exist - using root
warning: group fcf does not exist - using root
```

Workaround: None. You may ignore these messages.

Platform attribute in the ClusterConnector.config file is not updated

The Platform attribute in the ClusterConnector.config file remains set to Solaris irrespective of the installation platform. The ClusterConnector.config file is created by the ClusterConnectorConfig agent and is used to set values in resource type definitions and main.cf configurations for the agent. [837685]

The ClusterConnectorVersion attribute might have no value because this value is not used in the current release.

Known issue for the Migrate Site task

The Migrate Site task starts the Migrate Site wizard that enables you to migrate one or more global service groups to one or more remote target clusters. The Cluster Management Console does not migrate a faulted service group. If you attempt to migrate a faulted service group, you may see an entry similar to the following in the management server log:

```
2006-11-20 10:38:33 INFO    Unable to use the -force option when
the cluster that has Authority for the group is not completely
down {vrts.vxcs.mcm.gui.web.actions.wizard.MigrateSiteLastPage
lookupFinish()
```

Workaround: In the Global Application Group Selection panel, select only service groups that are in the online or partial state. Do not select service groups that are in the faulted state.

Erroneous output from gares command

The gares command returns a value for the Start attribute that is different from what the hares command returns. The local values are inverted (exchanged). For example, if gares returns 1, hares returns 0. [853969]

Workaround: This situation can result if the attribute values with local scope are missing for a newly-added system in the system list of a service group. Use the switch command for the CMC_CC service group (for configurations that use the cluster connector) or reconnect to the cluster (for configurations that use direct connection).

Cluster Management Console displays fatal errors

CMC displays fatal errors when it encounters an invalid XML file for an agent. [595973]

Workaround: None. Make sure the XML files for custom agents are valid.

The database fails to back up or restore to a path with Japanese characters

The database fails to back up or restore to the specified path with Japanese characters in it, when the command gadb -backup is run. [767796]

Workaround: Use English folder names when backing up, then copy the database file to the Japanese folder manually, if required.

Cannot uninstall updates on Windows management server

On Windows, uninstalling the VCS 5.0 MP1 management server using Add or Remove Programs removes only the entry from the Add or Remove Programs list. No files are removed. You must perform a management server uninstallation using the original VCS 5.0 uninstallation program. You cannot revert a VCS 5.0 MP1 management server back to a VCS 5.0 management server. [841149]

View displays incorrect version

After upgrading to the Cluster Management Console for VCS 5.0 MP1, the Admin:Management Server view (Admin –> Management Server) shows an incorrect version of 5.0.1136.0 and an incorrect installation history. The correct information is in the About box. [856103]

Console displays logs in English and Japanese

If your management server is configured to run in the Japanese locale, but the managed cluster does not have the Japanese language pack installed, the management server displays a mix of logs in English and Japanese. [778176]

Workaround: Make sure the managed cluster has the Japanese language pack installed.

Default SMTP and SNMP addresses in notification policies for Cluster Management Console

When you configure notification settings, the Edit SMTP Settings task asks you to provide default email or default SNMP console addresses. The policy configuration wizard uses these addresses only to populate the recipient lists during policy configuration. The wizard does not automatically configure policies with these addresses.

When you launch the Notification Policy Configuration wizard, the default email address you specified appears in the Notification Recipients dialog box.

If you add email addresses to this list, the wizard adds them to the policy along with the default address. However, if you delete all the addresses from the Email Recipients list, including the default email address, the wizard configures no email addresses in the policy.

Leave default email addresses in the recipients list to configure them into the policy.

The same behavior applies to specifying default SNMP addresses.

Some Cluster Management Console controls not immediately active

In some versions of Internet Explorer, you many need to click Flash-based screens, popups, and wizards once before the controls become active. Controls that require this activating click show the following message when you roll over them with your mouse pointer [603415]:

```
Press SpaceBar or Click to activate this Control
```

Login screen may not display after inactivity timeout

If your Cluster Management Console is inactive and the session times out, your next action in the console should return you to the login screen. However, if your next action is to request a sort or a new page, the console will not sort the data or load the page.

Workaround: Use the browser refresh feature and the login screen will display.

Very large clusters may not load into Cluster Management Console

Very large clusters may not load into Cluster Management Console. [493844]

Workaround: To accommodate very large clusters, increase the value of the loadClusterQueryTimeout property in the management server configuration file, /opt/VRTScmc/conf/ManagementServer.conf. The management server generates this file upon startup.

1 Stop the Cluster Management Server web console:

