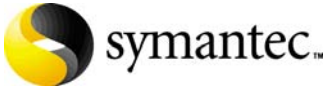
Veritas™ Cluster Server Release Notes

ESX

5.1 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 product. Such third-party software is licensed separately by its copyright holder.

Licensing and registration

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

Technical support

For technical assistance, visit:
http://www.symantec.com/business/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
- Changes in this release
- Features
- Veritas agents
- System requirements
- Installing VCS 5.1 MP1
- Upgrading to VCS 5.1 MP1
- Installation notes for VCS 5.1
- Software limitations
- Known issues
- Fixed issues
- Documentation
- Third-party legal notices
- Getting help

Introduction

This document provides important information regarding Veritas Cluster Server (VCS) 5.1 MP1 for VMware ESX. Review this entire document before installing VCS.

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

http://entsupport.symantec.com/docs/289940

Changes in this release

This section lists the changes in this release of VCS.

Support for IBM Metro Mirror

This release of VCS adds support for IBM Metro Mirror. For more information, refer to the *Veritas Cluster Server Agent for IBM MetroMirror Configuration Guide.*

Support for EMC SRDF

This release of VCS adds support for EMC SRDF. For more information, refer to the *Veritas Cluster Server Application Note: SRDF replication in a VCS for VMware environment.*

http://entsupport.symantec.com/docs/295185

Updates to the VMIP agent

The NICConf attribute for the VMIP resource has been added. The attribute helps support configuration of multiple network interfaces using a single resource of type VMIP. The updated attribute type takes the MAC address of the NIC as the key value and the IP address as the data. You can append a non-standard netmask in decimal notation to the IP address with a ":" as separator.

The updated type definition of the VMIP agent follows:

```
type VMIP (
    static int MonitorInterval = 300
    static str ArgList[] = { "VMwareResName:CfgFile", IPAddress,
    MACAddress, NetMask, Gateway, DNS, NICConf }
    str VMwareResName
    str IPAddress
    str MACAddress
    str NetMask
```

```
        str Gateway
        str DNS[]
        str NICConf{}
    )
```

A sample main.cf with the NICConf attribute, and its use follows:

```
VMIP vmIP_rhel4_32bit_vm (
    VMwareResName = esxVM_rhel4_32bit_vm
     IPAddress = "10.100.90.18"
     MACAddress = "00:50:56:94:57:05"
     NetMask = "255.255.248.0"
     Gateway = "10.100.88.1"
     DNS = { "10.100.88.20", "192.168.1.3" }
     NICConf {
     "00:50:56:94:06:5D " = "10.100.90.16:255.255.248.0",
     "00:50:56:94:64:B1" = "192.168.1.18" }
)
```

Changes in the installvcs program with the -configure option

The installvcs program with the -configure option has some modifications in the firewall configuration prompt and the VI3 login credentials prompt.

See “Configuring VCS 5.1 MP1” on page 19.

Virtual machine display name attribute is mandatory for the migrate and testVCConnect actions

The Vmname attribute for the ESXVirtualMachine resource is mandatory for the migrate and testVCConnect action agent functions for ESXVirtualMachine resources.

Features

This release of Veritas Cluster Server includes the following features.

Support for monitoring applications in virtual machines

VCS provides agents to monitor the following applications running inside virtual machines.

- Linux: Apache Web server; IBM HTTP Server; Oracle; SAP NetWeaver
- Windows: Exchange; Internet Information Services (IIS); SQL

See "Supported applications" on page 15.

Support for virtual machines running Solaris 10 x64 Platform Edition

VCS supports configuring virtual machines running Solaris 10 x64 Platform Edition. This release does not support monitoring applications running inside virtual machines running Solaris 10 x64 Platform Edition.

See "Supported operating systems" on page 12.

Support for agents to manage replication

This release of VCS supports the following replication technologies:

- EMC MirrorView
- Hitachi TrueCopy
- IBM Metro Mirror
- EMC SRDF

Support for monitoring NFS mounts in virtual machines

This release supports monitoring NFS mounts in virtual machines. Configure the Mount agent to monitor NFS mounts.

See the *Veritas Cluster Server Implementation Guide* for more information.

Support for virtual machine datastores on NFS

This release supports configuring virtual machine datastores on NFS.

See the *Veritas Cluster Server Implementation Guide* for more information.

Support for raw device mapping (RDM)

This release supports virtual machines with RDM disks. Use the Disk agent to configure RDM disks.

See the *Veritas Cluster Server Implementation Guide* for more information.

VCS interface to trigger VMotion

Use the `hagrp -migrate` command to trigger VMotion for a virtual machine configured as a VCS resource. You can also run this command from the VCS Management Console.

Support for VMotion and Distributed Resource Scheduler

VCS recognizes virtual machine migration initiated by VMotion or DRS. VCS does not interpret this motion as a fault.

Dynamic increase of storage allocated to virtual machines

You can dynamically increase the size of your application mount points or file systems inside the virtual machine without having to reboot the virtual machine. See the *Veritas Cluster Server Implementation Guide* for more information.

VCS Management Console (formerly the Cluster Management Console)

The VCS Management Console enables administration and analysis for VCS clusters in your enterprise from a single console. You can install the console on a standalone system to manage multiple clusters or you can install it on cluster nodes to manage a local cluster.

Cluster Manager (Java Console)

This release includes Cluster Manager (Java Console.) See the *Veritas Cluster Server Implementation Guide* for more information.

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.

Contact your Symantec sales representative for information about Veritas agents under development, and agents available through Symantec consulting services.

System requirements

System requirements for VCS follow:

- "VMware ESX Servers" on page 11
- "Required patches for ESX 3.0.x systems running VCS 5.1" on page 11
- "Supported operating systems" on page 12
- "Supported applications" on page 15
- "Supported hardware" on page 16

VMware ESX Servers

VCS supports ESX Server 3.0, 3.0.1, and 3.0.2 plus all required VMware ESX patches.

- VMware Infrastructure Enterprise. This edition is required for full VCS functionality and integration.
- VMware Infrastructure Standard. This edition has certain limitations.
  - Veritas Virtualization Manager (VVM) is not supported.
  - Service group migration via VMotion is not supported.

VCS supports datastores on VMFS 3 (SAN-attached or NFS.) VCS does not support the iSCSI protocol.

Required patches for ESX 3.0.x systems running VCS 5.1

On ESX 3.0.* systems that run VCS 5.1 or a subsequent VCS MP release on top of 5.1, ensure that the VMware Perl and COM Scripting API v2.3.1 (or later) are installed. These are required so that the ESXVirtualMachine agent can correctly determine virtual machine unavailbility. To download and install the Scripting API patch, refer to VMware documentation for details.

Supported operating systems

Refer to the following information for supported operating systems for VCS for ESX.

- "Supported operating systems in virtual machines for high availability" on page 12
- "Supported operating systems in virtual machines for application monitoring or disaster recovery" on page 13
- "Supported operating systems for increasing allocated storage" on page 14

Supported operating systems in virtual machines for high availability

VCS for ESX provides high availability for all the operating systems that are supported by VMware ESX as virtual machine guests.

If you need application monitoring or disaster recovery refer to the following section.

Supported operating systems in virtual machines for application monitoring or disaster recovery

Table 1-1 lists the architectures and operating systems that VCS for VMware supports.

