

Veritas Storage Foundation™ and High Availability Solutions Release Notes

Windows Server 2003, Windows Server
2008

5.1 Service Pack 2

Veritas Storage Foundation™ and High Availability Solutions Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Product version: 5.1 Service Pack 2

Document version: 5.1.SP2.3

Legal Notice

Copyright © 2012 Symantec Corporation. All rights reserved.

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

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. See the Third-party Legal Notices document for this product, which is available online or included in the base release media.

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

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

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

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

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Documentation

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

doc_feedback@symantec.com

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan

customercare_apac@symantec.com

Europe, Middle-East, and Africa

semea@symantec.com

North America and Latin America

[supportolutions@symantec.com](mailto:supportsolutions@symantec.com)

Release Notes

This document includes the following topics:

- [Introduction](#)
- [New features and changes in release 5.1 SP2](#)
- [New features and changes in release 5.1 SP1AP1](#)
- [New features and changes in release 5.1 SP1](#)
- [New features and changes in release 5.1 AP1](#)
- [New features and changes in release 5.1](#)
- [Application support](#)
- [Requirements](#)
- [No longer supported](#)
- [Installation notes](#)
- [Software limitations](#)
- [Known issues](#)
- [Software fixes and enhancements in 5.1 SP2](#)
- [Software fixes and enhancements in 5.1 SP1AP1](#)
- [Software fixes and enhancements in 5.1 SP1](#)
- [Software fixes and enhancements in 5.1 AP1](#)
- [Software fixes and enhancements in 5.1](#)
- [Documentation changes](#)

- [Veritas Storage Foundation for Administrator's Guide](#)
- [Documentation](#)
- [Acronyms](#)

Introduction

This document provides important information regarding the following two products included in Veritas Storage Foundation and High Availability Solutions 5.1 SP2 for Windows:

- Veritas Storage Foundation™ 5.1 SP2 for Windows (SFW)
- Veritas Storage Foundation™ HA 5.1 SP2 for Windows (SFW HA)

Please review this entire document before using SFW or SFW HA.

The information in the Release Notes supersedes the information provided in the product documents. You can download the latest version of this document from the Symantec Support website.

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

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

General information regarding Veritas Storage Foundation and High Availability Solutions for Windows is available on the Symantec website.

<http://www.symantec.com>

For information about Microsoft certification for Veritas Storage Foundation, see the *Veritas Storage Foundation 5.1 for Windows Service Pack 2 WinLogo Certification Readme* file. This `Readme` file is included with the SFW product documentation on the product media.

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

<http://www.symantec.com/docs/TECH138722>

For the latest updates to array support and for supported hardware configurations, see the Hardware Compatibility list (HCL) at

<http://www.symantec.com/docs/TECH138719>

New features and changes in release 5.1 SP2

This section describes the new features and changes introduced in Veritas Storage Foundation for Windows (SFW) and Veritas Storage Foundation HA for Windows (SFW HA) 5.1 Service Pack 2.

SFW and SFW HA 5.1 SP2 incorporate software updates and features that were introduced in SFW and SFW HA 5.1 SP1, and SFW HA 5.1 SP1AP1 release. This release also includes the technical support software updates (hotfixes) that were available before this release for the 5.1, 5.1 SP1, and 5.1 SP1AP1 releases.

For information about the new features and changes in release 5.1 SP1AP1:

See [“New features and changes in release 5.1 SP1AP1”](#) on page 14.

For information about the new features and changes in release 5.1 SP1:

See [“New features and changes in release 5.1 SP1”](#) on page 16.

General Support

The following are general enhancements for SFW HA 5.1 SP2.

Support for Microsoft SharePoint Server 2010

Support for Microsoft SharePoint Server 2010 includes the following:

- SFW supports VSS-based backup and restore operations for SharePoint Server 2010 databases. SFW uses the Veritas FlashSnap solution for SQL Server that provides the capability to quiesce the SQL databases and create persistent snapshots of SharePoint configuration and farm databases.

Refer to the *Veritas Storage Foundation Administrator's Guide* for more information.

- SFW HA supports HA and DR configurations for Microsoft SharePoint Server 2010. High availability support involves monitoring and recovery support for SharePoint 2010 applications and high availability support for SQL Server databases used by SharePoint Server 2010. VCS provides a new agent for SharePoint Server 2010 that monitors the Web Applications, Service Applications, and services configured in the SharePoint Server farm. VCS also provides a new configuration wizard for configuring SharePoint Server 2010 service groups.

Refer to the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for SharePoint Server 2010* for more details.

- The Solutions Configuration Center (SCC) now includes a separate workflow for configuring high availability, disaster recovery, and quick recovery for

SharePoint Server 2010. The online help and PDF files in the Solutions Configuration Center include documentation for SharePoint Server 2010 solutions.

Support for Microsoft SQL Server 2008 R2

Support for Microsoft SQL Server 2008 R2 includes the following:

- SFW supports VSS-based backup and restore operations with SQL Server 2008 R2. It includes support for FILESTREAM enabled database objects.
- SFW HA supports HA and DR configurations for SQL Server 2008 R2. Use the existing VCS SQL Server 2008 agents to configure both SQL Server 2008 and SQL Server 2008 R2. The VCS SQL Server 2008 Configuration Wizard is enhanced to support selection of the SQL Server version during configuration. Use the wizard to configure service groups for both SQL Server 2008 and SQL Server 2008 R2.

Refer to the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL 2008 and SQL 2008 R2* for instructions on how to configure a new HA and DR environment for SQL 2008 and SQL Server 2008 R2.

- The Microsoft SQL Server tab of the Symantec Solutions Configuration Center supports SQL Server 2008 R2 solutions. The SQL Server 2008 Configuration Wizard can be launched from the Solutions Configuration Center to configure SQL Server 2008 and SQL Server 2008 R2 service groups. The online help and PDF files in the Solutions Configuration Center include documentation for SQL Server 2008 and SQL Server 2008 R2 solutions.

Enhancements to the Solutions Configuration Center

The Storage Foundation and High Availability Solutions Configuration Center (SCC) guides you through setting up your SFW HA environment and setting up Quick Recovery.

For this release, the following new solutions have been added to the SCC for SharePoint Server 2010

- High availability
- Disaster recovery
- Quick Recovery

Veritas Storage Foundation

DMP and DSM changes for Storage Foundation for Windows (SFW) Device Driver Integration-1 and Device Driver Integration -2 are as listed below:

New additions to the DSMs/Arrays are for DMP DSM Support (VSUN) for the SUN arrays (7x10 and 7x20 series). Have added support for HP P2000 arrays in VHPMSA2.

Table 1-1 New SUN arrays and related product IDs

Vendor ID	Product ID
SUN	Sun Storage 7410
SUN	Sun Storage 7310
SUN	Sun Storage 7210
SUN	Sun Storage 7110
SUN	ZFS Storage 7420
SUN	ZFS Storage 7320
SUN	ZFS Storage 7220
SUN	ZFS Storage 7120

Added support for HP P2000 arrays in VHPMSA2 (Incident 2064153).

Table 1-2 New HP arrays and related product IDs

Vendor ID	Product ID
HP	P2000 G3 FC
HP	P2000 G3 SAS
HP	P2000 G3 iSCSI
HP	P2000G3 FC/iSCSI

New additions to the Device Driver Package (DDI-1 and DDI-2) and their related versions added to the 5.1 SP2 release package are as listed below.

Table 1-3 New arrays added to the DDI installer package and their related versions

Arrays	Versions
vcomplnt.sys	5.1.11000.0
vhuaweiap.sys	5.1.11000.0
vengap.sys	5.1.10000.553
vsun.sys	5.1.21000.5
vhpmsa2.sys	5.1.21000.3
vibmaads.sys	5.1.21000.3
vxiv.sys	5.1.21000.3

Veritas Cluster Server

This section describes the VCS changes and enhancements in this release.

Improved failover performance of cluster disk groups when used with VCS

The failover performance of cluster disk groups is enhanced by modifying the following:

- Performance improvement in SFW components
 - Nullified the time lapse for volume arrival while importing disk groups
 - Removed redundant operations performed by VCS during offline
- Performance improvement in VCS VMDg and MountV agents
 - Optimized the number of calls made to SFW components
 - Removed wait for monitor after online and offline operations
- Fixed the "Application Error" issue in VxBridge service

The MountV agent retrieves the state of the volumes, whether missing or unusable, from Volume Manager. On 64-bit systems, this information is routed using the VxBridge service. If the number of volumes in the unusable state exceeds five or more, the VxBridge service may crash with an "Application Error" message. This VxBridge service crash may lead to error conditions in the MountV agent. This fix handles the crash in the VxBridge service.
- Reduction in the failover time after storage fault is now detected

- Resolved the VDS and MPIO errors
- Fixed the MountV resource faults (ERROR_DIR_NOT_EMPTY) that were caused during service group failback
- Fixed memory leak in VMDg agent
- Optimized the MountV online and offline operations by performing the following:
 - Used online and offline volume IOCTLs in MountV agent
 - Removed volume locking and dismounting from DG deport operation

Changes to SQL Server 2008 agent

The SQL Server 2008 Database Engine agent is enhanced to address an issue where SQL databases are not accessible after service group failovers if the user account specified for the SQL services (SQL Server service, SQL Server Agent service) does not have local administrator privileges on all the cluster nodes that are part of the SQL service group.

A new optional attribute called SQLClusterAccount is added to the SQL Server 2008 Database Engine agent. Use this attribute if the SQL Server services account is not a member of the local Administrators group on the cluster nodes in the service group. You can specify either a domain group or the SQL Server service name for this attribute. The agent assigns this account with Full Control privileges to the SQL Server databases and log files. You can specify this attribute while configuring the SQL Server service group using the VCS SQL Server 2008 Configuration Wizard.

New attribute for the MountV agent

The MountV agent's CheckFSAccess function is now available in the form of an attribute. A new optional attribute, CheckFSAccess, is added to the MountV agent. Use CheckFSAccess to enable or disable MountV agent's file system check on volumes mounted using SFW.

Note: The MountV agent's CheckFSAccess action function is deprecated.

Support for configuring up to eight private network links for LLT

The VCS Cluster Configuration Wizard (VCW) now supports configuring up to eight private network links for LLT over Ethernet or LLT over the User Datagram Protocol (UDP) layer.

To configure the network links for LLT over UDP, use the Edit Ports button on the Private Network Configuration panel of the wizard to specify the UDP ports for the links.

Support for removing the faulted node from a cluster

While removing a node from a cluster, if the validation checks failed for the node you wanted to remove, you were required to rectify the cause of failure and then proceed to remove the node. However, VCS Cluster Configuration Wizard now enables you to remove the failed node, without rectifying the cause of failure.

Note: You must proceed to remove the failed node only if the node is permanently unavailable, due to any hardware or Operating System related issues, that can be resolved only by reinstalling the Operating System.

New features and changes in release 5.1 SP1AP1

This section describes the changes introduced in Veritas Storage Foundation for Windows (SFW) and Veritas Storage Foundation HA for Windows (SFW HA) version 5.1 SP1 Application Pack 1.

New application version support

This release provides support for the following new application versions:

- Microsoft Exchange Server 2010
 - SFW supports VSS-based backup and restore operations with Exchange Server 2010.
Refer to the *Veritas Storage Foundation and High Availability Solutions Quick Recovery Solutions Guide for Microsoft Exchange 2010*.
 - SFW HA supports HA and DR configurations for Exchange Server 2010.
Refer to the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange 2010 to configure a new HA and DR environment for Exchange 2010*.
 - The Microsoft Exchange Server tab of the Symantec Solutions Configuration Center supports Exchange Server 2010 solutions. The Exchange Server 2010 Configuration Wizard can be launched from the Solutions Configuration Center to configure Exchange Server 2010 service groups. The online help and PDF files in the Solutions Configuration Center include documentation for Exchange Server 2010 solutions.

Veritas Cluster Server

Microsoft Exchange Server 2010 support

This release provides High Availability (HA) and Disaster Recovery (DR) support for Exchange 2010. High availability support for Exchange 2010 is available for Exchange 2010 mailbox databases. VCS provides a new database agent for Exchange 2010 that monitors the mailbox databases configured on shared storage. VCS also provides a new configuration wizard for configuring the Exchange 2010 database service group.

Refer to the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange 2010* for more details.

hagetcf utility support for Exchange 2010

The VCS `hagetcf` utility can be used to retrieve and write detailed diagnostic information about the Exchange 2010 configuration in VCS. The `-exch` command line option can be used to get detailed information about Exchange 2010 in the VCS cluster configuration.

See the *Veritas Cluster Server Administrator's Guide* for more details about `hagetcf`.

VCS Exchange 2010 management pack for SCOM 2007

VCS provides a management pack for Exchange 2010. You can use this management pack to monitor Exchange 2010 instances configured under VCS in a Systems Center Operations Manager (SCOM) 2007 monitoring environment. This management pack is supported on SCOM 2007 SP1 and R2 versions.

MountV agent changes

The VCS MountV agent supports folder mounts on local system disks. You can mount shared disks on local system drives using folder mounts. The VCS MountV agent is modified such that during failover, the agent creates the folder mount directories, if they do not exist on the target node.