```
/opt/VRTSweb/bin/stopApp cmc
```

2 Add the following line to the file /opt/VRTScmc/conf/ManagementServer.conf:

```
loadClusterQueryTimeout=60000
```

Adjust the value as needed to allow complete initial load of your cluster information.

3 Start the Cluster Management Server web console:

```
/opt/VRTSweb/bin/startApp cmc ../VERITAS
```

Log entries in the Management Server:Logs view

The Management Server:Logs view might contain log entries for the management server and for the cluster. [610333]

Management server log entries have the value **`site`** in the Object Type column. Cluster log entries have the value **`cluster`** in the Object Type column.

Cannot install if VxAT 4.3 is installed

If you have installed Symantec Product Authentication Services on a system using the 4.3 client/server installer, install of Cluster Management Console will not succeed because the path to the AT binaries is not in the path. Since this path is not present, the custom action DLL in our MSI will not be able to run certain AT-related commands. [617861]

Workaround: Add the path for the AT binaries before attempting a Cluster Management Console install.

Uninstall of Cluster Connector in a secure cluster leaves the VxSS service group frozen

On UNIX, when you remove the cluster connector from a secure cluster, the VxSS service group is frozen. [619106]

Workaround: Manually unfreeze the VxSS group. Run the following commands.

```
haconf -makerw
hagrp -unfreeze VxSS -persistent
haconf -dump -makero
```

Windows management server uninstall using Add or Remove Programs does not remove folder

After using Add or Remove Programs to remove (uninstall) the Windows management server, an empty Cluster Management Console folder remains:

The default path is C:\Program Files\VERITAS.

Workaround: Delete the empty folder after the uninstall.

Windows cluster monitor uninstall does not remove folder

After a Windows cluster monitor uninstall, an empty folder remains:

The default path is C:\Program Files\VERITAS.

Workaround: Delete the empty folder after the uninstall.

Uninstalling Cluster Connector does not remove entry from Add\Remove Programs on Windows

After you uninstall cluster connector on Windows cluster nodes, the Add or Remove Programs control panel continues to show an entry for cluster connector. This persistent entry prevents any reinstallation of cluster connector. [599424]

Workaround: Remove the Veritas Cluster Management Console entry from the list using Windows Installer Cleanup Utility. Run the utility to remove the entry on each node. If you do not have the utility, you may download it from the Microsoft support site.

Windows install over Terminal Services needs Service Pack 4

Per Microsoft, Windows 2000 without at least Service Pack 4 has problems installing multiple MSI files that alter the same registry key over Terminal Services.

Workaround: If you want to install to a Windows 2000 host using Terminal Services, first ensure that the system has Windows 2000 Service Pack 4 installed.

Removing the *CMC_SERVICES* domain

Uninstalling the management server in multi-cluster environments does not remove the *CMC_SERVICES* domain. [612176]

You can verify the existence of this domain using the following command:

```
vssat showpd --pdrtype ab --domain CMC_SERVICES
```

You must manually remove the CMC_SERVICES domain using the command line. To manually remove all the peripherals in the CMC_SERVICES domain, enter the following command:

```
vssat deleteprpl --pdrtype ab --domain CMC_SERVICES --prplname
principalname
```

Enter the following command to remove the domain:

```
vssat deletepd --pdrtype ab --domain CMC_SERVICES@hostname
```

You can determine the host name using the following command:

```
vssat showpd
```

Issues related to VCS in Japanese locales

The following issues apply to VCS 5.0 in a Japanese locale.

Installer does not create user account and password

The product installer does not ask for a VCS user account and password in a Japanese locale. Only the English installer provides this function.
Workaround: Use the `hauser` command to create VCS user accounts after installation is complete.

The getcomms command does not create diagnostic file

The `getcomms` command does not successfully create a `.tar` diagnostic file in a Japanese locale. [311349]
Workaround: Change the system environment to LANG=C before running the `getcomms` command.

Fire drill wizards do not display Japanese messages

The configuration wizard for Fire Drill (`fdsetup`) cannot display Japanese messages. [298862, 299039]

Some messages and dialogs of VCS Java Console do not display correctly

A small number of messages and dialogs do not display correctly in the VCS Java Console. For example, the Oracle output from SqlTest.pl that is included in the VCS message V-16-20002-211 does not display correctly. [355710, 494575]

Symantec Web Server (VRTSWeb) requires restart after installing language packs

Cluster Management Console does not list Japanese as a language option after installing the language pack. [588560]

Workaround: Restart Symantec Web Server.

Error running CmdServer in Japanese eucjp locale

The command servers displays an unsupported encoding error when you run the Java Console in the Japanese eucjp locale. The error does not appear when you run the console in the Japanese UTF-8 locale. [533291]

Remote system log displays in English in Japanese locale

Log messages in the Java Console from remote systems display in English in the Japanese locale. [859457]

The perform check option in the virtual fire drill wizard does not work in Japanese locale

Running the `perform check` command in the virtual fire drill wizard in the Japanese locale results in the following error message [865446]:

“No fire drill found for type <typename> of resource".

Workaround: Change the locale to English, when you run fire drill wizard with the `perform check` option.

Other known issues

VCS Simulator does not start on Windows systems

On Windows systems, starting VCS Simulator displays an error that the required MSVCR70.DLL is not found on the system. [859388]

Workaround: Run the following command:

```
set PATH=%PATH%;%VCS_SIMULATOR_HOME%\bin;
```

Or append %VCS_SIMULATOR_HOME%\bin; to PATH env variable.

Documentation Errata

This section adds or replaces content in the VCS 5.0 documents.

Veritas Cluster Server User's Guide

User's Guide does not mention backward-compatibility of the Java Console

The VCS User's Guide does not mention the backward-compatibility of Cluster Manager (Java Console.) The console enables or disables features depending on whether the features are supported in the cluster that the console is connected to. For example, the Cluster Shell icon is grayed out when you connect to recent versions of VCS. But the icon is enabled when you connect to a pre-4.1 version of a VCS cluster. [641680]

Updated definition of the IntentOffline attribute

The definition of IntentOnline needs to be updated to include following information:

VCS sets IntentOnline attribute value to 2 for failover groups while VCS attempts to autostart a service group. Once the service group is online, VCS sets IntentOnline value to 1. [831858]

Veritas Cluster Server Centralized Management Guide

This information replaces the information in the Veritas Cluster Server Centralized Management Guide for 5.0. Numbers in parentheses indicate the page number of the Centralized Management Guide where this information appears.

Backing up the database

Backing up the database (page 158) is necessary so that crucial configuration and historical information can be recovered in the event of a failure. You can back up the database using the Cluster Management Console or the CLI. During the backup task, an archived copy of the database file and the associated transaction log file are backed up to a physically separate location. This location can be a tape drive or a disk drive. [703139]

To backup the database to a file

1. In the **Administration: Management Server Database** view, in the **Operations** task panel, click **Backup database to a file**.
2. In the **Enter a valid directory or tape drive on the server** dialog box, enter an existing directory path on the management server.
   If the directory path you specify does not exist, the database backup command does not create it.
3. Click **OK**.

To backup the database to a file using the command line

- `gadb -backup -to` *`archive`*
  This command creates an archive backup file that contains both the database and transaction log. The database archive file is created in the directory path specified by *`archive`*. The database archive file name is of the form:
  `CCAvailDbBackUp@yyyy-mm-dd_hh_mi_ss.1`
  The timestamp portion is in GMT.

Creating custom reports

The section on accessing the database information contains references to $ms_host, which is a variable. Read $ms_host as *ms_host*.

When configuring ODBC, replace *ms_host*. with the name of the management server host. Do not include the $ sign in the host name.

Veritas Cluster Server Bundled Agents Reference Guide

The SANVolume agent documentation has an incorrect sample configuration

Domain is a required attribute, but not included in the sample configuration for SANVolume agent. Using the sample configuration results in an error message. [644932]

Workaround: Use the following sample configuration:

SANVolume agent's sample configuration for Linux

The sample configuration on page 46 is missing the required domain attribute. The updated sample configuration should look like:

```
SANVolume svol (
    SANDiskGroup = vsdg
    SANVolume = vsvol
    VolumeServer = "sysA.veritas.com"
    Domain = "domain1"
    )
```

SANVolume agent's DiskGroup attribute

In the SANVolume agent, for the DiskGroup attribute on page 44 should be changed to SANDiskGroup, and its sample configuration should be changed from "dg1" to "sandg1". [644922]

Veritas Cluster Server Installation Guide

Symantec Product Authentication Service 4.3.x required for cluster connector installation

You must install cluster connector from a system that has Symantec Product Authentication Service 4.3.x, or at least the authentication broker installed.

You can also install cluster connector from a cluster node, provided that you are installing cluster connector on nodes that are part of the same cluster. [611353]

Cluster connector must be taken offline before it is uninstalled

Ensure that you take the CMC service group offline before you uninstall cluster connector. Otherwise, cluster connector remains running even after you uninstall the cluster connector software. [796739]

To take the CMC service group offline on UNIX platforms

1. Obtain a command prompt on the management server host system.
2. Enter the following command:
   ```
   hagrp -offline CMC -sys
   ```
   Replace sys with the name of the system that is running the CMC service group.

Instructions for adding and removing nodes are incorrect

Use the PDF file referenced in this TechNote for updated instructions [626515]:

http://entsupport.symantec.com/docs/281993

Veritas Cluster Agent for DB2 Installation and Configuration Guide

In the Veritas High Availability Agent for DB2 Installation and Configuration Guide, replace all custom file names of custom_monitor_$db2instance _$nodenum, with monitor_custom_$db2instance_$nodenum. [786209]

The section on Disabling in-depth monitoring refers to MonScript when it should refer to IndepthMonitor (786221).

Veritas High Availability Agent for Oracle Installation and Configuration Guide

On page 14, the command documented to invoke the Info entry point is not correct. Use the following command:

```
hares -value resource ResourceInfo [system]\
[-clus cluster | -localclus]
```

On page 18, the description of IGNORE action is missing the following information:

When the Veritas Agent for Oracle encounters an error that does not have a matching error code in the oraerror.dat file, then the agent ignores the error.

Software limitations

The following limitations apply to this release.

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.

System names in VCS

Systems specified in the VCS configuration file, main.cf, and in the files /etc/nodename and /etc/llthosts, must be consistent. The names cannot include periods and thus must not be in the fully qualified form. If you create the file /etc/VRTSvcs/conf/sysname to contain system names used by main.cf, VCS uses the file to verify the names.

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.

No support for NIC names larger than 8 characters (605163)

VCS does not support NIC names that are longer than eight characters.

GAB panics the systems while VCS gets diagnostic data

On receiving a SIGABRT signal from GAB, VCS engine forks off `vcs_diag` script. When VCS engine fails to heartbeat with GAB, often due to heavy load on the system, the `vcs_diag` script does a `sys req` to dump the stack trace of all processes in the system to collect diagnostic information. The dump of stack trace is intended to give useful information for finding out which processes puts heavy load. However, the dumping puts extra load on the system that causes GAB to panic the system in such heavy loads. See *VERITAS Cluster Server User's Guide* for more information.

Workaround: Disable the `vcs_diag` script. To disable, rename the file /opt/VRTSvcs/bin/vcs_diag to /opt/VRTSvcs/bin/vcs_diag.backup.

Using agents in NIS

Programs using networked services (for example, NIS, NFS, RPC, or a TCP socket connection to a remote host) can hang if the host is disconnected from the network. If such a program is used as an agent entry point, a network disconnect can cause the entry point to hang and possibly time out. For example, if the host is configured to use NIS maps as a client, basic commands such as `ps -ef` can hang if there is network disconnect. Symantec recommends creating users locally and configuring /etc/nsswitch.conf to reflect local users.

Fire drill does not support volume sets

The fire drill feature for testing fault readiness of a VCS configuration supports only regular Volume Manager volumes. Volume sets are not supported in this release.

Manually removing VRTSat package erases user credentials

Symantec recommends saving user credentials before manually removing the VRTSat package. If you need the credentials again, you can restore them to their original locations.

To save user credentials

1 Run the `vssat showbackuplist` command. The command displays the data files and backs them up into the SnapShot directory /var/VRTSatSnapShot. Output resembles the following:

```
 vssat showbackuplist
B| /var/VRTSat/.VRTSat/profile/VRTSatlocal.conf
B| /var/VRTSat/.VRTSat/profile/certstore
B| /var/VRTSat/RBAuthSource
B| /var/VRTSat/ABAuthSource
B| /etc/vx/vss/VRTSat.conf
Quiescing ...
Snapshot Directory :/var/VRTSatSnapShot
```

2 Move the credentials to a safe location. Preserving the directory structure makes restoring the files easier.

To restore user credentials

1 Navigate to the SnapShot directory or the safe location where you previously saved credentials:

```
  cd /var/VRTSatSnapShot/profile
```

2 Restore the files:

```
cp ABAuthSource /var/VRTSat/
cp RBAuthSource /var/VRTSat
cp VRTSat.conf /etc/vx/vss
cd /var/VRTSatSnapShot/
cp -r profile /var/VRTSat/.VRTSat
```

Using the KDE desktop

Some menus and dialog boxes on Cluster Manager (Java Console) may appear misaligned or incorrectly sized on a KDE desktop. To ensure the proper appearance and functionality of the console on a KDE desktop, use the Sawfish window manager. You must explicitly select the Sawfish window manager even if it is supposed to appear as the default window manager on a KDE desktop.

NFS locking

Due to RHEL 4 Update 2, update 3, and SLES 9 SP3 issues, lock recovery is not yet supported. Refer to issue 73985 for RHEL issues and bugzilla id 64901 for SLES 9 issues.

System reboot after panic

If the VCS kernel module issues a system panic, a system reboot is required. The supported Linux kernels do not automatically halt (CPU) processing. Set the Linux “panic” kernel parameter to a value other than zero to forcibly reboot the system. Append the following two lines at the end of the /etc/sysctl.conf file:

```
force a reboot after 60 seconds
   kernel.panic = 60
```

Bundled agent limitations

Volume agent clean may forcibly stop volume resources

When the attribute FaultOnMonitorTimeouts calls the Volume agent `clean` entry point after a monitor time-out, the `vxvol -f stop` command is also issued. This command forcibly stops all volumes, even if they are still mounted.

NFS failover

This issue occurs on SLES 9 systems.

If the NFS share is exported to the world (*) and the NFS server fails over, NFS client displays the following error, “Permission denied”.

Workaround: On SLES 9 systems, upgrade nfs-utils to the package version "nfs-utils-1.0.6-103.28".

False concurrency violation when using PidFiles to monitor application resources

The PID files created by an application contain the PIDs for the processes that are monitored by Application agent. These files continue to exist even after a node running the application crashes. On restarting the node, the operating system may assign the PIDs listed in the PID files to other processes running on the node.

Thus, if the Application agent monitors the resource using the PidFiles attribute *only*, the agent may discover the processes running and report a false concurrency violation. This could result in some processes being killed that are not under VCS control.

Networking agents do not support IPv6 protocol

The bundled IP, NIC, IPMultiNIC, and MultiNICA agents for VCS 5.0 do not support the IPv6 enhanced IP protocol.

VCS does not provide a bundled agent for volume sets

VCS 5.0 does not provide a bundled agent to detect Volume Manager volume sets, Problems with volumes and volume sets can only be detected at the DiskGroup and Mount resource levels.
Workaround: Set StartVolumes and StopVolumes attributes of the DiskGroup resource that contains volume set to 1. If a file system is created on the volume set, use a Mount resource to mount the volume set.

Mount agent

The Mount agent mounts a block device at only one mount point on a system. After a block device is mounted, the agent cannot mount another device at the same mount point.

Share agent

To ensure proper monitoring by the Share agent, verify that the /var/lib/nfs/etab file is clear upon system reboot. Clients in the Share agent must be specified as fully qualified host names to ensure seamless failover.

Driver requirements for DiskReservation agent

The DiskReservation agent has a reserver module in the kernel mode that reserves disks persistently. Any driver that works correctly with the `scsiutil` utility shipped with the VRTSvcsdr package is supported. Refer to the manual page for `scsiutil` functionality.

Cluster Management Console limitations

Cluster connector not supported on some OS versions

Cluster Management Console does not support cluster connector on AIX 5.1, Solaris 7, and RHEL 3.0. If your cluster runs on any of these platforms, you must use direct connection to manage the cluster from a management server.

Limited peer management server support

Peer management server support is limited to a configuration of two management servers in an enterprise. An enterprise of three or more management servers is not supported in this release.

Management server cannot coexist with GCM 3.5 Master

The Cluster Management Console management server should not be installed on the same system with a GCM 3.5 Master. These two products will conflict with each other and are not supported running on the same system.

Agent info files needed for Agent Inventory report

By design, the Agent Inventory report requires agent info files that supply the information reported on individual agents. These files are shipped with agents in VCS.