Table 1-1 Supported operating systems and architectures

Guest operating systems	Kernels	Architectures	File systems/ Volume managers
*Windows 2000 Server or Advanced Server with Service Pack 4	---	x86 (32-bit)	NTFS
*Windows Server 2003: Standard Edition or Enterprise Edition (SP2 required)	---	x86 (32-bit) x86 (64-bit)	NTFS
*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) x86 (64-bit)	ext2, ext3, reiserfs/ LVM
*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) x86 (64-bit)	ext2, ext3, reiserfs/ LVM
SUSE Linux Enterprise Server 10 (SLES 10) with SP1	2.6.16-37-0.18-smp 2.6.16-37-0.18-bigsmp	x86 (32-bit) x86 (64-bit)	ext2, ext3, reiserfs/ LVM
Solaris 10	---	x86	

* Supports the mount .iso feature.

On Linux-based operating systems: Veritas products will operate on subsequent kernel and patch releases provided the operating systems maintain kernel ABI (application binary interface) compatibility.

On Windows-based operating systems: Veritas products will operate on subsequent service pack (SP) releases provided that the vendor maintains forward compatibility.

Note: The EMC CLARiiON series and Symmentrix series storage arrays do not support virtual machines running Solaris 10 U1 guest operating systems. See the VMware documentation for more information.

Supported operating systems for increasing allocated storage

Table 1-2 lists the guest operating systems that VCS supports for increasing allocated storage.

Table 1-2 Supported operating systems for increasing allocated storage

Guest operating systems	32-bit	64-bit	Supported file systems
Windows 2000	Yes	No	NTFS
Windows Server 2003	Yes	No	NTFS
*RHEL 4 Update 3	Yes	Yes	ext3
SLES 9 with SP3	Yes	Yes	reiserfs/LVM
SLES 10 with SP1	No	No	N.A.
Solaris 10	N.A.	No	N.A.

* Supports increasing allocated storage once.

Note that file systems on raw device maps do not support increasing allocated storage.

Supported applications

VCS provides agents to monitor the following applications running in a virtual machine.

Table 1-3 Supported guest applications

Platform	Applications	Versions
Linux	Apache Web server	1.3, 2.0, and 2.2
“ “	IBM HTTP Server	1.3 and 2.0
“ “	Oracle	10g
“ “	SAP NetWeaver	SAP R/3-4.6C with a 4.6D Kernel, 4.6D, 4.7 Enterprise Version SAP Web AS-6.20, 6.40, 7.00 SAP NetWeaver-2004, 2004s
Windows	Exchange	Exchange Server 2003
“ “	IIS	5.0 and 6.0
“ “	SQL	Microsoft SQL Server 2000 Standard Edition or Enterprise Edition (both require SP4) Microsoft SQL Server 2005, 32-bit (SP1 required)

VCS additionally provides the following agents to monitor other applications:

- Application agent on virtual machines running Linux
- GenericService agent on virtual machines running Windows

Support for detecting intentional offline for specific applications

Certain agents can identify when an application has been intentionally shut down as opposed to when an application has crashed. When VCS detects an intentional offline, VCS does not trigger a failover. This feature allows administrators to manage the applications (start/stop) that run inside the virtual machines without causing additional failovers.

Table 1-4 Agents that support detection of intentional offline of the configured application

Guest operating systems	Applications
Linux	■ Apache ■ Oracle ■ Netlsnr ■ SAP NetWeaver
Windows	■ Exchange Server ■ Internet Information Services (IIS) ■ SQL Server ■ GenericService

Supported hardware

For the latest information on supported hardware, see the hardware compatibility list published by VMware.

See the documentation published by your array vendor for information about:

- Hardware compatibility with VMware ESX
- Supported microcode or firmware versions
- Supported versions of client software for the array
- Supported versions of the replication and mirroring software
- Recommended array settings

Selecting your installation or upgrade

If you have a “fresh” environment with no previous version of VCS, follow these instructions:

See “Installing VCS 5.1 MP1” on page 17.See “Installing VCS 5.1 MP1.

If you have a VCS 5.1 environment configured and running, follow these instructions:

See “Upgrading to VCS 5.1 MP1” on page 27.

Installing VCS 5.1 MP1

Install VCS on ESX Server systems, the Veritas Virtualization Manager on clients, and the Veritas Virtual Machine Tools in virtual machines. Use the following information to perform an installation of VCS:

- “Installing VCS on ESX Server systems” on page 17
- “Installing Veritas Virtualization Manager (VVM) on clients” on page 20
- “Installing Veritas Virtual Machine Tools in virtual machines running Windows” on page 21

Symantec recommends that you install all required patches prior to installation. For more information, see “System requirements” on page 11.

For instructions on upgrading to VCS 5.0 MP1, see:

- “Upgrading to VCS 5.1 MP1” on page 27

Installing VCS on ESX Server systems

When you perform an installation of VCS on ESX Server systems, you must install VCS 5.1 and stop the installation before you answer the configuration questions. You then install the 5.1 MP1 patch, and then configure VCS.

To install VCS 5.1 MP1 perform the following procedures.

- “Installing VCS 5.1” on page 18
- “Installing VCS 5.1 MP1” on page 18
- “Configuring VCS 5.1 MP1” on page 19
- “Upgrading your configuration” on page 20

Installing VCS 5.1

For complete installation instructions, refer to the *Veritas Cluster Server Implementation Guide*. For other updated information, see:

"Installation notes for VCS 5.1" on page 32

Note: When you install VCS on ESX Server systems, do not configure the cluster.

Answer **n** when the installvcs program prompts:

```
Are you ready to configure VCS? [y,n,q] (y) n
```

Installing VCS 5.1 MP1

Perform the following steps to install VCS 5.1 MP1. At the end of the installation, do not perform the suggested system shut down and reboot, instead follow the instructions provided.

To install VCS 5.1 MP1

1. Log in as superuser on one of the systems.
2. Insert the disc containing the VCS 5.1 MP1 software into the disc drive of one of the cluster nodes.
3. Mount the disc on a suitable mount point and change directory to the location of the disc mount.
4. Start the VCS 5.1 MP1 installation.

   ```
   ./installmp
   ```

   Running the installmp script stops VCS.
5. The installer prompts you for the system names where you want to install the maintenance pack.

   ```
   Enter the system names separated by spaces on which to install
   MP1: sysA sysB
   ```

   Where sysA and sysB are example system names.
6. After an initial system check, the setup program is ready to install VCS 5.1 MP1 and seeks confirmation.

   ```
   Are you sure you want to install MP1? [y,n,q] (y)
   ```

   Enter **y** to begin installation.

   Do not reboot after VCS 5.1 MP1 is installed.

Configuring VCS 5.1 MP1

Run the installvcs program with the -configure option from one of the ESX Server systems where you installed VCS.

To configure 5.1 MP1

1. On one of the ESX Server systems where you installed VCS, run the installvcs program with the -configure option.

   ```
   # /opt/VRTS/install/installvcs -configure sysA sysB
   ```

   Where sysA and sysB are example system names.

2. During the final phase of the configuration, VCS 5.1 MP1 prompts you to open certain ports for the VCS agents on the ESX Server nodes. Enter **y** to configure the firewall.

   ```
   Do you want continue with the firewall configuration? [y,n,q]
   (y) y
   ```

3. The installvcs program prompts you to generate an ESX system user. The same user is used to create a login credentials file for VCS agents. The default user name is **vcs**, but you can choose any other user name. For VCS agents to work correctly, do not remove or modify the VCS generated user or its password after it has been created. The installvcs program prompts for root password, but uses the password only to generate the new **vcs** system user.

   Enter **y** if you want to use the same root and keystore password on the other hosts.