For example, a shared disk is mounted as Mydata on a system drive (C:\). The path of the mount is now C:\Mydata. When the MountV agent is failed over to another node, it creates the folder Mydata, if it does not exist on that node, and then mounts it on C:\ on that node.

Exchange 2010 service group configuration wizard enhancement

VCS provides a new configuration wizard, the Exchange 2010 Configuration Wizard, for configuring Exchange 2010 database service groups.

This wizard detects shared disks that are mounted as folder mounts on the local system drives. You can mount shared drives as folder mounts on local system drives and then configure the folder mounts in the Exchange database service group.

Co-existence with Symantec Mail Security for Microsoft Exchange

You can install Symantec Mail Security for Microsoft Exchange (SMSMSE) version 6.5.0.67 in an environment where Microsoft Exchange 2010 is configured with VCS. VCS does not affect the SMSMSE functionality.

However, VCS does not provide HA support for SMSMSE itself.

Note the following:

- If you are installing SMSMSE on systems where VCS is already installed, then the SMSMSE installer prompts whether you wish to register the cluster resource components. Do not register the cluster components. Select No when prompted for the registration.
- If you have already installed SMSMSE and registered the cluster resource components in a VCS environment, then ensure that you do not configure the SMSMSE cluster resource in an environment where Exchange 2010 is configured with VCS. Such a configuration is not supported.

New features and changes in release 5.1 SP1

This section describes the new features and changes in 5.1 SP1.

This section describes the new features and changes introduced in Veritas Storage Foundation for Windows (SFW) and Veritas Storage Foundation HA for Windows (SFW HA) 5.1 Service Pack 1.

SFW and SFW HA 5.1 SP1 incorporate software updates and features that were introduced in the SFW and SFW HA 5.1 AP1 release, as well as any technical support software updates (hotfixes) that were available before this release for the 5.1 and 5.1 AP1 releases.

For information about the new features and changes in release 5.1 AP1:

See [“New features and changes in release 5.1 AP1”](#) on page 27.

For information about the new features and changes in release 5.1:

See [“New features and changes in release 5.1”](#) on page 29.

General support

The following are the general support new features and changes in release 5.1 SP1.

New DMP DSM support

This release provides support for the following additional DMP DSMs:

- 3PARDATA (V3PARAA)
- Dell EqualLogic array (VEQLOGIC)
- HP 2000 array (VHPMSA2)
- IBM DS AP (VIBMAPDS)
- IBM XiV Storage System (VXIV)
- HUAWEI S5300/S2300 array (VHUAWEIAP)
- FUJITSU ETERNUS 2000 array (VFUJITSUAA)
- NETAPP (VNETAPP)
- PILLAR (VPILLAR)
- WindowsStorage Server 2003R2iSCSI (VITARGET)
- XioTech Array (VXIOTECH)

For a complete list of supported DMP DSMs, see the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide*.

SFW Basic embedded license

SFW Basic has an embedded license key. You do not have to enter a license key to run SFW Basic.

Microsoft Windows Server 2008 R2 support

This release provides support for Microsoft Windows Server 2008 R2.

For additional information:

See [“Operating system requirements”](#) on page 45.

Microsoft Windows Server Core support

This release provides support for Microsoft Windows 2008 Server Core, Windows 2008 SP2 Server Core, and Windows 2008 R2 Server Core.

Microsoft Windows Client support

This release provides support for client components on the following operating systems:

- Windows XP SP3
- Windows 7

For additional information:

See [“Operating system requirements”](#) on page 45.

New application version support

This release provides support for the following new applications and application versions:

- Exchange 2007 SP2
- SQL Server 2008 SP1
- SQL Server 2005 SP3
- Enterprise Vault 8.0 SP1, SP2, and SP3
- SharePoint Server 2007
- BlackBerry Enterprise Server 4.1.5
- Oracle 11g on Windows Server 2003 and 2008 (x86 and x64)

Note: This release does not support Oracle 11g on Windows Server 2008 R2.

For additional information:

See [“Application support”](#) on page 35.

Enhancements to the Fire Drill Wizard

The Fire Drill Wizard, launched from the SFW HA Solutions Configuration Center, now supports configuring and running a fire drill in the following replication environments:

- Hitachi TrueCopy

- EMC SRDF

Enhancements to the Solutions Configuration Center

The SFW HA 5.1 SP1 Solutions Configuration Center (SCC) contains the following enhancements:

- A disaster recovery (DR) workflow has been added for Enterprise Vault Server.
- The **Solutions** tab contains additional buttons to launch the following wizards:
 - MSDTC Server Configuration Wizard configures an MSDTC Server service group.
 - MSMQ Configuration Wizard configures a Microsoft Message Queuing service group.
- A launch button has been added for VCS Application Manager (VAM) utility.

Installation

The following are the new features and changes for the installation process in release 5.1 SP.1.

New Configuration Checker features

The Configuration Checker has been updated with the following new features:

- Configuration Checker can now be run using a command line interface, in addition to using the Configuration Checker wizard.
- Symantec's Veritas Operations Services (VOS) now incorporates Configuration Checker features into VOS for Windows. The Configuration Checker, which is part of the Symantec product installer for SFW or SFW HA 5.1 SP1 now also produces a VOS formatted result file (`vos_results.xml`). You can run the Configuration Checker and upload the results file to the VOS website for analysis and report creation.

For additional information about VOS:

<https://sort.symantec.com/home>

- Configuration Checker now reports on whether the host for SFW or SFW HA is a virtual machine. The Configuration Checker reports and ensures compliance when running SFW or SFW HA in the following virtualized environments:
 - VMware guest
 - Hyper-V guest

After being identified as one of the type guests, the Configuration Checker then directs the user to technical notes on the Symantec support site describing the best-practices for running SFW or SFW HA in a virtualized environment.

- Configuration Checker reports on host files.
Configuration Checker now checks whether the contents of the hosts file in System drive\Windows\System32\drivers\etc has been modified and warns the user to verify the hosts file entries.

SFW HA supports Oracle agent for Windows Server 2008

SFW HA 5.1 SP1 now supports an Oracle agent for Windows Server 2008.

Note: This new Oracle agent is not supported on Windows Server 2008 R2 and Windows 2008 Server Core.

Windows Server 2008 to Windows Server 2008 R2 or SP2 upgrade is supported

This product release supports a Windows Server 2008 to Windows Server 2008 R2 or SP2 upgrade. For information about installing or upgrading to SFW or SFW HA 5.1 SP1, when upgrading Windows Server 2008 to Windows Server 2008 R2 or SP2, see the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide*.

Veritas SFMH component is installed by default

During an SFW or SFW HA 5.1 SP1 installation or upgrade, the SFMH component is installed by default.

Veritas Storage Foundation Manager (SFM) enables operations teams to manage Veritas Storage Foundation and related operations across all platforms from a centralized management framework. It provides information about the environment, focusing on the administration of server and storage infrastructure resources from the application perspective. SFM improves the productivity of server teams and availability of application and storage.

For additional details about SFM:

<http://www.symantec.com/business/storage-foundation-manager>

New Enterprise Vault Option

There is a new Enterprise Vault (EV) Cluster Setup Wizard installation option available from the product installer.

New option to replace Disk Management Snap-in

There is a new option available in the product installer or using the command line interface to replace the Disk Management Snap-in in the Windows Computer Management console and the Server Manager console with the Veritas Enterprise Administrator GUI for Windows Server 2008.

For additional information about this option, see the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide*.

Veritas Storage Foundation

The following are the new features and changes for Veritas Storage Foundation in release 5.1 SP1.

Summary of new features

The following is a summary list of new features for SFW for release 5.1 SP1:

- Capacity Monitoring configuration is available and enabled for all nodes in a cluster.
- Implementation of a VDS plug in to handle both Microsoft Disk Management disk groups and SFW disk groups under VDS.
- Support for conversion of Microsoft Disk Management disk groups to SFW disk groups.
- DMP MPIO support for advanced A/A load balancing for A/PC arrays.
- DMP MPIO support for ALUA enabled arrays.
- Integrated Flashsnap support for Microsoft SharePoint 2007.
- Support for Microsoft Systems Center Operations Manager 2007 R2.
- Support for Microsoft Windows Server 2008 R2.
- Integrated Flashsnap support for Enterprise Vault.
- Support for Microsoft Copy on Write (COW) snapshots.
- Integrated thin provisioning capability for storage efficiency

Note: Symantec maintains a Hardware Compatibility List (HCL) for SFW on the Symantec Support web site. Check the HCL for details about supported storage arrays enabled for thin provisioning.

Snapshot enhancement

The default naming convention for snapshot volumes has been changed to avoid duplicate volume names. Default naming of snapshot volumes begin with “SnapV” followed by a 12 character alphanumeric string. The 12 character alphanumeric string is a coded hexadecimal timestamp based upon the time that the snapshot was taken. The following is an example of a snapshot volume name:

```
SnapV4A7337AE038A
```

Veritas Cluster Server

The following are the Veritas Cluster Server new features and changes in release 5.1 SP1.

Oracle 11g Release 1 support

This release includes high availability support for Oracle 11g Release 1. Use the VCS Oracle agent to make Oracle 11g Release 1 databases highly available in a VCS environment.

Refer to the *Veritas Cluster Server Database Agent for Oracle Configuration Guide* for more details.

Note: This release does not support Oracle 11g on Windows Server 2008 R2.

Wizard for configuring MSMQ service group

VCS now provides a wizard that you can use to configure Microsoft Message Queuing (MSMQ) service groups. You can launch the wizard from the Solutions Configuration Center (SCC).

VCS Application Manager (VAM) utility

VCS provides a new utility, VCS Application Manager (VAM), that lets you manage applications in the virtual server context. Use VAM to launch application management tools and system management tools in the virtual server context.

You can launch the VAM utility from the Windows Start menu. (click **Start > Programs > Symantec > Veritas Cluster Server > Configuration Tools > Application Manager**)

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

VCS HAD Helper Service user account privileges modified

The privileges required by the VCS HAD Helper service user account have been modified. The hadhelper utility now does not assign the following privilege to the VCS helper service user account:

- Increase scheduling priority

Process agent changes

A new attribute, LanmanRename, is added to the Process agent. You can use this attribute to configure the agent to monitor processes in the context of the virtual name specified in the Lanman resource.

PrintShare agent changes

The PrintShare agent is modified to retain the comments that were added to the printers. When the printers are added to the print share service group, VCS retains the comments and adds a VCS tag to it.

Enhancements in FileShare and CompositeFileShare agents

The FileShare and CompositeFileShare agents are modified to include the following changes:

- Support for the Windows access-based enumeration option is added to the agents. The File Share Configuration Wizard provides options to enable or disable access-based enumeration.
- The File Share Configuration Wizard now includes option to define the value of the attribute Client Cache Type.
- A new function, ForceControl, is added to the agents. You can use ForceControl to restore the properties of file shares as per what is defined in the VCS configuration. The agent overwrites all changes made to the file share properties, irrespective of whether they were made externally or from within VCS, and resets them to what is defined in the VCS configuration. .
- The AutoControl attribute is modified. You can now use this attribute to define the agent behavior when share properties are modified when the FileShare or CompositeFileShare resource is online.
- The IgnorePermissions attribute is deprecated. You can use the AutoControl attribute instead..
- A new attribute, ShareComment, is added to the agents. You can use this attribute to add comments to the file share resource

See the *Veritas Cluster Server Bundled Agents Guide* for more information about the FileShare and CompositeFileShare agents.

See the *Veritas Cluster Server Administrator's Guide* for more information about the File Share Configuration Wizard.

VCS Exchange Server Setup Wizard changes

While installing Exchange 2003 in a VCS environment, the VCS Exchange Server Setup Wizard performs certain operations on the Exchange Domain Servers object in Active Directory (AD). The wizard uses the logged-on user account context to perform these AD operations; therefore the logged-on user account is required to have the privileges to update AD objects.

AD update privileges are generally assigned to Domain Administrators and this may create a problem in environments where there are security restrictions on the privileges available to users in the domain.

The VCS Exchange Server Setup Wizard is now modified to use either the logged-on user account context or the VCS Helper Service user account context to perform the required AD updates. The wizard uses the VCS Helper Service account if the logged-on user account does not have the required privileges.

Note that for the wizard to perform the AD operations using the VCS Helper Service user account, the Exchange Domain Servers object in the AD must be managed by the VCS Helper Service user account (**Managed By** tab on the **Object Properties** window).

Support for provisioned Exchange Server 2007 installations

Provisioning a server allows Exchange to be installed later by using delegated setup. This procedure allows a delegated account to install Exchange Server in the domain without being a member of the Exchange Organization Administrators group.

This release supports Exchange Server 2007 installations performed by delegated account.

Microsoft VHD support

This release is qualified on operating systems running on physical (hosts) and virtual (guests) machines based on Microsoft's Virtual Hard Disk (VHD) virtualization file format.

MountV agent changes

The MountV agent is modified to include the following changes:

- The MountV agent's CheckFSAccess function has been enhanced to allow granular control on the behavior of MountV resources.
- The behavior of the ForceUnmount attribute is modified. Depending on the attribute value, the agent unmounts the volumes either gracefully or forcefully, irrespective of the type of access applications have on the volumes.
- The default value of the attribute ListApplications is now set to 1. While unmounting the volume, the agent lists all the applications that are accessing it.
- The default value of the attribute AutoFSClean is now set to 1. If the agent detects corruption, it runs the Chkdsk /X command to clean the file system on the volume that is being brought online.