Global clusters must be CMC-managed clusters

All clusters forming a global cluster (using the VCS 4.0 Global Cluster Option) must be managed clusters in order for Veritas Cluster Management Console views to display correct and consistent information. Managed clusters are running the cluster connector or have a direct connection with the management server.

Windows Active Directory installation requires NetBIOS

If you install Cluster Management Console management server in a Windows Active Directory domain, NetBIOS must be turned on. A native (non-NetBIOS) Active Directory environment is not supported in this release.

Remote root broker not supported on Windows

If you set up a management server on a Windows system, you must configure a root broker on the management server system. This release does not support specifying a remote root broker during management server install [841739].

The root broker can be changed after install using the configureRemoteRoot.exe installed in C:\Program Files\VERITAS\Cluster Management Console\bin (default install directory).

Cluster Manager (Java console) limitations

Use the VCS 5.0 Java Console to manage clusters

Cluster Manager (Java Console) from previous VCS versions cannot be used to manage VCS 5.0 clusters. Symantec recommends using the latest version of Cluster Manager. See the *Veritas Cluster Server 5.0 Installation Guide* for instructions on upgrading Cluster Manager.

Run Java Console on a non-cluster system

Symantec recommends not running Cluster Manager (Java Console) for an extended period on a system in the cluster. The Solaris version of the Java Virtual Machine has a memory leak that can gradually consume the host system's swap space. This leak does not occur on Windows systems.

Cluster Manager and wizards do not work if the hosts file contains IPv6 entries

VCS Cluster Manager and Wizards fail to connect to the VCS engine if the /etc/hosts file contains IPv6 entries.

Workaround: Remove IPv6 entries from the /etc/hosts file.

VCS Simulator does not support I/O fencing

When running the Simulator, be sure the UseFence attribute is set to the default, “None.”

Undocumented commands, command options, and libraries

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

Documentation

Product guides are available on the documentation disc in PDF and HTML formats. We recommend copying pertinent information, such as installation guides and release notes, from the disc to your system directory /opt/VRTS/docs for reference.

VCS documentation set

VCS includes the following documents.

Title	File Name
Veritas Cluster Server Installation Guide	vcs_install.pdf
Veritas Cluster Server Release Notes	vcs_notes.pdf
Veritas Cluster Server User's Guide	vcs_users.pdf
Veritas Cluster Server Bundled Agents Reference Guide	vcs_bundled_agents.pdf
Veritas Cluster Server Agent Developer's Guide	vcs_agent_dev.pdf
Veritas Cluster Server Centralized Management Guide	vcs_central_mg.pdf
Veritas High Availability Agent for DB2 Installation and Configuration Guide	vcs_db2_install.pdf
Veritas High Availability Agent for Oracle Installation and Configuration Guide	vcs_oracle_install.pdf
Veritas High Availability Agent for Sybase Installation and Configuration Guide	vcs_sybase_install.pdf

The manual pages for `VRTSvcs` are installed in /opt/VRTS/man. Manual pages are divided into sections 1, 1m, 3n, and 4. Edit the `man`(1) configuration file /etc/man.config to view these pages.

To edit the man(1) configuration file

1. If you use the `man` command to access manual pages, set LC_ALL to "C" in your shell to ensure that the pages are displayed correctly.

   ```
   export LC_ALL=C
   ```

   See incident 82099 on the Red Hat Linux support website for more information.

2. Add the following line to /etc/man.config:

   ```
   MANPATH /opt/VRTS/man
   ```

where other man paths are specified in the configuration file.

3 Add new section numbers. Change the line:

```
MANSECT         1:8:2:3:4:5:6:7:9:tcl:n:l:p:o
```

to

```
MANSECT         1:8:2:3:4:5:6:7:9:tcl:n:l:p:o:3n:1m
```

Documentation feedback

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions to clustering_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.

Getting help

For technical assistance, visit http://www.symantec.com/enterprise/support/assistance_care.jsp

and select phone or email support. Select a product to use the Knowledge Base Search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and the customer email notification service. If you encounter an error when using a product, include the error number preceding the message when contacting Technical Services. You can also use the error number to search for information in TechNotes or documents on the website.