   ```
   Do you want to use the same root and keystore password on the
   other hosts?[y,n,q] (y)
   ```

   This generates the login credentials file.

4. Make sure that the installvcs program successfully configures the cluster, and prompts you to start the VCS components when it completes.

5. In a separate command window, verify the configuration with the following command:

   ```
   $ hacf -verify config
   ```

   If the configuration has no errors, the command exits with no error printed on the console.

6. Return to the installvcs command window, and choose **Y** to start VCS components.

7. Run the following command on each node of the cluster to start VCS.

   ```
   $ /etc/init.d/vcs start
   $ hasys -state vcs_system_name
   ```

   Make sure the system is in the running state before moving on to start VCS on the next system.

Upgrading your configuration

Perform this section after completing the previous section:

"Configuring VCS 5.1 MP1" on page 19.

This section provides information on how to upgrade your configuration from VCS 5.1 to VCS 5.1 MP1. Use the upgradeconf.sh script (on the disc in cluster_server/tools/) to automate your upgrade.

The upgradeconf.sh script performs the following tasks, it:

- Adds the MetroMirror types file to the configuration.
- Adds the NICConf attribute to the configuration.
- Removes all existing VSwitch resources to follow the network infrastructure scheme.
- Detects any duplicate VSwitch resources in the configuration and Creates a Proxy resource that points to a common VSwitch resource in the Network Infrastructure service group.

To upgrade your configuration

1. Run the upgradeconf.sh script to upgrade the VCS configuration to the 5.1 MP1 level.

   ```
   # ./upgradeconf.sh
   ```

2. The script prompts you to start configuration.

   ```
   Are you ready to configure the VCS 5.1MP1 configuration (Y/N)[Y] ?
   ```

   Enter **y** to begin the configuration.

3. As the script prompts you, provide answers, and make sure that the script completes with no errors.

Installing Veritas Virtualization Manager (VVM) on clients

If you do not have the VVM installed on your system, you can install or upgrade it from the maintenance pack disc.

To install or upgrade VVM

1. Insert the product disc into a drive on the client system.
2. Change the directory to windows/vvm.
3. Run the vcsvm.msi file.
4. Review the Welcome screen and click **Next**.
5. Click **Install** to begin the installation of the Veritas Virtualization Manager.

6 After the InstallShield wizard completes the installation, click **Finish** to exit the wizard.

7 To confirm that the upgrade is successful, you can go to **Start** > **Settings** > **Control Panel** > **Add Remove Programs** and click on Support Information for Veritas Virtualization Manager to verify that the version is 5.1.1000.

Installing Veritas Virtual Machine Tools in virtual machines running Windows

Install Veritas Virtual Machine Tools on a Windows virtual machine where you want to monitor an application for high availability. The utility is on the disc inside the vcsvm_tools directory.

The utility is on the disc inside the vcsvm_tools directory. It is in the ISO format:

- For x86 (32-bit) architectures, use:
  win-x86-vcsvm-tools.iso
- For x64 architectures, use:
  win-x64-vcsvm-tools.iso

To add the tools .iso file

1 From a Windows client, click **Start** > **Programs** > **Symantec** > **Veritas Virtualization Manager**.

2 Right-click the virtual machine where you want to add the .iso file. Select **Add VCSVM-Tools ISO**. VVM automatically selects the proper .iso file to match the operating system.

3 The Add CD-ROM ISO window appears.

4 Click the **OK** button to add the .iso file.
The ISO file is now available for your use.

To install Veritas Virtual Machine Tools

1 Once you have mounted the appropriate ISO file to your virtual machine, run the vcsvm-tools.exe file to install the tools.

2 Review the Welcome screen and click **Next**.

3 Review the License Agreement, choose to accept, and then click **Next**.

4 In the Destination Folder screen, either accept the default location or click **Browse** to choose another location. Click **Next** when done.

5 In the Halogin Configuration screen, enter the cluster login credentials. You must configure halogin before running the SQL and IIS agent wizards; otherwise, the wizards won't be able to complete the configuration.
   - IP address or DNS name of your VCS ESX cluster
   - User name and password for your VCS ESX cluster
   - VCS virtual machine resource associated with this system

6 Click **Next**.

7 In the Convert Basic Disks to Dynamic screen, only check the box if you have basic disks that you need to convert to dynamic disks. Make sure that if you have any volumes mounted on a basic disk, unmount the volumes before converting the disks to dynamic.
   Note that this applies for Windows 2003 users only, as Windows 2000 users won't see this screen.
   Click **Next** when done.

8 In the PageFile Drive Selection screen, you are presented with a list of available drives, the size and type of the pagefile if present, and the available space on the drive.
   Select a drive and
   - Delete the pagefile, if it exists on a replicated volume. Click **Delete Pagefile**.
   - Create a pagefile. You can choose to either create a Custom pagefile or a System-managed pagefile.
     For a custom pagefile, you must enter the initial size (in MB) and the maximum size (in MB), and then click **Create**. Note that the maximum size is constrained by the Windows maximum size limit of 4096 MB. Or check the System Managed check box and click **Create**.

   Click **Next** when done.

9 In the Ready to Install screen, click **Install**.

10 Click **Finish** to close the installer.

11 Verify the installation. Check to see if the VCSAgMD service is present in the Services panel. (**Start** > **Programs** > **Administrative Tools** > **Services**)

Validating the configuration and success of Veritas Virtual Machine Tools installation

Use the following procedure to verify that the tools are properly configured.

To validate Veritas Virtual Machine Tools configuration

1. Get the virtual machine resource name, which is in the file $VCS_HOME\.vcsvmresname. Typically, you can find the .vcsvmresname file in the C:\Program Files\Veritas\cluster server\. To get the name, type the following:

   ```
   C:\Program Files\Veritas\cluster server\.vcsvmresname
   ```

   Warning: Ensure that the .vcsvmresname file does not get deleted. This file is critical to convey application faults to the ESX layer.

2. Use the virtual machine resource name to run the following command and make sure that the command completes. At the prompt, type:

   ```
   C:\Program Files\Veritas\cluster server\hares -value
   vmres_name Type
   ```

   Where vmres_name is the virtual machine resource name.

3. Again, use the virtual machine resource name and run the following command:

   ```
   C:\Program Files\Veritas\cluster server\hares -state
   vmres_name
   ```

   Where vmres_name is the virtual machine resource name.

4. To confirm that the installation is successful, go to **Start** > **Settings** > **Control Panel** > **Add Remove Programs** and click on Support Information for vcsvm-tools-dotnet or vcsvm-tools-winx64 to verify that the version is 5.1.1000.

Installing Veritas Virtual Machine Tools in virtual machines running Linux

Before you install Veritas Virtual Machine Tools, you need to mount the .iso file for the virtual machine.

Before you mount or install the tools, prepare the following information:

- The virtual IP address for the cluster.
- The username and password required to administer the service group.
- The name of the ESXVirtualMachine resource that is associated with the virtual machine.
- In disaster recovery environment only, you need the device path for the location of the pagefile datastore on another storage device.

Mounting the Veritas Virtual Machine Tools

VVM can make the Veritas Virtual Machine Tools installation program available to you for easy access.

To mount the tools .iso file

1. From a Windows client, click **Start** > **Programs** > **Symantec** > **Veritas Virtualization Manager**.
2. Right-click the virtual machine where you want to mount the .iso file. Select **Add VCSVM-Tools ISO**.
   If you receive this message, "This virtual machine has the ISO image mounted already," refer to the procedure:
   "To resolve the "virtual machine has the ISO image mounted already" error" on page 24.
3. Click the **OK** button to add the .iso file.
   The Add CD-ROM ISO window appears. The .iso file is now available for your use.