Refer to the *Veritas Cluster Server Bundled Agents Guide* for more information.

Enhancements to the VCS GAB module

The VCS Global Automatic Broadcast (GAB) module is enhanced to include the registration monitoring feature. You can use this feature to configure the GAB behavior when the VCS High Availability Engine (HAD) is terminated and fails to respond within the specified time interval.

When both HAD and the hashadow processes fail to respond, the registration monitoring timer initiates. The registration monitoring timer is defined by the VCS_GAB_RMTIMEOUT environment variable. If HAD does not respond within the specified time interval, GAB can either log a message or panic the system, depending on the value defined in the VCS environment variable VCS_GAB_RMACTION.

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

BlackBerry, VirtualCenter, and MSMQ service group templates for Cluster Manager (Java Console)

Service group configuration templates are now available for the following applications:

- BlackBerry Enterprise Server (BlackBerryVMGroup)
- Microsoft Message Queuing (MSMQVMGroup)
- VMware VirtualCenter (VirtualCenterGrp)

These templates are installed at %vcs_home%\templates directory.

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

Launch the Service Group Configuration Wizard (**Tools > Configuration Wizard**) from the Cluster Manager (Java Console) and use these templates to configure the respective application service groups.

In addition, a service group configuration template for VMware vCenter 4.0 is downloadable, along with *Veritas Cluster Server Application Note: High Availability for VMware vCenter Server*, from the following Support Tech Note:

<http://www.symantec.com/docs/TECH76479>

Updates to the MirrorView agent

The MirrorView agent now supports the use of both navicli.jar and naviseccli to manage replication. The agent supports consistency groups for synchronous replication.

On Windows Server 2008 systems, add the system user “<HOSTNAME>\$” as a privileged array user for MirrorView operations using navicli or naviseccli. The attribute MirNames is a scalar attribute. If your configuration has more than one mirror, use the GrpName attribute to configure the consistency group.

VCS SQL Server 2008 management pack for SCOM 2007

VCS provides a management pack for SQL Server 2008. You can use the management pack to monitor SQL 2008 instances configured under VCS in a Systems Center Operations Manager (SCOM) 2007 monitoring environment.

This management pack is supported on SCOM 2007 SP1 and R2 versions.

Contact Symantec Technical Support for more information about the management packs.

Veritas Volume Replicator

Veritas Volume Replicator (VVR) is an option available with Veritas Storage Foundation 5.1 SP1 for Windows or Veritas Storage Foundation HA 5.1 SP1 for Windows.

For more information on the new features and supported software listed refer to the *Veritas Storage Foundation™ Volume Replicator Administrator's Guide*.

VVR compression

Compression enables VVR to send data in a compressed form from a primary to a secondary host. It reduces network bandwidth consumption by VVR.

The Compression option can be enabled on a per RLINK basis either through the CLI or GUI. At any time, the user can disable or enable the compression feature without stopping the replication.

VVR graphs

VVR Graphs are used to display statistical information through the VEA GUI about the following:

- Bandwidth usage by an RLINK in an RDS
For bandwidth usage, a graph of the data sent per second in kilobits (KB) is plotted against time. This graph gets updated every five seconds. The bandwidth usage can be monitored both in the Online as well as Historic mode.
- The Non-Paged Pool (NPP) memory usage by SFW
VVR and SFW together use VOLIOMEM, NMCOM, and READBACK memory pools. The NPP Memory Usage graph plots the allocated and maximum values for these memory pools. It gets updated every five seconds and displays the memory usage in kilobits (KB) against time.

VVR memory tuning support

NPP memory is used by VVR mostly for stabilizing an incoming write from an application, for reading back the data from the replicator log or data volumes, and for holding the incoming updates on the secondary host. However, sometimes the NPP memory gets depleted due to large consumption of the memory pools by VVR. Memory tuning feature monitors the system NPP usage and reduces VVR's usage of NPP.

VVR support for Hyper V on Windows Server 2008 and Windows Server 2008 R2

VVR provides support for replicating virtual machine images on Hyper-V. When combined with Microsoft failover clustering services, this setup can ensure complete disaster recovery as well as high availability for the virtual machines.

New features and changes in release 5.1 AP1

This section describes the new features and changes introduced in Veritas Storage Foundation for Windows (SFW) and Veritas Storage Foundation HA for Windows (SFW HA) 5.1 Application Pack 1.

Support for Microsoft SQL Server 2008

Support for Microsoft SQL Server 2008 includes the following:

- SFW supports VSS-based backup and restore operations with SQL Server 2008. It includes support for FILESTREAM enabled database objects.
- SFW HA supports HA and DR configurations for SQL Server 2008. Refer to the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL 2008* to configure a new HA and DR environment for SQL 2008.
- The **Microsoft SQL Server** tab of the Symantec Solutions Configuration Center supports SQL Server 2008 solutions. The SQL Server 2008 Configuration Wizard can be launched from the Solutions Configuration Center to configure SQL Server 2008 service groups. The online Help and PDF files in the Solutions Configuration Center include documentation for SQL Server 2008 solutions.

Microsoft Windows Server 2008 Hyper-V

Veritas Storage Foundation for Windows 5.1 (SFW) and Veritas Storage Foundation and High Availability 5.1 for Windows (SFW HA) are enabled to run in a Windows Server 2008 Hyper-V child partition (Guest) with full functionality of all features and options. The installation and configuration process for SFW and SFW HA is similar to that on a physical server.

Certain limitations exist for this support:

See [“Software limitations”](#) on page 53.

VCS MOM 2005 management pack for SQL 2008

SFW HA 5.1 Application Pack 1 includes a VCS Management Pack for Microsoft SQL Server 2008. This management pack is for Microsoft Operations Manager 2005. The management pack file (.akm) is integrated with the Application Pack 1 package but you will need to import it separately. There is no change in the procedures for using this VCS management pack.

Refer to the *Veritas Storage Foundation and High Availability Solutions Management Pack Guide for Microsoft Operations Manager 2005* for instructions on how to use this management pack to monitor SQL 2008 using Microsoft Operations Manager (MOM) 2005 in a VCS environment.

High availability support for VMware VirtualCenter

SFW HA 5.1 for Windows includes support for VMware VirtualCenter. You can configure a high availability and a disaster recovery environment for VirtualCenter.

Note: Support for VMware VirtualCenter is not available on VCS 5.1 for Windows.

Refer to the following application note for more detailed information:

<http://www.symantec.com/docs/TECH64740>

Changes to the VCS wizards

The VCS application and service group configuration wizards provide an option (Advanced button on the Network Configuration panel or the virtual server configuration panel) to add the virtual server name to the Active Directory. The wizards discover all the Organization Units (OU) in the domain and populate them in a drop-down list. You specify an OU by selecting the OU name from the drop-down list.

This functionality is enhanced in the application pack. The wizards now let you type the Organization Unit name or search the OU name in the domain using the Windows **Find Organizational Units** dialog box. This makes searching and specifying an OU significantly easier in cases where there are a large number of Organizational Units in the domain and where the OU structure is deeply nested.

You can type the OU details in the format

"CN=Computers,DC=domainname,DC=com". If you want to search for an OU, you can click the ellipsis button and specify the search criteria in the Windows **Find Organizational Units** dialog box.

New features and changes in release 5.1

This section describes the new features and changes introduced in Veritas Storage Foundation for Windows (SFW) and Veritas Storage Foundation HA for Windows (SFW HA) version 5.1.

General support

The following are the new features and changes in release 5.1.

Windows Server 2008 support

SFW and SFW HA introduce support for the following Windows operating systems:

- Windows Server 2008 (32-bit): Standard Edition, Enterprise Edition, or Datacenter Edition
- Windows Server 2008 x64 Editions (for AMD64 or Intel EM64T): Standard x64 Edition, Enterprise x64 Edition, or Datacenter x64 Edition

- Windows Server 2008 for 64-bit Itanium (IA64): Server Edition

Windows Server 2008 Server Core support

SFW and SFW HA support manual configuration of file shares, print shares, and IIS sites on a Windows Server 2008 Server Core machine. You can configure the service group directly on the Server Core machine using the command line, or remotely using the Cluster Manager (Java console).

Client support on Windows Vista

SFW and SFW HA introduce support for client components on Windows Vista, including Vista SP1.

Microsoft Operations Manager (MOM)

Storage Foundation 5.1 and Storage Foundation HA 5.1 include the following

- Support for Microsoft Operations Manager 2007
- Updates to Management Packs for MOM 2005

New application support

Storage Foundation 5.1 and Storage Foundation HA 5.1 include the following

- Expanded support for Microsoft Exchange Server 2007 and for Microsoft Exchange Server 2007 SP1
- Support for Microsoft SharePoint Server 2007
- Support for Enterprise Vault 2007 with Windows Server 2003

VCS Management Console 5.1

This release includes the product media for Veritas Cluster Server (VCS) Management Console 5.1. VCS Management Console was earlier known as Cluster Management Console.

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

For information on updates and patches for VCS Management Console 5.1, see:

<http://www.symantec.com/docs/TECH53160>

To download the most current version of VCS Management Console, go to www.symantec.com, browse to the Cluster Server page and click **Utilities**.

Enhancements to the Solutions Configuration Center

The Storage Foundation and High Availability Solutions Configuration Center guides you through setting up your SFW HA environment and setting up Quick Recovery. The Configuration Center provides solutions for Microsoft Exchange Server, for Microsoft SQL Server, and for additional applications. For this release, a high availability solution has been added for Enterprise Vault Server.

Configuration Center enhancements include the following:

- Automatic launch on startup, with option to disable
- Launch from the Windows **Start** menu by running the command **scc**
- A **Solutions** tab for quick access to Solutions Configuration Center wizards
- Support for resizing the window
- Support added for using the Configuration and its wizards to set up your environment for the following solutions:
 - High availability at a single site for a new Enterprise Vault server
 - High availability at a single site for an existing Exchange server
 - High availability at a single site for an existing SQL server
 - Campus cluster disaster recovery, including the following:
 - Campus cluster using Veritas Cluster Server (SFW HA)
 - Campus cluster using Microsoft clustering

Enhancements to the Solutions wizards

The Solutions wizards have the following enhancements:

The Disaster Recovery Configuration Wizard has been enhanced as follows:

- Support for configuring the following hardware array-based replication options:
 - EMC SRDF
 - Hitachi TrueCopy
- Support for configuring multiple DR sites in a VVR replication environment
- Support for a replicated data cluster configuration on the primary site

The Quick Recovery Configuration Wizard has been enhanced as follows:

- The Quick Recovery wizard now supports configuring snapshots for Exchange 2003 and 2007 in Microsoft clusters as well as VCS clusters.

- The Quick Recovery wizard now supports configuring snapshots for SQL 2005 in both VCS clusters and in Microsoft clusters.
- The Quick Recovery wizard now checks for existing schedules and cleans up obsolete schedule files and entries. In a clustered server environment, the wizard synchronizes schedules between cluster nodes to ensure that existing schedules are available on new nodes.

The Fire Drill wizard has been enhanced to provide support for recreating the fire drill service group if the application service group has changed.

Installation

The following are the new features and changes for the installation process in release 5.1.

Configuration Checker enhancements

The following are Configuration Checker enhancements:

- Better differentiation between preinstallation and post-installation checks
- Improved check descriptions and reports

Veritas Storage Foundation

The following are the new features and changes for Veritas Storage Foundation in release 5.1.

Storage Management

The following are enhancements to support storage management:

- Storage management coexistence on Windows Server 2008.
SFW and SFW HA support the availability of Microsoft Disk Management, the storage management feature of Windows Server 2008. SFW coexists with Microsoft Disk Management and can manage the dynamic disk group that it creates.
- SFW has been enhanced to support a maximum of 4096 dynamic disk groups.

SmartMove

SFW has been enhanced with the new SmartMove feature. SmartMove helps reduce the resynchronization time required by mirror operations and subdisk moves. SmartMove reduces the resynchronization time by using the NTFS file system metadata to resynchronize only selected regions. Operations that involve

mirrors, like adding a mirror to a volume, off-host backup, and array migration, can have improved performance by using the SmartMove feature.

VSS snapshot wizard enhancements

The following are the VSS snapshot wizard enhancements:

- VSS snapshot wizards now provide support for SQL 2005 in an SFW HA environment.
- The VSS SQL Restore wizard provides support for recovery when a volume is missing.

Microsoft Exchange Server 2007

SFW supports VSS-based backup and restore operations with the Recovery Storage Group.

Microsoft clustering

Storage Foundation for Windows supports the installation of Microsoft clustering and SFW Microsoft clustering (MSCS) support after SFW has already been installed.

Refer to the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide* for more information.

iSCSI

The following are enhancements to support iSCSI:

- Improved iSCSI target and initiator management.
- Automatic configuration of VxDgDI, the Veritas DG Delayed Import Service, for iSCSI disks that are imported at system startup.

Dynamic Multi-pathing (Veritas DMP)

For the latest updates to array support and for supported hardware configurations, see the Hardware Compatibility list at:

<http://www.symantec.com/business/support/index.jsp>

Veritas Cluster Server

The following are the new features and changes in release 5.1.

Microsoft Exchange Server 2007 support

SFW HA supports Exchange 2007 (including Service Pack 1). SFW HA support for Exchange 2007 is available for the Mailbox Server role only.

Support for Microsoft Sharepoint Server 2007 in a disaster recovery configuration

Microsoft SharePoint Server 2007 is supported in a disaster recovery configuration. See the *Veritas Cluster Server Application Note: Disaster Recovery for Microsoft SharePoint Server* for detailed information.

Support for networks using DNS scavenging

Updated VCS Lanman Agent supports DNS scavenging by monitoring and adding required records back to the DNS database automatically.

EMC SRDF/Star enterprise agent

The VCS enterprise agent for EMC SRDF/Star provides failover support and recovery in the environments that use the SRDF/Star solution to protect their data.

VCW support for configuring VCS LLT over UDP

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

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

Support for Oracle on 64-bit Windows servers

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

BlackBerry Enterprise Server support

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

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

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

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

Veritas Volume Replicator

Veritas Volume Replicator (VVR) is an option available with Veritas Storage Foundation 5.1 for Windows or Veritas Storage Foundation HA 5.1 for Windows.

VVR support for TCP Multi-Connection

To achieve better network throughput, multiple TCP connections have been introduced with this release of Veritas Volume Replicator (VVR). Parallel TCP connections can boost the throughput of TCP in Long Fat Networks (LFNs) when used on a lossy link. Replicating through multiple transport connections for each RLINK will maximize the usage of higher bandwidth networks. Multiple connections improve the overall replicating performance of VVR.

VSS snapshot wizard enhancement

While doing a synchronized snapshot, the user can select the plex to be snapshotted on the secondary. If a plex is already snapshotted, it is not shown in the Plex list. This feature is supported on both the GUI and CLI.

Application support

Before installing or upgrading SFW or SFW HA 5.1 Service Pack 2, review the current compatibility lists to confirm the compatibility of your hardware and software.

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

<http://www.symantec.com/docs/TECH138722>

The following listed applications are supported for this release.

Microsoft Exchange Server

SFW HA 5.1 Service Pack 2 supports Microsoft Exchange Server 2003, Microsoft Exchange Server 2007, and Microsoft Exchange Server 2010.

Supported Microsoft Exchange 2003 versions

[Table 1-4](#) lists the Microsoft Exchange 2003 versions supported with SFW HA 5.1 SP2.

Table 1-4 Microsoft Exchange 2003 supported environments

Microsoft Exchange Server 2003	Window Servers
Microsoft Exchange Server 2003 Standard Edition or Enterprise Edition on Windows Server 2003 (Exchange Server 2003 SP2 required)	<ul style="list-style-type: none"> ■ Windows Server 2003 (32-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions) ■ Windows Server 2003 R2 (32-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions)
Microsoft Exchange Server 2003 Standard Edition or Enterprise Edition on Windows Server 2008 (Exchange Server 2003 SP2 required)	<ul style="list-style-type: none"> ■ Windows Server 2008 (32-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions)

Supported Microsoft Exchange 2007 versions

[Table 1-5](#) lists the Microsoft Exchange 2007 versions supported with SFW HA 5.1 SP2.

Table 1-5 Microsoft Exchange Server 2007 supported environments

Microsoft Exchange Server 2007	Window Servers
Microsoft Exchange Server 2007 (SP1, SP2, or SP3) Standard Edition or Enterprise Edition on Windows 2003 Server (Mailbox server role required)	<ul style="list-style-type: none"> ■ Windows Server 2003 x64 Standard Edition or Enterprise Edition (SP2 required for all editions) ■ Windows Server 2003 R2 x64 Standard Edition or Enterprise Edition (SP2 required for all editions)

Table 1-5 Microsoft Exchange Server 2007 supported environments
(continued)

Microsoft Exchange Server 2007	Window Servers
Microsoft Exchange Server 2007 (SP1, SP2, or SP3) Standard Edition or Enterprise Edition on Windows 2008 Server (Mailbox server role required)	<ul style="list-style-type: none"> ■ Windows Server 2008 x64 Editions (for AMD64 or Intel EM64T): Standard x64 Edition, Enterprise x64 Edition, or Datacenter x64 Edition ■ Windows Server 2008 x64 R2 without Hyper-V on Standard, Enterprise, Datacenter Editions ■ Windows Server 2008 x64 R2 on Standard, Enterprise, Datacenter Editions (for physical host or guest, not parent partition/Hyper-V integration) ■ Windows Server 2008 R2 for IA Systems - IA64 ■ Windows Server 2008 x64 R2 Web Edition ■ Windows Server 2008 on all current editions and architectures Symantec currently supports (SP2 required) ■ Windows Storage Server 2008

Supported Microsoft Exchange 2010 versions

[Table 1-6](#) lists the Microsoft Exchange Server 2010 versions supported with SFW HA 5.1 SP2.

Table 1-6 Microsoft Exchange Server 2010 supported environments

Microsoft Exchange Server 2010	Window Servers
Microsoft Exchange Server 2010, Standard Edition or Enterprise Edition (Mailbox server role required) (SP1 supported)	<ul style="list-style-type: none"> ■ Windows Server 2008 with Service Pack 2: Standard x64 Edition, Enterprise x64 Edition ■ Windows Server 2008 R2 on Standard x64 Edition, Enterprise x64 Edition

Microsoft SQL Server

SFW HA 5.1 SP2 supports Microsoft SQL Server 2000, Microsoft SQL Server 2005, and Microsoft SQL Server 2008 and 2008 R2.

Supported SQL 2000 versions

[Table 1-7](#) lists the SQL Server 2000 versions supported with SFW HA 5.1 SP2.

Table 1-7 Supported Microsoft SQL Server 2000 versions

SQL Server 2000	Windows Servers
Microsoft SQL Server 2000 Standard Edition or Enterprise Edition (SP4 required)	<ul style="list-style-type: none"> ■ Windows Server 2003 (32-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions) ■ Windows Server 2003 R2 (32-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions)
Microsoft SQL Server 2000 (64-bit) Enterprise Edition	<ul style="list-style-type: none"> ■ Windows Server 2003 for Itanium-based Systems Enterprise Edition or Datacenter Edition (SP2 required for both)
Microsoft SQL Server 2000 (64-bit) Standard Edition or Enterprise Edition (SP4 required)	<ul style="list-style-type: none"> ■ Windows Server 2003 x64 Editions (for AMD64 or Intel EM64T): Standard x64 Edition, Enterprise x64 Edition, or Datacenter x64 Edition (SP2 required for all editions) ■ Windows Server 2003 x64 Editions (for AMD64 or Intel EM64T): Standard x64 R2 Edition, Enterprise x64 R2 Edition, or Datacenter x64 R2 Edition (SP2 required for all editions)

Supported Microsoft SQL Server 2005 versions

[Table 1-8](#) lists the Microsoft SQL Server 2005 versions supported with SFW HA.

Table 1-8 Microsoft SQL Server 2005 supported environments

SQL Server 2005	Window Servers
Microsoft SQL Server 2005, 32-bit Standard Edition or Enterprise Edition on Windows Server 2003 (SQL Server 2005 SP1, SP2, or SP3)	<ul style="list-style-type: none"> ■ Windows Server 2003 (32-bit) Standard Edition, Enterprise Edition or Datacenter Edition (SP2 required) ■ Windows Server 2003 R2 (32-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required) ■ Windows Server 2003 for Itanium-based Systems Enterprise Edition or Datacenter Edition (SP2 required for both) ■ Windows Server 2003 Standard x64 Edition, Enterprise x64 Edition, or Datacenter x64 Edition (SP2 required) ■ Windows Server 2003 x64 Editions (for AMD64 or Intel EM64T): Standard x64 R2 Edition, Enterprise x64 R2 Edition, or Datacenter x64 R2 Edition (SP2 required)

Table 1-8 Microsoft SQL Server 2005 supported environments (*continued*)

SQL Server 2005	Window Servers
Microsoft SQL Server 2005, 32-bit Standard Edition or Enterprise Edition on Windows Server 2008 (SQL Server 2005 SP2 or SP3)	<ul style="list-style-type: none"> ■ Windows Server 2008 (32-bit) Standard Edition, Enterprise Edition, or Datacenter Edition ■ Windows Server 2008 x64 R2 without Hyper-V on Standard, Enterprise, Datacenter Editions ■ Windows Server 2008 x64 R2 on Standard, Enterprise, Datacenter Editions (for physical host or guest, not parent partition/Hyper-V integration) ■ Windows Server 2008 R2 for IA Systems - IA64 ■ Windows Server 2008 x64 R2 Web Edition ■ Windows Server 2008 on all current editions and architectures Symantec currently supports (SP2 required) ■ Windows Storage Server 2008
Microsoft SQL Server 2005, 64-bit Standard Edition or Enterprise Edition on Windows Server 2003 (SQL Server 2005 SP1, SP2, or SP3)	<ul style="list-style-type: none"> ■ Windows Server 2003 for Itanium-based Systems Enterprise Edition or Datacenter Edition (SP2 required for both) ■ Windows Server 2003 Standard x64 Edition, Enterprise x64 Edition, or Datacenter x64 Edition (SP2 required) ■ Windows Server 2003 x64 Editions (for AMD64 or Intel EM64T): Standard x64 R2 Edition, Enterprise x64 R2 Edition, or Datacenter x64 R2 Edition (SP2 required)
Microsoft SQL Server 2005, 64-bit Standard Edition or Enterprise Edition on Windows Server 2008 (SQL Server 2005 SP1, SP2, or SP3)	<ul style="list-style-type: none"> ■ Windows Server 2008 for 64-bit Itanium (IA64) ■ Windows Server 2008 x64 Editions (for AMD64 or Intel EM64T): Standard x64 Edition, Enterprise x64 Edition, or Datacenter x64 Edition ■ Windows Server 2008 x64 R2 without Hyper-V on Standard, Enterprise, Datacenter Editions ■ Windows Server 2008 x64 R2 on Standard, Enterprise, Datacenter Editions (for physical host or guest, not parent partition/Hyper-V integration) ■ Windows Server 2008 R2 for IA Systems - IA64 ■ Windows Server 2008 x64 R2 Web Edition ■ Windows Server 2008 on all current editions and architectures Symantec currently supports (SP2 required) ■ Windows Storage Server 2008

Supported SQL 2008 and SQL 2008 R2 versions

SFW HA 5.1 SP2 supports SQL 2008 and SQL 2008 R2.

[Table 1-9](#) lists the Microsoft SQL Server 2008 versions supported with SFW HA 5.1 SP2.

Table 1-9 Supported Microsoft SQL Server 2008 versions

SQL Server 2008	Windows Servers
<p>Microsoft SQL Server 2008, 32-bit Standard Edition, Enterprise Edition, or Web Edition on Windows Server 2003 (SQL Server 2008 SP1)</p>	<ul style="list-style-type: none"> ■ Windows Server 2003 (32-bit) Standard Edition, Enterprise Edition or Datacenter Edition (SP2 required) ■ Windows Server 2003 R2 (32-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required) ■ Windows Server 2003 for Itanium-based Systems Enterprise Edition or Datacenter Edition (SP2 required for both) ■ Windows Server 2003 Standard x64 Edition, Enterprise x64 Edition, or Datacenter x64 Edition (SP2 required) ■ Windows Server 2003 x64 Editions (for AMD64 or Intel EM64T): Standard x64 R2 Edition, Enterprise x64 R2 Edition, or Datacenter x64 R2 Edition (SP2 required)
<p>Microsoft SQL Server 2008, 64-bit Standard Edition, Enterprise Edition, Enterprise IA64 Edition, Web Edition on Windows Server 2003 (SQL Server 2008 SP1)</p>	<ul style="list-style-type: none"> ■ Windows Server 2003 (64-bit) Standard x64 Edition, Enterprise x64 Edition or Datacenter x64 Edition (SP2 required) ■ Windows Server 2003 x64 Editions (for AMD64 or Intel EM64T): Standard x64 R2 Edition, Enterprise x64 R2 Edition, or Datacenter x64 R2 Edition (SP2 required) ■ Windows Server 2003 (64-bit) for Itanium-based systems Enterprise Edition or Datacenter Edition (SP2 required for both)
<p>Microsoft SQL Server 2008, 32-bit Standard Edition, Enterprise Edition, or Web Edition on Windows Server 2008 (SQL Server 2008 SP1)</p>	<ul style="list-style-type: none"> ■ Windows Server 2008 (32-bit) Standard Edition, Enterprise Edition, Datacenter Edition, or Web Edition ■ Windows Server 2008 x64 R2 without Hyper-V on Standard, Enterprise, Datacenter Editions ■ Windows Server 2008 x64 R2 on Standard, Enterprise, Datacenter Editions (for physical host or guest, not parent partition/Hyper-V integration) ■ Windows Server 2008 R2 for IA Systems - IA64 ■ Windows Server 2008 x64 R2 Web Edition ■ Windows Server 2008 on all current editions and architectures Symantec currently supports (SP2 required) ■ Windows Storage Server 2008

Table 1-9 Supported Microsoft SQL Server 2008 versions (*continued*)

SQL Server 2008	Windows Servers
Microsoft SQL Server 2008, 64-bit Standard Edition, Enterprise Edition, Enterprise IA64 Edition, Web Edition on Windows Server 2008 (SQL Server 2008 SP1)	<ul style="list-style-type: none"> ■ Windows Server 2008 x64 Editions (for AMD64 or Intel EM64T): Standard x64 Edition, Enterprise x64 Edition, or Datacenter x64 Edition ■ Windows Server 2008 64-bit Itanium (IA64) ■ Windows Server 2008 x64 R2 without Hyper-V on Standard, Enterprise, Datacenter Editions ■ Windows Server 2008 x64 R2 on Standard, Enterprise, Datacenter Editions (for physical host or guest, not parent partition/Hyper-V integration) ■ Windows Server 2008 R2 for IA Systems - IA64 ■ Windows Server 2008 x64 R2 Web Edition ■ Windows Server 2008 on all current editions and architectures Symantec currently supports (SP2 required) ■ Windows Storage Server 2008

[Table 1-10](#) lists the Microsoft SQL Server 2008 R2 versions supported with SFW HA 5.1 SP2.