To resolve the "virtual machine has the ISO image mounted already" error

1. Open the VMware Infrastructure Client.
2. Click the virtual machine, and go to the Summary tab.
3. On the Summary tab, click **Edit Settings**.
4. Check **Client Device** in the Device Type section, and click **OK** to save.
5. In VVM, right-click the virtual machine and select **Add VCSVM-Tools ISO**.

Installing the Veritas Virtual Machine Tools

Install the Veritas Virtual Machine Tools.

To install the Veritas Virtual Machine Tools

1. Navigate to the installvcsvm-tools program location.
   ```
   # cd /media/cdrom
   ```
2. On the virtual machine, enter the `vcsvm-tools -i` command.
   ```
   # ./installvcsvm-tools -i
   ```
3. When you are prompted to install the tools, press the **y** key to proceed.
4. The installvcsvm-tools program prints some information and asks if you want to configure the tools. Press the **y** key to configure the tools.

Configuring the Veritas Virtual Machine Tools

Configure the Veritas Virtual Machine Tools.

To configure the Veritas Virtual Machine Tools

1. On the virtual machine, enter the `installvcsvm-tools -c` command.
   ```
   ./installvcsvm-tools -c
   ```
   On a virtual machine that already has the tools mounted, use the full path for the command. At the prompt, enter:
   ```
   /opt/VRTSvcs/bin/installvcsvm-tools -c
   ```
2. When asked if you are ready to configure the tools, answer **y**.
3. Enter the virtual IP address of the VCS cluster that the virtual machine belongs to.
4. Enter the username and password for the cluster that the virtual machine belongs to. This is the same administrator that you created when you configured the virtual machine for high availability or disaster recovery.
5. Enter the name of the ESXVirtualMachine resource that is associated with the virtual machine.
6. In a disaster recovery environment, enter the device path for the location of the pagefile datastore on the secondary storage device. Note that this step is not required for a high availability environment.
   Veritas Virtual Machine Tools configuration is now complete.

Validating the configuration and success of Veritas Virtual Machine Tools installation

You can verify that the tools are properly configured and that the installation is successful.

To validate the tools' configuration and success of installation

1. Get the virtual machine resource's name, which is in the file /etc/VRTSvcs/.vcsvmresname. To get the name, type:

   ```
   # cat /etc/VRTSvcs/.vcsvmresname
   ```

   Warning: Ensure that the .vcsvmresname file does not get deleted. This file is critical to convey application faults to the ESX layer.

2. Use the virtual machine resource's name to run the following command and make sure that the command completes. At the prompt, type:

   ```
   # /opt/VRTSvcs/bin/hares -value vmres_name Type
   ```

   Where vmres_name is the virtual machine resource's name.

3. Again use the virtual machine resource's name and run the following command:

   ```
   # /opt/VRTSvcs/bin/hares -state vmres_name
   ```

   Where vmres_name is the virtual machine resource's name.

4. To confirm that the installation is successful, run the following command inside the Linux virtual machine:

   ```
   $ /opt/VRTSvcs/bin/vcsvm-tools -v
   ```

   Verify that the version is 5.1.30.00.

Upgrading to VCS 5.1 MP1

Upgrade VCS on ESX Server nodes, the Veritas Virtualization Manager on clients, and the Veritas Virtual Machine Tools in virtual machines. Use the following information to perform an upgrade of VCS:

- "Upgrading VCS on ESX Server nodes" on page 27
- "Upgrading Veritas Virtualization Manager (VVM) on clients" on page 29
- "Upgrading Veritas Virtual Machine Tools in virtual machines running Windows" on page 30

Symantec recommends that you install all required patches prior to upgrade. For more information, see "System requirements" on page 11.

Upgrading VCS on ESX Server nodes

To upgrade from VCS 5.1 to VCS 5.1 MP1 perform the following procedures.

- See "Upgrading to VCS 5.1 MP1" on page 27.
- See "Upgrading your configuration" on page 28.

Upgrading to VCS 5.1 MP1

To upgrade from VCS 5.1 to VCS 5.1 MP1, perform the following instructions. At the end of the upgrade, do not perform the suggested system shut down and reboot, instead follow the instructions provided.

To upgrade to VCS 5.1 MP1

1. Log in as superuser on one of the systems for installation.
2. Insert the disc containing the VCS 5.1 MP1 software into the disc drive of one of the cluster nodes.
3. Mount the disc on a suitable mount point and change directory to the location of the disc mount.
4. Install VCS 5.1 MP1 using the installmp script:

   ```
   # ./installmp
   ```

   Running the installmp script stops VCS.
5. The installer prompts for the system names on which you want to install the maintenance pack.

   ```
   Enter the system names separated by spaces on which to install
   MP1: sysA sysB
   ```

   Running the installmp script stops VCS but leaves the applications under VCS control in their current state.

6 After an initial system check, the setup program is ready to install VCS 5.1 MP1 and seeks confirmation.

```
Are you sure you want to install MP1? [y,n,q] (y)
```

Enter **y** to begin installation.

7 Review the output as VCS 5.1 MP1 installs.

8 Once the installation is complete verify if VCS restarts and it is at the VCS 5.1 MP1 level. Run the `rpm -qa | grep VRTSvcs` and the `hasys -state` commands. Example output follows below:

```
# rpm -qa | grep VRTSvcs
VRTSvcs-5.1.30.00-MP1_ESX30
# hasys -state
#System    Attribute           Value
sysA       SysState            RUNNING
```

9 Run the following command on each node of the cluster to start VCS.

```
$ /etc/init.d/vcs start
$ hasys -state vcs_system_name
```

Make sure the system is in the running state before moving on to start VCS on the next system.

Upgrading your configuration

Perform this section after completing the previous section:

"Upgrading to VCS 5.1 MP1" on page 27.

This section provides information on how to upgrade your configuration from VCS 5.1 to VCS 5.1 MP1. Use the upgradeconf.sh script (on the disc in cluster_server/tools/) to automate your upgrade.

The upgradeconf.sh script performs the following tasks, it:

- Adds the MetroMirror types file to the configuration.
- Adds the NICConf attribute to the configuration.
- Removes all existing VSwitch resources to follow the network infrastructure scheme.
- Detects any duplicate VSwitch resources in the configuration and Creates a Proxy resource that points to a common VSwitch resource in the Network Infrastructure service group.

To upgrade your configuration

1. Run the upgradeconf.sh script to upgrade the VCS configuration to the 5.1 MP1 level.

   ```
   # ./upgradeconf.sh
   ```

2. The script prompts you to start configuration.

   ```
   Are you ready to configure the VCS 5.1MP1 configuration (Y/N)[Y] ?
   ```

   Enter **y** to begin the configuration.

3. As the script prompts you, provide answers, and make sure that the script completes with no errors.

Upgrading Veritas Virtualization Manager (VVM) on clients

If you do not have the Veritas Virtualization Manager installed on your system, you can install or upgrade it from the maintenance pack disc.

To install or upgrade Veritas Virtualization Manager (VVM)

1. Insert the product disc into a drive on the client system.
2. Change the directory to windows/vvm.
3. Run the vcsvm.msi file.
4. Review the Welcome screen and click **Next**.
5. Click **Install** to begin the installation of the Veritas Virtualization Manager.
6. After the InstallShield wizard completes the installation, click **Finish** to exit the wizard.
7. To confirm that the upgrade is successful, you can go to **Start** > **Settings** > **Control Panel** > **Add Remove Programs** and click on Support Information for Veritas Virtualization Manager to verify that the version is 5.1.1000.