Table 1-10 Supported Microsoft SQL Server 2008 R2 versions

SQL Server 2008 R2	Windows Servers
Microsoft SQL Server 2008 R2, 32-bit Standard Edition, Enterprise Edition, Datacenter Edition on Windows Server 2003	<ul style="list-style-type: none"> ■ Windows Server 2003 (32-bit) Standard Edition, Enterprise Edition or Datacenter Edition (SP2 required) ■ Windows Server 2003 R2 (32-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required) ■ Windows Server 2003 for Itanium-based Systems Enterprise Edition or Datacenter Edition (SP2 required for both) ■ Windows Server 2003 Standard x64 Edition, Enterprise x64 Edition, or Datacenter x64 Edition (SP2 required) ■ Windows Server 2003 x64 Editions (for AMD64 or Intel EM64T): Standard x64 R2 Edition, Enterprise x64 R2 Edition, or Datacenter x64 R2 Edition (SP2 required)

Table 1-10 Supported Microsoft SQL Server 2008 R2 versions (*continued*)

SQL Server 2008 R2	Windows Servers
<p>Microsoft SQL Server 2008 R2, 64-bit Standard Edition, Enterprise Edition, Datacenter Edition on Windows Server 2003</p>	<ul style="list-style-type: none"> ■ Windows Server 2003 (64-bit) Standard x64 Edition, Enterprise x64 Edition or Datacenter x64 Edition (SP2 required) ■ Windows Server 2003 x64 Editions (for AMD64 or Intel EM64T): Standard x64 R2 Edition, Enterprise x64 R2 Edition, or Datacenter x64 R2 Edition (SP2 required) ■ Windows Server 2003 (64-bit) for Itanium-based systems Enterprise Edition or Datacenter Edition (SP2 required for both)
<p>Microsoft SQL Server 2008 R2, 32-bit Standard Edition, Enterprise Edition, or Datacenter Edition on Windows Server 2008</p>	<ul style="list-style-type: none"> ■ Windows Server 2008 (32-bit) Standard Edition, Enterprise Edition, Datacenter Edition, or Web Edition ■ Windows Server 2008 x64 R2 without Hyper-V on Standard, Enterprise, Datacenter Editions ■ Windows Server 2008 x64 R2 on Standard, Enterprise, Datacenter Editions (for physical host or guest, not parent partition/Hyper-V integration) ■ Windows Server 2008 R2 for IA Systems - IA64 ■ Windows Server 2008 x64 R2 Web Edition ■ Windows Server 2008 on all current editions and architectures Symantec currently supports (SP2 required) ■ Windows Storage Server 2008
<p>Microsoft SQL Server 2008 R2, 64-bit Standard Edition, Enterprise Edition, Datacenter Edition on Windows Server 2008</p>	<ul style="list-style-type: none"> ■ Windows Server 2008 x64 Editions (for AMD64 or Intel EM64T): Standard x64 Edition, Enterprise x64 Edition, or Datacenter x64 Edition ■ Windows Server 2008 64-bit Itanium (IA64) ■ Windows Server 2008 x64 R2 without Hyper-V on Standard, Enterprise, Datacenter Editions ■ Windows Server 2008 x64 R2 on Standard, Enterprise, Datacenter Editions (for physical host or guest, not parent partition/Hyper-V integration) ■ Windows Server 2008 R2 for IA Systems - IA64 ■ Windows Server 2008 x64 R2 Web Edition ■ Windows Server 2008 on all current editions and architectures Symantec currently supports (SP2 required) ■ Windows Storage Server 2008

Enterprise Vault

Application support for Enterprise Vault is as follows:

- Enterprise Vault 8.0 SP1, SP2, and SP3
- Enterprise Vault 9.0

Note: Review the Symantec Enterprise Vault documentation on the Symantec support website for the latest installation and configuration instructions.

Sharepoint

SFW HA 5.1 Service Pack 2 provides support for SharePoint Portal Server 2003, SharePoint Server 2007 and SharePoint Server 2010.

Application support for Sharepoint is as follows:

- Microsoft SharePoint Portal Server 2003 SP2
- Microsoft SharePoint Server 2007, 32-bit Standard Edition or Enterprise Edition
- Microsoft SharePoint Server 2007, 64-bit Standard Edition or Enterprise Edition
- Microsoft SharePoint Server 2010

SharePoint 2010 is supported with SFW HA 5.1 SP2 on the following operating systems: Windows Server 2008 with Service Pack 2 or later, x64 Edition
Windows Server 2008 R2, x64 Edition See the Microsoft documentation for details on required SQL Server database versions supported with Sharepoint Server 2010.

BlackBerry Enterprise Server

Application support for BlackBerry Enterprise Server is as follows:

- BlackBerry Enterprise Server (BES) 4.1.5

Oracle

[Table 1-11](#) lists the supported Oracle versions and the operating systems. Note that all systems must be running the same operating system.

Table 1-11 Supported application software for Oracle

Oracle versions	Windows Server versions
<p>Oracle 9i, Release 2 (9.2.0.2) Standard Edition, Enterprise Edition</p> <p>Oracle 10g, Release 1 (10.1.0.2) Standard Edition, Enterprise Edition</p>	<ul style="list-style-type: none"> ■ Windows Server 2003 (32-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions) ■ Windows Server 2003 (32-bit) R2 Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions) ■ Windows Server 2003 for Itanium-based Systems Enterprise Edition or Datacenter Edition (SP2 required for both)
<p>Oracle 10g, Release 2 (10.2.0.1.0) Standard Edition, Enterprise Edition</p>	<ul style="list-style-type: none"> ■ Windows Server 2003 (32-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions) ■ Windows Server 2003 (32-bit) R2 Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions) ■ Windows Server 2003 for Itanium-based Systems Enterprise Edition or Datacenter Edition (SP2 required for both) ■ Windows Server 2003 (64-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions) ■ Windows Server 2003 (64-bit) R2 Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions)
<p>Oracle 10g, Release 2 (10.2.0.4) Standard Edition, Enterprise Edition</p>	<ul style="list-style-type: none"> ■ Windows Server 2008 (32-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions) ■ Windows Server 2008 (64-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions)
<p>Oracle 10g, Release 2 (10.2.0.5) Standard Edition, Enterprise Edition</p>	<p>Windows Server 2008 R2 (64-bit) Standard Edition, Enterprise Edition, or Datacenter Edition</p>
<p>Oracle 11g, Release 1 (11.1.0.6.0)</p>	<ul style="list-style-type: none"> ■ Windows Server 2003 (32-bit, 64-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions) ■ Windows Server 2003 (32-bit, 64-bit) R2 Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions)

Table 1-11 Supported application software for Oracle (*continued*)

Oracle versions	Windows Server versions
Oracle 11g, Release 1 (11.1.0.7.0)	■ Windows Server 2008 (32-bit, 64-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions)
Oracle 11g Release 2 (11.2.0.1)	■ Windows Server 2008 (32-bit, 64-bit) Standard Edition, Enterprise Edition, or Datacenter Edition (SP2 required for all editions) ■ Windows Server 2008 R2 (64-bit) Standard Edition, Enterprise Edition, or Datacenter Edition

Requirements

This section covers software and hardware requirements for installation. Before installing the product, refer to the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide* for additional installation instructions.

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

<http://www.symantec.com/docs/TECH138722>

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

<http://www.symantec.com/docs/TECH138719>

Operating system requirements

SFW and SFW HA 5.1 SP2 have server and client components that run on specific Windows operating systems. For information about the supported Windows operating systems:

- SFW and SFW HA 5.1 SP2 software for servers:
See “[SFW and SFW HA 5.1 SP2 software for servers](#)” on page 46.
- SFW and SFW HA 5.1 SP2 software for clients:
See “[SFW and SFW HA 5.1 SP2 software for clients](#)” on page 47.

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

<http://www.symantec.com/docs/TECH138722>

SFW and SFW HA 5.1 SP2 software for servers

Your server must run one of the operating systems listed below to install the SFW or SFW HA 5.1 SP2 server software.

Note: SFW 5.1 SP2 software for servers supports Hyper-V and parent partitions. SFW HA 5.1 SP2 software for servers does not support Hyper-V and parent partitions.

- Windows Server 2003 x86: Web Edition (SP2 required)
- Windows Server 2003 x86, x64, IA64: Standard Edition, Enterprise Edition, Datacenter Edition (SP2 required for all editions)
- Windows Server 2003 R2 x86, x64: Standard Edition, Enterprise Edition, Datacenter Edition (SP2 required for all editions)
- Windows Server 2003 R2 x86, x64: Small Business Server (SP2 required)
- Windows Storage Server 2003 R2 x86, x64: Standard Edition, Enterprise Edition (SP2 required for these editions)
- Windows Unified Data Storage Server 2003 x86, x64: Standard Edition, Enterprise Edition (SP2 required for these editions)
- Windows 2008 Server Core
- Windows 2008 R2 Server Core
- Windows 2008 SP2 Server Core
- Windows Server 2008 x86, x64: Standard Edition, Enterprise Edition, Datacenter Edition, Web Edition, Small Business Server (SP1 or SP2 required for all editions)

Note: SFW HA 5.1 SP2 supports Windows Server 2008 without Hyper-V x86, x64: Standard Edition, Enterprise Edition, Datacenter Edition (SP1 or SP2 required for all editions).

- Windows Server 2008 for Itanium Systems (IA64) (SP1 or SP2)
- Windows Server 2008 R2 x64: Standard Edition, Enterprise Edition, Datacenter Edition, Web Edition

Note: SFW HA 5.1 SP2 supports Windows Server 2008 R2 without Hyper-V x64: Standard Edition, Enterprise Edition, Datacenter Edition.

- Windows Server 2008 R2 for Itanium Systems (IA64)
- Windows Storage Server 2008

SFW and SFW HA 5.1 SP2 software for clients

Your system must run one of the following operating systems to install the SFW or SFW HA 5.1 SP2 client software:

- Any one of the operating system versions, editions, and architectures that the Server Components are supported on except Server Core:
See “[SFW and SFW HA 5.1 SP2 software for servers](#)” on page 46.
- Windows XP x86, x64 (SP3 required)
- Windows Vista x86, x64: Ultimate Edition, Business Edition, Premium Edition (SP1 or SP2 required)
- Windows 7 x86, x64: Ultimate Edition, Business Edition, Premium Edition

Hardware requirements

Before you install the SFW or SFW HA 5.1 SP2 software, verify that your configuration meets the following criteria and that you have reviewed the SFW 5.1 SP2 Hardware Compatibility List to confirm supported hardware:

<http://www.symantec.com/docs/TECH138719>

Table 1-12 displays the hardware requirements for an SFW or SFW HA 5.1 SP2 software installation.

Table 1-12 Hardware requirements for SFW or SFW HA 5.1 SP2

Requirements	Specifications
Memory	1 GB of RAM required
32-bit processor requirements	800-megahertz (MHz) Pentium III-compatible or faster processor 1GHz or faster processor recommended
x64 processor requirements	1GHz AMD Opteron, AMD Athlon 64, Intel Xeon with Intel EM64T support, Intel Pentium IV with EM64T support processor or faster
IA64 processor requirements	1GHz Itanium or faster processor 1GHz Dual-Core Intel Itanium 2 or faster processor
Display	Minimum resolution: 1024 X 768 pixels or higher VCS Cluster Manager (Java and Web Console) requires an 8-bit (256 colors) display and a graphics card that can render 2D images

Disk space requirements

For normal operation, all installations require a minimum of 50 MB of disk space in addition to the requirements listed in [Table 1-13](#) below.

Note: For installation, space required is calculated regardless of selected options or components.

[Table 1-13](#) summarizes approximate disk space requirements for SFW and SFW HA 5.1 SP2 on 32-bit and 64-bit systems.

Table 1-13 Disk space requirements

Installation options	Install directory or drive	Install directory or drive
	32-bit	64-bit
SFW + all options + client components	1430 MB	1860 MB
SFW + all options	1140 MB	1400 MB
SFW Client components	590 MB	560 MB
SFW HA + all options + client components	1950 MB	2370 MB
SFW HA + all options	1520 MB	1880 MB
SFW HA Client components	780 MB	650 MB

Bootimg for SAN device (BFS) requirements

SFW 5.1 Service Pack 2 requires at least a 40GB Boot Partition for Windows 2008 Server X64, when booting from a SAN device (BFS) with Dynamic Multi-pathing (DMP).