Upgrading Veritas Virtual Machine Tools in virtual machines running Windows

You must upgrade each virtual machine individually.

If you do not have the 5.1 Veritas Virtual Machine Tools previously installed on your virtual machines, see:

"Installing Veritas Virtual Machine Tools in virtual machines running Windows" on page 21.

The utility is on the disc inside the installvcsvm_tools directory. It is in the ISO format:

- For x86 (32-bit) architectures, use:
  win-x86-vcsvm-tools.iso
- For x64 architectures, use:
  win-x64-vcsvm-tools.iso

To add the Tools .iso file

1. From a Windows client, click **Start** > **Programs** > **Symantec** > **Veritas Virtualization Manager**.
2. Right-click the virtual machine where you want to add the .iso file. Select **Add ISO Image**. VVM automatically selects the proper .iso file to match the operating system.
   The Add CD-ROM ISO window appears.
3. Click the **OK** button to add the .iso file.
   The ISO file is now available for your use.

To upgrade the Veritas Virtual Machine Tools

1. Once you have mounted the appropriate ISO file to your virtual machine, run the vcsvm-tools.exe file to upgrade the Tools.
2. Review the Welcome screen and click **Next**.
3. Click **Finish** to close the installer.
4. Verify the installation. Check to see if the VCSAgMD service is present in the Services panel. (**Start** > **Programs** > **Administrative Tools** > **Services**)
5. To confirm that the upgrade is successful, you can go to **Start** > **Settings** > **Control Panel** > **Add Remove Programs** and click on Support Information for vcsvm-tools-dotnet or vcsvmm-tools-winx64 to verify that the version is 5.1.1000.

Upgrading Veritas Virtual Machine Tools in virtual machines running Linux

You must upgrade each virtual machine individually.

If you do not have the 5.1 Veritas Virtual Machine Tools previously installed on your virtual machines, see:

"Installing Veritas Virtual Machine Tools in virtual machines running Linux" on page 24

To upgrade VCS Virtual Machine Tools from VCS 5.1 to 5.1 MP1 on virtual machines running Linux

1. Mount the product disc.
2. Navigate to the installvcsvm-tools location.
   ```
   cd /media/cdrom/
   ```
3. On the virtual machine, enter the `installvcsvm-tools -n` command.
   ```
   ./installvcsvm-tools -n
   ```
4. To confirm that the upgrade is successful, run the following command inside the Linux virtual machine:
   ```
   $ /opt/VRTSvcs/bin/vcsvm-tools -v
   ```
   Verify that the version is 5.1.30.00.
5. If the result of step 4 is unsuccessful, perform the following procedure:
   "To configure the Veritas Virtual Machine Tools" on page 25.

Installation notes for VCS 5.1

Refer to the *Veritas Cluster Server Implementation Guide* for instructions on how to install VCS. The guide is in the docs directory of the software disc.

The following information includes guidelines, tips, and other considerations for installing the 5.1 version of the product.

Merge updated type definitions after upgrade from 5.0 to 5.1

After upgrading to VCS 5.1, you must merge the type definitions in the types.cf file.

To merge the type definitions

1. Stop VCS on the ESX Server nodes:
   # **hastop -all -force**
2. Merge the new types.cf with the old types.cf. If you have not added any new type definitions to your types.cf, you can replace the old types.cf file with the new one.
   The new types.cf file is installed at: /etc/VRTSvcs/conf/default/
   The old types.cf file is at: /etc/VRTSvcs/conf/config/
3. Start VCS on the node where you updated the types.cf file:
   # **hastart**
   Do not start VCS on other nodes at this time.
4. After VCS goes into running state on that node, start VCS on the other nodes.

Do not configure Security Services when installing VCS

This release of VCS does not support configuring the Symantec Product Authentication Service. Do not configure the service when installing VCS.

Change the default password after installing VCS

When you install and configure VCS, if you do not choose the secure mode (which is recommended), 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.

Installer does not recognize valid license keys in specific situations

This issue occurs while installing VCS, if you enter an invalid license key, and terminate the installation program. If you run the installation program again and enter a valid license key, the program prints a message saying the license key is not valid. This may also occur if you run the installation program after the /etc/vx directory was inadvertently erased. [1076425]

Workaround: Uninstall the VRTSvlic package before running the installvcs program.

Installer may hang when restarting VMware management service

Because of a VMware ESX Server issue, the installation program may hang while trying to restart the VMware management service. [1111867]

Workaround: Manually stop and start the management service using the following commands:

```
service mgmt-vmware stop
service mgmt-vmware start
```

You may need to stop and start the management service on each node during the install process.

Installing VCS with the response file does not work

This release does not support installing VCS using the response file. [802303, 1130788]

Cannot attach the virtual machine console from the VirtualCenter

After installing VCS, you cannot attach the virtual machine console from the VirtualCenter. [1107798]

Workaround: Follow this procedure:

1. Edit the file /etc/vmware/config file.
2. Set the value of vmauthd.server.alwaysProxy to TRUE.

   ```
   vmauthd.server.alwaysProxy=TRUE
   ```
3. Reboot the ESX servers.

Disaster recovery configuration requires the latest bind utilities

The DNS agent requires bind-utils-9.2.4-16.EL4. Symantec recommends installing the latest version of bind utilities before configuring the cluster for disaster recovery. [1081009.]

For more information on obtaining the latest version, visit the VMware website.

Software limitations

The following limitations apply to this release.

The rui.crt file has a new location in VirtualCenter 2.0.x

When you use VirtualCenter 2.0.x, and if you cannot fine the rui.crt file, you may have to look in this directory for it:

```
C:\Documents and Settings\All Users\Application Data\VMware\
VMwareVirtualCenter\SSL\
```

Note that this file is in a hidden folder, and cannot be found using the Windows search. [1157286]

VCS does not support cold migration of virtual machines

VCS supports migrating virtual machines by using VMotion or by running the `hagrp -migrate` command. VCS provides this support only if the service group configured for the virtual is in an ONLINE state. [1108005]

Do not freeze service groups without the evacuate option

Symantec recommends that you always run the `hasys -freeze` or `hasys -freeze -persistent` commands with the `-evacuate` option. Use the `-evacuate` option to maintain compatibility between VCS and the VMware cluster.

VCS does not support raw devices in disaster recovery environments

VCS does not support raw device configurations in disaster recovery environments.

VCS replicated data clusters

Replicated data clusters are not supported in this release of VCS.

Application Configuration Wizards on windows virtual machines do not support modifying configurations

Every time you run a VCS configuration wizard on a Windows virtual machine, the process creates a new configuration. To preserve your earlier configuration, you must recreate the configuration when running the wizard.

The IIS agent does not detect intentional offline of websites or virtual servers

The IIS agent detects an intentional offline of IIS services. The agent, however, does not detect an intentional offline of IIS websites or the FTP, NNTP, and SMTP virtual servers. If you stop a virtual server or a website, the IIS agent interprets the action as a resource fault and triggers a failover. [809217]

To stop the website or virtual server, you must stop the corresponding service.

The Exchange agent does not detect intentional offline of protocol virtual servers

The Exchange agent detects an intentional offline of protocol services. The agent does not, however, detect an intentional offline of protocol virtual servers like the SMTP Virtual Server. If you stop an Exchange protocol server, the Exchange agent interprets the action as a resource fault and triggers a failover. [1052626]

To stop an Exchange protocol virtual server, you must to stop the corresponding service.

Limitations related to LVM settings

VCS agents for Hitachi TrueCopy, EMC MirrorView, and IBM MetroMirror rescan datastores using the following parameters:

- LVM.EnableResignature = 0
- LVM.DisallowSnapshotLUN = 0

The agents set these values to detect datastores on the disaster recovery site.

The fire drill agents (HTCSnap and MirrorViewSnap) rescan datastores after temporarily setting the following parameters:

- LVM.EnableResignature = 1
- LVM.DisallowSnapshotLUN = 0.

The agents set these values to detect snapshots that can be used for the fire drill.

These settings impose some limitations on VCS configuration and usage. VMware provides a global setting, which enables rescanning of all LUNs, as against a mechanism that can selectively rescan LUNs. See the VMware documentation for more information on ESX server behavior with these settings.

Remote fire drill limitation

Before running a remote fire drill on the secondary site, make sure that the secondary site does not have any global service groups in the ONLINE state. This restriction applies to service groups that may have failed over or switched to the secondary site. If this restriction is not met, running a fire drill may cause undesirable resignaturing of other unrelated datastores.

Local fire drill limitation

Do not run a local fire drill on the secondary site, even if the secondary site has become the new primary site after a failover. If this restriction is not met, running a fire drill may cause undesirable resignaturing of other unrelated datastores.

Run fire drills on dedicated node and make snapshot LUNs visible to only that node

Symantec recommends dedicating one node in the cluster for fire drills. Configure fire drill service groups on this node. Do not configure replication resources (for example HTC or MirrorView) on this node. Configure your array such that snapshot LUNs are visible to this node only; the other nodes must not see snapshot LUNs.

The restriction occurs because other nodes in the cluster may have LVM settings LVM.EnableResignature = 0 and LVM.DisallowSnapshotLUN = 0 set by the replication agents, in which case VMWare recommends that no snapshot LUNs should be exposed to such ESX hosts.

Cluster address for global cluster requires resolved virtual IP

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

Systems in a cluster must have same system locale setting

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

Networking agents do not support IPv6 protocol

The bundled networking agents for VCS do not support the IPv6 IP protocol.

Undocumented commands, command options, and libraries

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

Known issues

The following issues are open for this release of VCS.

The diskpart.exe and shutdown.exe files are not available on the base installation of Windows 2000

The absence of these binaries may cause problems for GrowFS and VMIP. [1188035]

Workaround: For diskpart.exe, you can use a Microsoft provided Resource Kit extension that the agent uses if installed in the default location:

"C:\PROGRA~[0-9]\RESOUR~[0-9]\diskpart.exe".

No workaround exists for shutdown.exe currently.

The IIS agent configured with IIS bound to an IP address requires manual intervention on disaster recovery failover

The Windows IIS agent takes in an IP address as an attribute if the iis-webserver is bound to only a single IP on the node. When a disaster recovery failover event occurs, however, the IP address of the VM changes. [1071149]

Workaround: After a disaster recovery failover of a Windows virtual machine with IIS setup for VCS monitoring, reconfigure the IIS resource. Log into the virtual machine and run the IIS configuration wizard. When the wizard prompts you to select the Web sites, chose the Web sites that you want to monitor, and enter the newer IP addresses that correspond to each Web site for this particular disaster recovery site.

The SQL Wizard sets the default instance name to the computer name when configuring SQL 2000 on Win 2000

When running the SQL Configuration wizard on Windows 2000 SP4 to configure the default instance of SQL 2000, the instance name gets set to the computer name.

This causes the agent to not be able to find the service and the resource remains in an UNKNOWN state. The instance name attribute for the default instance should be NULL. Manually making the change and restarting the vcsagmd service fixes the issue. [1190750]

Workaround: Locate the main.cmd file and the .SQLServer2000.main.cmd file at: %VCS_HOME%\conf\config. Type `set vcs_home` at the command prompt to find the value of %VCS_HOME%. For example:

```
C:\Documents and Settings\Administrator>set vcs_home
    VCS_HOME=C:\Program Files\Veritas\cluster server
```

The main.cmd file contains configuration information for agents. If SQL Server 2000 default instance on Windows 2000 is configured, find an entry similar to:

```
"modifyres SQLServer2000 MSSQLSERVER_SQLServer2000_SQL Instance str
hostName".
```

Remove hostname from last statement, the new statement is:

```
"modifyres SQLServer2000 MSSQLSERVER_SQLServer2000_SQL Instance
str"
```

Make sure there is no other change to this file. Save and close this file.

Re-start the vcsagmd service in the service control manager.

DNS entries not getting updated

The VMIP agent updates or replaces the virtual machines existing DNS entries with a new set of values. It cannot be used to add more DNS entries to the virtual machine. [1186611, 1191220]

For example, if a virtual machine has two DNS entries listed in the resolv.conf, but the VMIP agent attribute (*DNS of the exact name) has three listed, the VMIP agent only updates the first two entries listed in the attribute for the virtual machine.

Workaround: If you need VCS to update more DNS entries on the virtual machine, add them in /etc/resolv.conf manually, then they are updated during a failover by the VMIP agent.

Gateway attribute does not get updated on certain rhel4 virtual machines

The VMIP agent is not able to update the default gateway of certain virtual machines running RedHat Linux on a VCS disaster recovery failover. [1191220]

Workaround: To ensure that the VMIP agent is able to correctly update the gateway, make sure that the gateway setting is updated inside the /etc/sysconfig/network file, instead of the individual /etc/sysconfig/network-scripts/ifcfg-eth* files.

Windows 64-bit guest operating systems path redirection for VMIP and GrowFS agents

On Windows 2003 server 64-bit guest operating systems access to system commands is redirected from system32 to sysWOW64 for the VMIP and GrowFS agent for all 32-bit applications. [1186533]

Workaround 1: A Microsoft workaround is KB942589. Find it and an associated hotfix here: http://support.microsoft.com/kb/942589. The hotfix creates a NTFS junction from %SYSTEMROOT%\Sysnative to %SYSTEMROOT%\system32.

Workaround 2: In case the hotfix is not available, use the junction utility (available at http://www.microsoft.com/technet/sysinternals/FileAndDisk/Junction.mspx). Execute the following command after installing junction.exe inside of the guest operating system's file system:

install_path\junction.exe %SYSTEMROOT%\Sysnative %SYSTEMROOT%\system32

The monitor.pl entry points of the VMIP and the GrowFS agent for Windows guest OS will check the alternative Sysnative path for missing commands.

Version field for VCS VMware ESX license key may be set incorrectly

When the `vxlicrep` command is run, the version field for the Veritas Cluster Server (VCS) for VMware ESX license key may be set to an incorrect value of 7. This issue occurs only with license keys released with the 5.1 version of the VCS for VMware ESX product. [1115392]

Workaround: To determine the actual version of VCS installed on the cluster nodes, type the `had -version` command.

To confirm that the actual version of VCS 5.1 for VMware ESX is installed, verify that the following fields are set to these values.

```
Engine Version    5.1
Join Version      5.1.30.0
Build Date        Thu 03 Jan 2008 07:01:00 PM PST
PSTAMP            Veritas-5.1.30.0-01/03/08-19:01:00
```

Service group does not come online in some scenarios

This issue occurs if VCS is not running and the ExternalStateChange attribute of the ESXVirtualMachine resource has the OnlineGroup token. If you try to bring the service group online, VCS detects that the ESXVirtualMachine resource is online, but does not bring the service group online. [1110943]

Cannot add ISO image for virtual machines on some platforms

The Veritas Virtualization Manager does not support adding an ISO image for virtual machines on some platforms. On SLES 10 systems, Veritas Virtualization Manager mounts the ISO image meant for SLES 9 systems. [1185584]

See "Required patches for ESX 3.0.x systems running VCS 5.1" on page 11.