The boot volume must be large enough for DMP to work properly if failover occurs with an EMC array. A BFS device may not be large enough to meet the required configuration for the Windows Server 2008 x64 environment.

Microsoft provides the following Windows Server 2008 System Requirements link:

<http://msdn.microsoft.com/en-us/windowsserver/cc196364.aspx>

If you encounter this issue, then perform one of the following possible solutions:

1. Re-install the operating system on a the larger volume that is at least 40 GB
2. Reinstall SFW and configure DMP on the Windows Server 2008 system.

or

1. Increase the boot device to at least 40GB.
2. Reinstall SFW and configure DMP on the Windows Server 2008 system.

The above solutions allow for a successful path failover if a path failure occurs, or when testing the configuration by manually pulling the cables and causing a path failure.

The Windows event viewer and Veritas Enterprise Administrator (VEA) will now also report the removal and arrival of device paths.

Storage device compatibility

If you are not using Veritas Dynamic Multi-pathing or clustering (SFW HA or Microsoft clustering), SFW supports any device in the Microsoft Windows Server Catalog.

For Veritas Dynamic Multi-pathing and clustering configurations, refer to the Hardware Compatibility List to determine the approved hardware for SFW:

<http://www.symantec.com/docs/TECH138719>

Note: If your storage devices are SCSI-3 compliant, and you wish to use SCSI-3 Persistent Group Reservations (PGR), you must enable SCSI-3 support using the Veritas Enterprise Administrator (VEA).

For additional information about this procedure:

See the *Veritas Storage Foundation Administrator's Guide*.

General requirements

The following are additional requirements that apply for SFW and SFW HA installation.

Supported browsers for Veritas Cluster Server Management Console

Veritas Cluster Server Management Console is supported on the following browsers:

- Microsoft Internet Explorer 6.0 and 7.0
- Firefox 2.0 and 3.0.x

Veritas Cluster Server Management Console also requires Macromedia Flash Plug-in, Version 8.0 or greater.

Note: VCS Management Console does not support Firefox on Linux platforms.

Firewall port settings and anti-spyware

Before installing SFW or SFW HA, disable spyware monitoring and removal software. This is done only for your installation and should be re-enabled immediately after installation.

Ensure that your firewall settings allow access to ports used by SFW HA 5.1 SP2 wizards and services. For a detailed list of services and ports used by SFW HA 5.1 SP2:

See the appendix in the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide*.

For any updates on port requirements, see the Support TechNote:

<http://www.symantec.com/docs/TECH83441>

Remote systems

Installation on remote systems is supported using a silent install or GUI. Silent installation may be done on one node at a time. Use the GUI to install on multiple nodes. Remote Desktop Protocol (RDP) connections must use the console switch.

You must have network access and appropriate administrative privileges to each remote computer.

Veritas Volume Replicator static IP address

VVR requires a static IP for replication and clustering. If you are installing the VVR option, make sure the system has at least one IP address configured that is not assigned by Dynamic Host Configuration Protocol (DHCP).

Single instance of SFW

Only one instance of Veritas Storage Foundation 5.1 for Windows (SFW 5.1 SP2) should be running on a system.

If you have a previous version of Volume Manager or SFW already installed, refer to the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide*.

VMware ESX server support

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

VMware Workstation support

In this release, VMware Workstation 6.5 is required for running SFW on VMware virtual machines.

No longer supported

The following behavior has changed in the 5.1 SP2 release.

Discontinued support for VCS Cluster Management Console (Single Cluster Mode)

Support for the VCS Cluster Management Console (Single Cluster Mode) is discontinued in 5.1 SP2. The VCS VRTSWebApp agent has been deprecated and is uninstalled during the upgrade. Also, the VCS Cluster Configuration Wizard (VCW) no longer provides the option to configure the Cluster Manager service components.

If VRTSWebApp resource is configured in ClusterService group, after upgrading to 5.1SP2 the resource fails to get probed and thus the ClusterService group would fail to come online in the cluster. You must manually delete the VRTSWebApp resource from the ClusterService group. Use the Cluster Manager (Java Console), the command line (hares -delete), or the Veritas Operations Manager (VOM) to remove the resource.

Symantec Live Update client is no longer installed and supported

Symantec Live Update client is no longer installed and supported as a part of Storage Foundation and High Availability solutions for Windows.

Symantec License Inventory Management (SLIM)

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

Windows Server 2000

SFW and SFW HA no longer support Windows Server 2000. Therefore Exchange Server 2000 and Microsoft Operations Manager (MOM) 2000 are also no longer supported.

Language Pack for Japanese

The Language Pack for Japanese is no longer available for SFW and SFW HA.

Dynamic Multipathing Array Support Libraries

SFW and SFW HA no longer support Dynamic Multipathing Array Support Libraries (DMP ASLs).

Dependent service groups with the DR wizard

The Disaster Recovery wizard (DR) no longer supports configuring dependent service groups with VVR replication.

NetBackup agents and wizards

SFW HA no longer includes agents and configuration wizards for NetBackup. Refer to the NetBackup documentation for information on clustering support for NetBackup.

Installation notes

The following information includes guidelines, tips, and other considerations for installing or upgrading the product.

- Remote installation using a Remote Desktop Protocol (RDP) connection must use a console session or console switch.
- An evaluation license key is built into the product code. To use this evaluation key, click **Next** on the **License key** screen.
- To use a command line rather than the product installer to add license keys after installation, for example on Windows Server 2008 Server Core, you must use the `vxlicinst` utility that is provided on the SFW HA product media or in the Volume Manager install directory.
For additional information:
See [“License management”](#) on page 54.
- If you are in need of the debug symbols for this release, contact Symantec Technical Support.
- For information about installing or upgrading this product, refer to the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide*.

- The product installer provides an installation option for Symantec Trusted Software Publisher Certificate. On a Windows Server 2008 remote install, this option is required to install any Veritas Storage Foundation for Windows drivers that are not certified by Microsoft.
For more information on this option, refer to the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide*.
- Install the Veritas Storage Foundation and HA Solutions software in the following sequence:
 - Veritas Storage Foundation and HA Solutions 5.1 SP2, with any installation options for version 5.1, such as VCS Agents or VVR.
 - Symantec recommends that you copy the release notes to the directory `%Program Files%\Veritas\Docs\ENU`, so they are available on your system for reference.
- When installing or upgrading to SFW or SFW HA 5.1 SP2, ensure that there are no parallel installations, live updates, or Microsoft Windows updates in progress.
- Symantec provides clean-up and recovery tools and scripts in case of failed SFW or SFW HA 5.1 SP2 installs, uninstalls, or upgrades. These clean-up and recovery tools and scripts can be downloaded from the following Symantec link:
<http://www.symantec.com/docs/TECH76129>
The Symantec link also provides tech notes and FAQs about SFW or SFW HA 5.1 installs, uninstalls, upgrades, and troubleshooting issues

Software limitations

The following software limitations apply to this release of the product. For the latest information on updates, patches, and software issues regarding this release, see the following TechNote:

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

Installation or upgrade

The following are installation or upgrade software limitation issues.

UUID files are always installed to the default installation path

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

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

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

License management

The following is a license management software limitation.

Silent installation does not support updating license keys after install

You can install SFW or SFW HA using either the product installer or the command line interface (for a silent installation).

Both installation methods enable you to specify license keys during product installation. The product installer also includes the functionality to update license keys after installation. However, the command line interface used in a silent installation does not support updating license keys after an installation.

To add license keys after a silent installation using the CLI, for example on Windows Server 2008 Server Core systems, you use the `vxlicinst` utility located on the SFW HA product DVD:

To add license keys after silent installation using CLI

- 1 Insert the product DVD in a drive that you can access from the system on which you want to add the license.
- 2 Navigate to the `vxlic_util` directory on the product DVD:

```
<DVD_ROOT_DIRECTORY>\Tools\storage_foundation_for_windows\vxlic_tools
```

- 3 Type the command as follows to specify the key to be added:

```
vxlicinst -k <key>
```

You can also access the `vxlicinst` utility after an installation in the Volume Manager install directory.

The directory is: `%VMPATH%`.

Veritas Storage Foundation

This section covers limitations specific to Storage Foundation functionality.

SFW FlashSnap solution for EV does not support basic disks

The SFW FlashSnap solution for Enterprise Vault (EV) is not supported for EV databases that reside on basic disks. (2116246, 2122790)

The vxsnap command may fail with the following errors:

```
V-76-58657-2053: Failed to prepare some of the EV components.
```

```
See EVStatus.log for more details.
```

```
The operation to prepare the volumes for a snapshot has failed.
```

```
See the log file for details.
```

To use the FlashSnap solution for EV, ensure that the EV databases reside on dynamic disks.

Requirements for iSCSI or VDS-based functionality

Storage Foundation for Windows requires the following components for iSCSI or VDS-based support:

- For Windows Server 2003 R2 (32-bit): Standard Edition, Enterprise Edition, or Datacenter Edition:
- Include the VDS 1.1 Update for R2 (execute `CMPONENTS\R2\PACKAGES\VDS11\UPDATE\UPDATE.EXE` found on Disc 2 of the Windows Server 2003 R2 software).
- For Windows Server 2003 SP2 or Windows Server 2008:
 - VDS 1.1 is included with these versions.
- VDS Hardware Provider (optional; available as part of Windows Storage Server)
- Microsoft iSCSI Software Initiator, version 2.06 or higher

Note: iSCSI support is available for Windows Server 2003 R2 (32-Bit), Windows Server 2003 SP2 (32-Bit), and Windows Server 2008 (32-Bit).

Limitations on 64-bit systems

This section describes limitations on 64-bit systems.

SFW cannot support ASR on disk groups that contain GPT partitions (295179, 327180, 855781)

On servers running Windows Server 2003, the automated system recovery (ASR) feature may fail to recover some or all of the disk groups of an SFW configuration of dynamic disks with GPT style formats.

The problem is a result of the Windows Server 2003 ASR code not being able to partition the GPT disks at restore time. On 64-bit systems, this is a known Microsoft Windows Server 2003 issue. Refer to Microsoft case 100-42023 for additional information.

Limitations of SFW support for Dynamic Multi-pathing (DMP)

This section describes limitations of SFW support for Dynamic Multi-pathing (DMP).

Load balancing policies of third-party MPIO DSMs are not supported in SFW (820077)

Load balancing policies and path settings of third-party MPIO DSMs are not supported in SFW. This is because third-party MPIO DSMs may not implement a common method in the Microsoft MPIO framework for getting or setting load balancing policies.

Disconnected paths may not be reflected in VEA GUI with MPIO DSMs installed (326603)

Disconnecting paths from a host using MPIO DSMs may not be reflected in the VEA GUI. The VEA GUI is not automatically updated because of a communication problem between SFW and WMI.

Workaround: Perform a rescan operation to allow SFW to obtain information about the disconnected paths.

Limitations of SFW with Exchange and SQL

The following is a limitation of SFW with Exchange and SQL.

Database or log files must not be on same volume as SQL Server (266133)

When using the `vxsnapsql` utility, user-defined databases and logs must not be stored on the same volume as the SQL Server program files or system data files.

Other issues

The following are other issues:

The boot.ini may not update after adding mirror (321557)

Adding a mirror to a dynamic system and boot volume that uses the MBR partition style may not update the `boot.ini` file. This issue is observed on servers running Windows Server 2003 (32-bit) and Windows Server 2003 x64 Editions on Xeon processors. The operation for adding the mirror completes successfully on these systems, but the `boot.ini` file that enables the server to boot from the mirror may not be updated automatically. An error message appears if the file is not updated automatically.

Workaround: Manually update the `boot.ini` file. Refer to Microsoft documentation for instructions on how to update the file.

Operations in SFW may not be reflected in DISKPART (100587, 101776)

If you perform an operation in DISKPART, it is reflected in the VEA GUI and the CLI. However, operations that are performed in SFW may not be automatically reflected in DISKPART.

Workaround: The workaround is to rescan in DISKPART to obtain these changes. The DISKPART utility does not support multiple disk groups, so it cannot reflect multiple disk groups that were created in SFW. DISKPART does indicate whether a disk is basic or dynamic

Disk signatures of system and its mirror may switch after ASR recovery (100540)

After an ASR recovery of a system with a mirrored system and boot disk, the disk signatures of the original system and boot disk and its mirror are sometimes switched.

The problem happens as a result of Microsoft's disk mapping algorithm. Under some conditions, the algorithm switches disk signatures. This is a known Microsoft issue.

Adding a storage group that contains many disks and volumes causes SFW and Microsoft Exchange System Manager to respond very slowly. (530035)

Adding or creating a storage group that has a dynamic disk group that contains many disks and volumes to an MSCS Exchange Virtual Server causes the VEA GUI and the Exchange System Manager GUI to respond very slowly. It seems that a greater number of disks and volumes increases the response time. This is a known Microsoft problem (SRX060621604113).

SFW does not support growing a LUN beyond 2 TB (704839)

Growing a dynamic disk that has the MBR partition style to a size of 2 TB or greater renders the disk unusable.