Workaround: Mount the correct ISO image using the VirtualCenter client. The images are available at /vmimages/tools-isomages.

VCS may report incorrect status of applications in some situations

This issue occurs if you attempt to configure a resource after intentionally stopping the corresponding application inside a virtual machine. The issue applies to agents that support detecting intentional offline of applications.

In this scenario, VCS incorrectly reports the status of the application as waiting to go online. [1109924]

Workaround: Flush the service group before attempting to bring it online again.

VCS does not support VMotion if ESX Server nodes are configured using IP addresses

VCS does not support running the `hagrp -migrate` command to trigger VMotion if you have configured ESX Server nodes in VMware VirtualCenter using IP addresses instead of fully qualified hostnames. You can run VMotion using the VirtualCenter client. [922540]

VCS does not detect Vmotion in a multi-VM environment

VCS does not support the migration of multiple virtual machines that are configured in a single service group. [789348]

Workaround: If you plan to migrate virtual machines, make sure that you configure a service group for each virtual machine.

Remote failover does not work with auto-generated MAC addresses

If you use auto-generated MAC addresses, switching service groups multiple times may cause the MAC address associated with the virtual machine to change. [850148]

Workaround: Do not use auto-generated MAC addresses. Assign static MAC addresses to virtual machines configured as VCS resources.

Set the MAC address by adding the following line to a virtual machine's configuration file:

```
ethernet0.addressType = "static"
ethernet0.Address = "00:50:56:XX:YY:ZZ"
```

Make sure you choose hex values that are unique among your hard-coded addresses to prevent conflicts between the automatically assigned MAC addresses and the manually assigned ones.

The values of XX must be between 00 to 3F.

The values of YY and ZZ must be between 00 to FF.

See the VMware documentation for more information.

Cannot configure disaster recovery if LUNs are in PSUS state

This issue applies to configurations that use Hitachi TrueCopy for replication.

If you have configured Shadow Image and the LUNs is in the PSUS state, the datastore gets imported on shadow LUNs and not on the original LUNs.

In this scenario, if you try to configure disaster recovery, Veritas Virtualization Manager displays a message saying the LUNs are not replicated.

Workaround: Follow this procedure:

1. Set /proc/vmware/config/LVM/EnableResignature = 1.
2. Rescan the storage from the Virtual Infrastructure Client.
   The datastore gets imported on the LUNS at the primary site.
3. Configure disaster recovery using Veritas Virtualization Manager.

Misleading error message when reversing the direction of replication

This issue occurs if you attempt to reverse the replication direction of arrays from the secondary site in a disaster recovery configuration. In a VCS environment, replicated arrays at the secondary site have read only permissions.

If you do try to reverse the direction of replication, VCS logs the following error:

```
There are no replicated LUNS on the clariion array
```

Workaround: Ignore the error. Symantec recommends that you do not attempt to reconfigure the arrays or reverse the direction of replication from the secondary site.

Misleading error message when running installvcsvm-tools

When you specify a device for the swap and page file location, installvcsvm-tools displays the following error. [896474]

```
No such file or directory
```

Workaround: Ignore the error. The utility completes the configuration successfully.

Erroneous message in the testVCConnect utility

The testVCConnect action entry point for the ESXVirtualMachine agent prints the following output when the connection to the VC Server is successfully established:

```
Successfully connected to the VirtualCenter Server
Error: Virtual Machine (/path/filename.vmx) not found in
repository
Successfully Disconnected to the VC Server
```

Workaround: Ignore the message about the virtual machine not being found in the repository. The following string indicates that the attributes are configured properly for the ESXVirtualMachine agent:

```
Successfully connected to the VirtualCenter Server
```

If any of the attributes are not configured correctly, the output of this action entry point will be a Java trace, similar to:

```
Exception in thread "main" AxisFault
 faultCode: {http://schemas.xmlsoap.org/soap/envelope/
}Server.userException
 faultSubcode:
 faultString: java.net.UnknownHostException:
DR51.enterprise.veritas.com
 faultActor:
 faultNode:
 faultDetail:
...
...
```

Misleading error message when running vcsag_config.pl

When you run the vcsag_config.pl utility to configure an agent, the utility adds a resource of type GuestOSApp to the VCS cluster and waits for the resource to get probed. The utility displays a message saying the resource is not probed. [1112757]

```
ERROR : Resource apache_vm1 is not getting probed on the ESX
cluster. Contact your ESX Server Administrator.
```

Workaround: Ignore the error. To verify that resources have been probed, run the following command:

```
[virtual-machine-prompt]# hares -display apache_vm1 |grep Probed
```

The command returns:

```
apache_vm1 Probed           esxnode1  1
apache_vm1 Probed           esxnode2  1
```

The value 1 indicates that resources have been probed.

Naming issue with VCS resources

In some situations, VCS resources display incorrect behavior when the resource name contains a 0 followed by another number. [851277]

Workaround: Rename the resource such that it does not include a 0 followed by a number.

Localized attributes not supported on Windows virtual machines

This release does not support configuring localized attributes for VCS resources in virtual machines running Windows. [794789]

Unexpected results with long switch names

The monitor agent function of the VSwitch agent may cause unexpected results when used to monitor switches with long names. [779190]

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.

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.

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 fail over within cluster %s and ClusterFailOverPolicy is set to %s. Administrative action is required.
50916	Unable to automatically fail over 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 fail over within cluster %s. However, group is still online/partial on one or more systems in the cluster
51033	Global group %s is unable to fail over within cluster %s and AutoFailOver is %s. Administrative action is required.

ESX local host credentials file may need to be regenerated

The ESXHost agent, the replication agents, and the firedrill agents use the ESX local host credentials file. The ESX local host credentials file is generated by the VCS installer for authentication and is required to use the VMware SDK interface.

If the ESX local host credentials file is accidentally deleted or corrupted, you may need to regenerate this file. [1141366]

Workaround: Before running this command, ensure that you back up the following files:

- `/etc/VRTSvcs/conf/config/main.cf`
- `/etc/VRTSvcs/conf/config/types.cf`

Regenerate the ESX local host credentials file by running the following command at /opt/VRTSvcs/bin:

```
# installvcs -configure
```

After running this command, restore the backup files.

Issues related to VCS Management Console

Replication information on the IBM MetroMirror agent does not appear in the VCS Management Console UI

Information on the IBM MetroMirror agent replication does not appear in the VCS Management Console 5.1 user interface. Use the VCS management console to manage an IBM MetroMirror resource. You may not get additional information regarding the state and details of replication in the user interface. [1171325] [1187155]

Issues related to virtual machines running Windows

Configuration wizards require VCS_HOME to be set correctly

If the VCS_HOME environment variable is not set or is set incorrectly in a Windows virtual machine, the VCS configuration wizards may not work correctly. [1112622]

Workaround: Reboot the virtual machine. If that does not solve the problem, reinstall Veritas Virtual Machine Tools in the Windows virtual machine and reboot the virtual machine.

SQL Configuration wizard requires all SQL Server instances to be running

Before running the SQL configuration wizard, make sure that all SQL instances are running. If all instances are not running, the configuration wizard may not correctly detect one or more instances. [1112400]

Issues related to Veritas Virtualization Manager (VVM)

VVM does not configure disaster recovery for virtual machines already configured for high availability

If a virtual machine is configured for HA, VVM does not configure disaster recovery. It displays a message that the virtual machine is already configured for high availability.

Workaround: Delete the existing service group and then configure for disaster recovery. [1190226]

VVM does not detect missing ISO files

If ISO files for the guest virtual machine are missing on host, in some situations, VVM does not detect that the files are missing. [1001263]

Workaround: Restore the missing ISO files from the product media. The ISO files are located at the following path /cluster_server/vcsvm_tools.

Copy the ISO images to the following directory on the ESX Server /vmimages/tools-isoimages.

Veritas Virtualization Manager requires Java Access Bridge

Veritas Virtualization Manager displays errors when run on a system that does not have the Java Access Bridge installed. [1087820]

Workaround: Download and install the Java Access Bridge from http://java.sun.com/products/accessbridge/

Issues related to fire drill

When running a fire drill, a different virtual machine may boot up

This issue occurs if the configuration has a a single datastore that contains multiple virtual machine configuration files.

In this scenario, when running a fire drill, VCS detects an incorrect virtual machine configuration file, which leads to the wrong virtual machine getting booted on the system.

Workaround: Configure the correct CfgFile attribute of the ESXVirtualMachine resource and bring the ESXVirtualMachine resource online manually.

Firedrill automation works incorrectly when a datastore contains multiple virtual machines

This issue occurs when the firedrill automation incorrectly detects only the first vmx file from the datastore generated as a result of the snapshot. This affects both EMC Mirrorview and Hitachi TrueCopy agents. [1114535]

Workaround: You must manually correct the attribute of the ESXVirtualMachine resource in the configuration file and bring the firedrill service group online.

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 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.

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 the highest priority cluster as a failover target

When a global cluster fault occurs, the Declare Cluster dialog enables you to fail over groups 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.

Issues related to the Oracle agent

Health check may not work

If you set the MonitorOption attribute 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 the value of the MonitorOption attribute to 0 to continue monitoring the resource.

Health check does not work in a csh environment

Health check monitoring is not supported for the csh shell.

Fixed issues

The following section discusses fixed known issues in VCS 5.1 MP1, and in previous releases.

Issues fixed in VCS 5.1 MP1

The following issues are fixed in this release of VCS.

1104350	Fire drill resource fails due to incorrect pairdisplay output
612587	The haclus -wait command hangs when cluster name is not specified.
1119239	VMIP guest operating system agent fails to configure VMIP correctly on SLES VM
1114612	Intermittent error messages thrown by the ESXHost agent
1123062	Online timeout of one VMIP resource when multiple VMIPs are configured on a single VM.

See “Changes in this release” on page 6.

Issues fixed in VCS 5.1

The following issues were fixed in VCS 5.1.

855817	Issue with the Browse button in the SQL Agent Configuration wizard.
838275	ESXVirtualMachine agent may not detect virtual machine fault
764018	Virtual machine may remain in a stuck state during boot process Switching a service group that contains ESX virtual machine resources may not work.
898182	Newly-added disk not detected by virtual machine running Windows.
793819	GuestOSApp agent may fault during VMotion

Documentation

Symantec recommends copying 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 Implementation Guide	`vcs_implementation.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 Agent for EMC MirrorView Configuration Guide	`vcs_mirrorview_config.pdf`
Veritas Cluster Server Agent for Hitachi TrueCopy Configuration Guide	`vcs_truecopy_config.pdf`
Veritas Cluster Server Agent for IBM MetroMirror Configuration Guide	`vcs_metromirror_config.pdf`
Veritas Cluster Server Application Note: SRDF replication in a VCS for VMware environment	http://entsupport.symantec.com/docs/295185

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 errata

Veritas Cluster Server User's Guide

The accompanying documentation includes information about the following features that are either unsupported or not shipped with this release:

- I/O fencing
- Symantec Product Authentication Service
- Replicated data clusters (RDC)

Veritas Cluster Server Implementation Guide

VCS agent for Oracle

On page 180, the Agent functions for VCS agent for Oracle has wrong information about the default basic monitor option.

The default basic monitor option is health check monitoring and the value of MonitorOption attribute is set to 1 by default. The intentional offline functionality is enabled only with the default health check monitoring.

Mount agent

The AccessPermissionChk attribute for the Mount agent is not supported for 5.1 MP1.

Documentation addenda

The Veritas Cluster Server Implementation Guide, Communication between GuestOSApp and application agents on virtual machines

The GuestOSApp agent that runs in the ESX Server layer must communicate with the application agents that run in virtual machines. The Application agent monitors the application that runs in the virtual machine and indicates its state to the VCS Agent Management Daemon (vcsagmd) on the virtual machine.

In case of a change in the state of the application, vcsagmd reports it to VMware's guestinfo interface. The GuestOSApp resource monitors the VMware guestinfo interface for any change in the state of the application and reports this to VCS that runs on the ESX Server layer. VCS on the ESX Server layer takes the appropriate action depending on the state change reported.

If state changes are not reflected, make sure the resource name used for the application inside the virtual machine does not have a 0 followed by another number.

You can test VMware's guestinfo interface by requesting guest information from the virtual machine:

In Windows:

```
[C:\program files\vmware\vmware tools\] vmwareservice.exe --cmd
"info-set guestinfo.mytest1 myvale1"
```

In Linux:

```
[/usr/sbin/] vmware-guestd --cmd "info-set guestinfo.mytest1
myvale1"
```

Read the above guest information from the ESX host where the virtual machine is online.

```
vmware-cmd path_to_vmx_config_file getguestinfo mytest1
```

Run the following command on the ESX node where the virtual machine is online to obtain the state of the application:

```
/opt/VRTSvcs/bin/hares -action GuestOSApp-resource getappstate \
-sys sysA
```

This provides the following information in the given order:

- The state of the resource as reported by the agent running inside the virtual machine
- The contents of the vcsagmd heartbeat file, which tells you whether the vcsagmd heartbeats are functioning properly or not
- The current vcsagmd heartbeat value

If vcsagmd heartbeats are not updated, check the virtual machine to see if vcsagmd was stopped for maintenance and never restarted. Also, check if the Veritas Virtual Machine Tools package was upgraded to the current version.

You may check the vcsagmd log file at the following locations to verify if the agents inside the virtual machine report the state to vcsagmd.

- /var/VRTSvcs/log/vcsagmd_A.log
- C:\Program Files\VERITAS\cluster server\log\vcsagmd_A.txt
- For Windows 2003 64bit:
  C:\Program Files(x86)\VERITAS\cluster server\log\vcsagmd_A.txt

The Veritas Cluster Server Bundled Agents Reference Guide, ESXVirtualMachine agent

The ESXVirtualMachine agent detects when an operating system crashes, and initiates the node failover.

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.

Third-party legal notices

Certain third-party software may be distributed, embedded, or bundled with this Symantec product, or recommended for use in conjunction with Symantec product installation and operation. Such third-party software is separately licensed by its copyright holder.

For the license agreements that govern the use of third-party software and its copyright holder's proprietary notices, see vcs_third-party_copyrights.pdf in the docs directory of the software disc.

Use of the third-party software must be in accordance with its license terms. Symantec makes no representation or warranty of any kind regarding such third-party software. Symantec offers no support for such third-party software and shall have no liability associated with its use.

Getting help

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.