SFW cannot coexist with early Symantec Anti-virus software (804143)

Abnormal termination of SFW occurs when Symantec Anti-virus version 11.6.2 coexist on a system.

Workaround: Upgrade to Symantec Anti-virus version 11.6.8 or later.

Shrinking an NTFS volume that is greater than 2 TB is not supported (814881)

The Shrink Volume command does not support NTFS volumes that are greater than 2 TB. In addition, you may not be able to shrink the volume if the free space beyond the last used cluster is less than 1 MB.

SCSI reservation conflict occurs when setting up cluster disk groups

Setting up a cluster on Windows Server 2008 creates physical disk resources for all the basic disks on the shared bus. Later you create resources for the SFW cluster disk groups. Before doing so, you must remove any physical disk group resources for disks that are used in the cluster disk groups. Otherwise, a reservation conflict occurs.

Unused public view objects remain after upgrading to SFW 5.1 MOM 2005 pack

Upgrading an earlier version of the SFW MOM 2005 pack adds new public view objects, but it does not remove no longer used public view objects that were present in the earlier version. To remove these unused public view objects, follow the procedure about importing the SFW 5.1 MOM 2005 pack in the *Veritas Storage Foundation and High Availability Solutions Management Pack Guide for Microsoft Operations Manager 2005*.

Snapshot operation fails when the Veritas VSS Provider is restarted while the Volume Shadow Copy service is running and the VSS providers are already loaded

When the Volume Shadow Copy VSS service starts, it loads the Veritas VSS provider. If the Veritas VSS provider is restarted while the Volume Shadow Copy service is running and the VSS providers are already loaded, the snapshot operation fails with a VSS error (Event ID:12293).

When a node is added to a cluster, existing snapshot schedules are not replicated to the new node

When you create snapshot schedules in a clustered environment, schedule-related registry entries are created on all cluster nodes. When a failover occurs, the failover node can continue to run the schedules. However, if a new node is added to a cluster after the schedules are created, the schedules are not replicated to

the new node. If the service group fails over to the node that was added, the scheduled snapshot tasks do not occur.

Workaround: Start the Quick Recovery Configuration Wizard from the Solutions Configuration Center (**Start>Run>scc**). Continue through the wizard until the **Synchronizing Schedules** panel shows that synchronization between cluster nodes is complete. Click **Finish** to exit the wizard.

Restore from Copy On Write (COW) snapshot of MSCS clustered shared volumes fails (1796788)

On Windows 2003 and Windows 2008, the restore operation using a COW snapshot of MSCS clustered shared volumes fails. This is a known Microsoft problem (KB 945361).

Dynamic Disk Groups are not imported after system reboot in a Hyper-V environment (1406512)

In a Hyper-V environment, dynamic disk groups that reside on virtual disks that are attached to a SCSI controller are not imported automatically. This is a known Microsoft problem.

Workaround: Configure the system to use the Veritas DG Delayed Import Service (VxDgDI) for these dynamic disk groups. Alternatively, you can manually import these disk groups after the system has completed the boot process.

Storage Agent cannot reconnect to VDS service when restarting Storage Agent (1794522)

Stopping the VDS service while a VDS client is running on a system, results in a system error. Subsequently, stopping the Storage Agent and then restarting the Storage Agent, results in the Storage Agent not being able to reconnect to the VDS service.

All VDS clients, such as DISKPART, Storage Agent, or the Disk Management GUI, must be closed to avoid errors when stopping the VDS service and to enable the Storage Agent to be started again.

Workaround: When the VDS service is stopped resulting in a system error, the vxvdsdyn.exe and vxvds.exe processes must be terminated. Also ensure that the vds.exe process has been terminated.

Use the following commands to stop these processes:

```
TASKKILL /F /IM vxvdsdyn.exe  
TASKKILL /F /IM vxvds.exe  
TASKKILL /F /IM vds.exe
```

At this point, restarting the Storage Agent restarts the VDS service automatically.

SFW does not support transportable snapshots on Windows Server 2008

SFW does not support transportable snapshots on Windows Server 2008. SFW support for transportable snapshots is limited to Windows Server 2003.

Windows Disk Management console does not display basic disk converted from SFW dynamic disk (930388)

A basic disk that was converted from an SFW dynamic disk does not appear in the Windows Disk Management console or in the results of the `DISKPART list disk` command.

Workaround: The disk can be displayed in the Windows Disk Management console by performing a refresh or a rescan disks operation. In addition, the disk can be displayed in the results of the `DISKPART list disk` command by performing a `DISKPART rescan` operation first.

SharePoint components must have unique names (1851186)

When creating SharePoint components, ensure that the names of the components are unique. Performing operations on components with names that are not unique may cause unpredictable results.

DCM or DRL log on thin provisioned disk causes all disks for volume to be treated as thin provisioned disks (1601143)

Having a volume on a disk that is not a thin provisioned disk and then adding a DCM or DRL log that resides on a thin provisioned disk to the volume, causes the volume to be enabled for thin provision disk operations. Performing thin provision disk operations in this situation causes the operations to fail.

After import/deport operations on SFW dynamic disk group, DISKPART command or Microsoft Disk Management console do not display all volumes (1671337)

The Microsoft Disk Management console and `DISKPART` CLI command may not display all volumes after repeated import/deport operations are performed on an SFW dynamic disk group.

Symantec recommends that using SFW CLI commands instead of the Microsoft `DISKPART` command for scripts to monitor the status of volumes.

Restored Enterprise Vault components may appear inconsistent with other Enterprise Vault components (1780009)

Selected Enterprise Vault components that were restored may appear to be inconsistent with Enterprise Vault components that were not restored.

Inconsistencies may appear as dangling Saveset entries in a VaultStore database

or index, or a Saveset component with missing Saveset entries in a database or index.

Symantec recommends that the user verify the restored component and components dependent on the restored component.

Use the EVSVR.exe tool (available with the Enterprise Vault installation) for the verification operation.

Note: Any discrepancies that are discovered can be repaired with the EVSVR.exe tool that is available with Enterprise Vault 8.0 SP2.

Enterprise Vault restore operation may fail for some components (1788920)

The restore operation fails for an Enterprise Vault component when an open handle exists for a volume on which the component resides.

Workaround: Specify the **Force** option in the Enterprise Vault restore wizard or CLI command to allow the operation to proceed successfully.

VDS limits the length of a volume name (1598800)

On Windows Server 2008, Virtual Disk Service (VDS) limits the length of volume names. As a result, VDS commands may fail on SFW dynamic volumes that have names that are too long.

This is a known Microsoft issue and has been resolved with KB958556. KB958556 is automatically installed with this release.

Note: You must activate Windows before installing or upgrading to SFW 5.1 SP1, otherwise the installation of KB958556 fails.

Shrink volume operation may increase provisioned size of volume (1935664)

Performing a shrink volume operation on a volume that resides on a thin provisioned disk may result in an increase of the provisioned size of the volume.

Reclaim operations on a volume residing on a Hitachi array may not give optimal results (1922235)

Reclaim operations on a striped volume that resides on thin provisioned disks in Hitachi arrays may not give optimal results. This is due to the size of the allocation unit of the arrays.

Veritas Cluster Server

This section covers limitations specific to Veritas Cluster Server.

Windows Safe Mode boot options not supported (1234512)

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

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

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

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

File shares on Windows Server 2008 are not accessible using the virtual IP address (1214494)

File shares configured in VCS can be accessed using the virtual server name (ShareName attribute) or the virtual IP address on Windows Server 2003 systems. However, on Windows Server 2008, you are unable to access file shares using the virtual IP address. This is a restriction in the operating system.

You can access file shares using the virtual server name.

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

While configuring the cluster using the VCS Cluster Configuration Wizard (VCW) if you do not choose the secure mode (Use Single Sign-on option) on the **Configure Security Service Option** panel, VCW creates a user with user name as admin and password as password. The user credentials are auto-populated in the respective fields, by default. This user has administrative privileges to the cluster.

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

VCW does not support configuring broadcasting for UDP

VCW does not provide options to configure broadcasting information for UDP. You can configure broadcasting for UDP by manually editing the `l1ttab` file. Refer to the *Veritas Cluster Server Administrator's Guide* for more information.

Solutions wizard support in a 64-bit VMware environment

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

Cluster Manager (Java Console)

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

Latest version of Java Console for VCS is required

Cluster Manager (Java Console) from previous VCS versions cannot be used to manage VCS 5.1 SP2 clusters. Symantec recommends always using the latest version of Cluster Manager.

Running Java Console on a non-cluster system is recommended

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

All servers in a cluster must run the same operating system

All servers in a cluster must run the same operating system. You cannot mix 32-bit (x86), x64, or IA64 Windows operating systems within a cluster.

You cannot mix Windows Server 2008 (full install) systems and Windows Server 2008 Server Core systems within a cluster.

Service group dependency limitations

The following are Service group dependency software limitations.

No failover for some instances of parent group

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

System names must not include periods

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

Volume Shadow Copy Service is not supported

The MountV agent is not supported on volumes with the copy-on-write feature of Volume Shadow Copy Service enabled.

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

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

Lock by third-party monitoring tools on shared volumes

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

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

VCS lock on shared volumes during Exchange recovery

VCS monitors the shared volume used for storing Exchange databases. During online, offline, or clean operations, VCS MountV resources exclusively lock the shared volume. This exclusive lock may conflict with recovery of an Exchange volume.

Workaround: Symantec recommends freezing the service group containing the MountV resources before recovering Exchange volumes.

To recover an Exchange volume that is monitored by VCS

- 1 In the VCS Java Console, identify the service group containing the MountV resources corresponding to the volume to be recovered.
- 2 Freeze the service group.
 - In the **Service Groups** tab of the configuration tree, right-click the service group name.
 - Choose **Freeze**, then choose **Temporary** or **Persistent** from the menu.

- 3 Recover the Exchange volume.
- 4 Unfreeze the service group.
 - In the **Service Groups** tab of the configuration tree, right-click the service group name.
 - Choose **Unfreeze**, then choose **Temporary** or **Persistent** from the menu.

If custom resources are configured in VCS to monitor a snapshotted volume, follow the procedure before snapping back to the original or the replica.

Note: If you cannot lock a volume for snapback, you can either force the operation or fail the operation and await administrator intervention.

Schedule backups on online nodes

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

Undefined behavior when using VCS wizards for modifying incorrectly configured service groups (253007)

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

MirrorView agent resource faults when agent is killed (508066)

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

Exchange virtual servers are shown as non-reachable in the Exchange Service Manager (333108)

In a clustered Exchange 2003 configuration, the following issue is observed: Exchange virtual servers were displayed as non-reachable in the Exchange Service Manager (ESM) under tools, monitoring, and status, if the Routing Group Master is configured on the Exchange cluster nodes.

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

Cluster address for global cluster requires resolved virtual IP

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

Systems in a cluster must have same system locale setting

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

Virtual fire drill not supported in Windows environments

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

However, the **Fire Drill Wizard** available from the **Solutions Configuration Center** enables you to set up and run a fire drill on a disaster recovery environment that uses Veritas Volume Replicator replication.

Cluster Manager consoles do not update GlobalCounter

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

Symantec Product Authentication Service does not support node renaming

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

WAN cards are not supported

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

Disaster Recovery Configuration Wizard

The following is a Disaster Recovery Configuration Wizard software limitation.

DR Wizard does not create or validate service group resources if a service group with the same name already exists on the secondary site

If a service group with the same name as the one selected in the Disaster Recovery Wizard already exists on the secondary site, the Disaster Recovery Wizard does not validate the configuration or add missing resources.

Workaround: Remove the service group with the same name that exists on the secondary site. Then run the wizard again so that it can clone the service group that exists on the primary site.

Veritas Volume Replicator

This section covers limitations specific to Veritas Volume Replicator (VVR).

Resize Volume and Autogrow not supported in Synchronous mode (103613)

The Resize Volume and Autogrow operations are not supported when replication is done in Synchronous mode. While Synchronous replication is paused to resize volumes, writes necessary to grow the file system cannot occur.

Workaround: To resize the volume, temporarily change the mode of replication to Asynchronous or Synchronous Override. After you finish resizing the volume, you can switch replication back to the Synchronous mode.

Expand volume not supported if RVG is in DCM logging mode

VVR does not support the Expand Volume operation if the Replicated Volume Group (RVG) is in DCM-logging mode.

Solutions Configuration Center

This section describes the Solutions Configuration Center software limitations.

The Solutions Configuration Center and its wizards have signature verification disabled by default to speed startup time

A .NET Framework 2.0 managed application that has an Authenticode signature can take longer than usual to start because of signature verification. The Solutions Configuration Center and its wizards are such applications.

When you disable signature verification, the .NET Framework 2.0 managed application starts faster. Microsoft has provided a fix for this issue in .Net 2.0 SP1, which is deployed with SFW HA 5.1. The fix lets you disable the signature verification through use of a configuration file setting. Information on the fix is provided in the following article on the Microsoft support site:

<http://support.microsoft.com/kb/941990>

The SFW HA software installs the required configuration settings to disable the signature verification for the Solutions Configuration Center, its wizards, and the Plugin Host service used by these wizards.

Workaround: If you do not want to disable the signature verification, edit the following configuration file setting to change "false" to "true".

```
<configuration>
  <runtime>
    <generatePublisherEvidence enabled="false"/>
  </runtime>
</configuration>
```

The configuration files to edit are the following files in the [InstallDirectory]\Veritas\winsolutions\bin\directory:

- CEngineDriver.exe.config
- PluginHost.exe.config
- SFWConfigPanel.exe.config

Quick Recovery wizard displays only one XML file path for all databases, even if different file paths have been configured earlier

When running the Quick Recovery wizard, the XML file path you specify applies to all the databases selected in that run of the wizard. If you schedule databases in separate runs of the wizard, you could specify a different XML file path for each database. However, if you later run the wizard to modify the snapshot schedule and select more than one database, the Quick Recovery wizard displays the XML file path for the first database only.

Workaround: If you want to view the XML file path of each database, run the wizard again and specify one database at a time to modify.

Disaster Recovery, Fire Drill and Quick Recovery wizards fail to load unless the user has administrative privileges on the system

Disaster Recovery, Fire Drill, and Quick Recovery wizards require that the user have administrative privileges on the system where they are launched. If a user with lesser privileges, such as user privileges, tries to launch the wizards, the wizards will fail to load, with the message "Failed to initialize logging framework".

Discovery of SFW disk group and volume information sometimes fails when running Solutions wizards (1802119)

Discovery of Storage Foundation for Windows disk group and volume information may fail when running a Solutions wizard. This issue applies to the Fire Drill Wizard, Quick Recovery Configuration Wizard, or the Disaster Recovery Configuration Wizard.

To workaround this known discovery failure issue

- 1 Make sure that the Storage Agent service is running on the target system.
- 2 From the VEA console, click **Actions** > **Rescan** to perform a rescan.
- 3 Restart the wizard.

Known issues

The following known issues exist in this release of the product.

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

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

Installation, upgrades, and licensing

This section provides information on known installation, upgrade, and licensing issues.

Installer may fail during uninstallation

This issue occurs when you try to remove 5.1 SP2 from the cluster nodes. The Veritas Product Installer (VPI) may fail with an msi error. (2137388)

The installer post-uninstall summary panel may display the following error:

Error 1704.An installation for Microsoft Windows SDK for Windows Server 2008 Samples (6001.18000.367) is currently suspended. You must undo the changes made by that installation to continue. Do you want to undo those changes? Product: <product msi module name>

The VPI logs may additionally contain the following message:

Error 1712.One or more of the files required to restore your computer to its previous state could not be found. Restoration will not be possible. Product: <product msi module name>

Workaround

Close VPI and then reboot the system where the uninstallation has failed. After the system reboots, run the uninstallation again.

"Run Configuration Checker" link available on the CD browser only downloads the Configuration Checker (2143564)

The "Run Configuration Checker" link available on the CD Browser, enables you to only download the Configuration Checker. To launch the Configuration Checker, you must navigate to the directory path and double-click the setup.exe

"hareg.exe not found" error may occur while upgrading to 5.1SP2 (2140973)

"hareg.exe not found" error may occur during the upgrade process.

Workaround:

Ignore and close the error message. The software upgrade process is completed without any issues.

Upgrading to a permanent license, using the License Management option requires you to remove all the demo license keys (2143557)

Using the License Management option, if you choose to upgrade the SFW HA license key to a permanent license, you must remove all VCS and SFW demo licenses.

Additionally,

While upgrading the license key to a permanent license using the License Management option, the wizard may display "invalid license key" error, inspite of entering the valid key.

Workaround:

Close the error and relaunch the wizard.

Upgrading to 5.1SP2 from 5.0 RP2 may get held up with "IDriver.exe - Machine Type Mismatch" error (2142204)

While upgrading to 5.1SP2 from 5.0RP2, the product installation may get held up at certain stage with the following error.

```
-----  
IDriver.exe - Machine Type Mismatch  
-----
```

The image file C:\Program Files\Veritas\Security\Authentication\bin\InstHelper64.exe is valid, but is for a machine type other than the current machine.

Note: If you are using a non-console remote desktop connection, the above error might not be visible.

Workaround:

Click **OK** to continue with the installation.

SFW HA installer may fail if you try to remove the base product (2031945)

The product installer may fail if you try to remove the base SFW HA product on the systems where you have installed SP1AP1.

This issue occurs if you have installed SP1AP1 on systems where the product installation order was any of the following:

SFW HA 5.1 > SFW HA 5.1 AP1 > SFW HA 5.1 SP1

or

SFW HA 5.1 > SFW HA 5.1 SP1

Workaround: If you wish to remove the base product in such a configuration, you must first remove SP1AP1 completely and then proceed to uninstalling the base product.

hastop.exe command prompt may remain open when the installer fails to stop HAD (2141297)

While upgrading to or repairing the 5.1SP2 installation, the product installer stops the required services. While stopping HAD, a command prompt "hastop.exe" may launch. If HAD fails to stop in defined time out, the installer stops and does not proceed with the installation. However, the command prompt "hastop.exe" remain open.

Leaving the command prompt open may lead to handle leak.

Workaround:

You must manually close the command prompt.

On a Windows Server 2008 or 2008 R2 node, installer may fail to restart the services after the installation is complete (2140506)

The product installer may fail to restart the services, if the logged on user account does not have the required administrative privileges on the cluster node.

This issue occurs even if you choose to log on using the User Access Control (run as administrator) option.

Solutions Configuration Center not refreshed by installation or uninstallation (2025404)

If you leave the Solutions Configuration Center (SCC) window open during Application Pack 1 installation, the SCC window does not refresh to show the new content when installation is complete. The same applies if you uninstall Application Pack 1.

Workaround: To refresh the window, close the SCC window and then re-launch the SCC. You can launch the SCC from **Start > All Programs > Symantec > Veritas Storage Foundation > Solutions Configuration Center** or from **Start > All Programs > Symantec > Veritas Cluster Server > Solutions Configuration Center**.

Uninstalling Service Pack 1 may fail to remove certain VCS files (1857987)

If you remove Service Pack 1, the product installer may fail to remove the following files from the %VCS_Home%\bin directory:

- AppManager.exe
- AppManager_Lang_en.dll
- Clusterize.exe
- MQHelp.dll

`%VCS_Home%` is the product installation directory for VCS, typically, `C:\Program Files\Veritas\Cluster Server`

This issue occurs if you install and then uninstall Service Pack 1 on systems where the following releases were installed:

- SFW HA 5.1
- SFW HA 5.1 AP1

Workaround: You may have to delete the files manually.

FlashSnap License error message appears in the Application Event log after installing license key (1862627)

When an evaluation copy of SFW with the FlashSnap feature is installed on a system, and then later a permanent license key for SFW that does not have the FlashSnap feature is installed on it, an error message is logged periodically in the Application Event log:

```
Storage Foundation FlashSnap License is not installed
```

To avoid having the error message logged in the Application Event log, use the **Add or Remove Programs** of the **Windows Control Panel** to remove the demo license and add the permanent license key.

SFW or SFW HA 5.1 SP1 installation or upgrade do not support parallel installations or upgrades (1808521)

When installing or upgrading to SFW or SFW HA 5.1 SP1, ensure that there are no parallel installations, live updates, or Microsoft Windows updates in progress.

Activate Windows before an installation on Windows Server 2008 (1793374)

Before proceeding with an installation of the 5.1 SP1 software on a server running Windows Server 2008, activate Microsoft Windows. If you do not activate Windows before an installation, an “Optional update delivery is not working” pop-up may appear warning that you may be a victim of software counterfeiting.

Servers where you are installing the 5.1 SP1 software that are running Windows Server 2008 SP2 or Windows Server 2008 R2 do not require a Microsoft Windows activation before installation.

Installation may intermittently fail on one or more systems (1673123, 2144673)

SFW HA installation may intermittently fail on one or more systems.

You may see the following error in the logs:

```
Action start 17:13:13: InstallFinalize.  
DEBUG: Error 2356: Couldn't locate cabinet in stream:  
Data1.cab.  
Internal Error 2356. Data1.cab
```

Workaround: If this problem occurs, exit the installer and then launch the installer again and continue reinstalling.

Veritas VDS Dynamic Provider fails during upgrade to SFW 5.1 SP1 (1721051, 1729259)

When upgrading SFW 5.1 to SFW 5.1 SP1, Veritas VDS Dynamic Provider (vxvds.exe) may fail with an error. This situation occurs when Veritas VDS Dynamic Provider is working on SFW operations during the upgrade.

Workaround: Ensure that Veritas VDS Dynamic Provider has completed working on SFW operations before starting the upgrade operation.

Log on to remote nodes before installation (106013)

Installation on a remote node may fail if the user does not first log on to the remote node. This situation occurs when using a domain account and the installer to install on a remote machine that has just joined the domain. If the user does not log on to the remote node before installing, the node will be rejected and fail the validation phase of the installation. For remote nodes that join the domain, there is a security requirement that the user must log on to the node at least once before the node can be accessed remotely.

SFW and SFW HA install registry keys with read-write permission for Power Users group (964870)

On Windows Server 2003, the Veritas Storage Foundation for Windows and Veritas Storage Foundation HA for Windows products install registry keys in `HKEY_LOCAL_MACHINE\Software\Veritas` with read-write permissions for members of the Power Users group. If desired, you can set more restrictive permissions on these keys using the Microsoft tool `subinacl.exe`.

This tool is part of the Windows Server 2003 Resource Kit Tools and is available from the following website:

<http://www.microsoft.com>

SFW HA 5.1 SP2 upgrade or install failure with “another installation in progress” error message (1809142)

When installing or upgrading to SFW HA 5.1 SP2, the installation or upgrade may fail with "another installation in progress" error message.

If this problem occurs, exit the installer and make sure that all the other installations running on the machine are stopped, then launch the installer again and continue reinstalling.

Upgrading to SFW HA 5.1 SP2 from earlier versions (SFW HA 5.0 RP2, 5.1, or 5.1 AP1) may cause a vxatd.exe and/or vxpal.exe error report (1808718)

Upgrading to SFW HA 5.1 SP2 from earlier versions (SFW HA 5.0 RP2, 5.1, or 5.1 AP1) on a cluster is successful, but after the reboot a Windows error report appears indicating that the vxatd.exe and/or vxpal.exe have crashed. However, this issue does not seem to affect any functionality and can be ignored.

For additional information or updates about this issue:

<http://www.symantec.com/docs/TECH77132>

Internationalization

The following known issues may be observed when running Storage Foundation for Windows or Storage Foundation HA for Windows in locales other than U.S. English.

Timestamp in Veritas Cluster Management Console logs reflects Pacific Standard Time (PST) or Pacific Daylight Time (PDT) (847646)

The timestamp for Veritas Cluster Management Console logs is recorded and displayed only in Pacific Standard Time (PST) or Pacific Daylight Time (PDT) regardless of your system's local time zone setting. For example, even after you set your system's time zone to your local Beijing Time, CMC logs are recorded and displayed only in PST or PDT depending on the time of the year.

Only U.S. ASCII characters are supported in file paths (862762, 860579, 860186)

File paths including non-ASCII characters are not supported by SFW or SFW HA.

Workaround: Use U.S. ASCII characters only when naming servers, clusters, disk groups, databases, directories, files or anything that may be included in a file path.

Language preference in Veritas Enterprise Administrator (VEA) must be set to English (United States) or Japanese (Japan) (849597)

You can set the display language preference for the Veritas Enterprise Administrator (VEA) console by selecting Tools > Preferences. However, after selecting languages other than English (United States) or Japanese (Japan),

displayed characters will be corrupted and unreadable even if you have the local language's character set installed in your system and the system's default language is set for your local language. The Japanese (Japan) displays properly only if the SFW Japanese language pack is installed. In Japanese, SFW or SFW HA displays most screens, buttons, and descriptions in Japanese.

Workaround: Select only English (United States) or Japanese (Japan) as the display language.

General issues

This section provides information about general issues.

Troubleshooting errors (766137)

Unexplained errors in the Quick Recovery configuration wizard or Disaster Recovery configuration wizard may be resolved by stopping and then starting the Plugin Host service. Note that Restart does not resolve the issue.

VMDg resource may not failover in a cluster environment (774442)

When a node is rebooted or fails in an MSCS or VCS environment that uses the SCSIPort driver, the VMDg resource may not failover to another node. The problem is that too many SCSI bus reset commands are sent down each bus during the failover. This is a result of the SCSIPort driver converting the SCSI break reservation command that is sent to each disk to a SCSI bus reset command.

Workaround: The workaround is to set the registry key, `HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\VxSvc\CurrentVersion\VolumeManager\UseBusReset`, to a `REG_DWORD` value of 1.

This ensures that only one bus reset command is sent down each bus during the failover.

Symantec PBX installation proceeds even when reserved port is occupied (801671)

Private Branch Exchange (PBX) provides single-port access to clients outside the firewall connecting to various services offered by Symantec products. Port 1556 is reserved for the PBX service. If port 1556 is occupied by another service, the SFW or SFW HA installation will complete, however the PBX service will fail to start.

Additionally, port 1557 is used for legacy (pre CSF 1.2.1) services to register with PBX Exchange. If port 1557 is not available, then legacy services may not be able

to register with exchange, and a warning message will be displayed in the exchange log files. However, the PBX service will continue to run if port 1556 is available.

Workaround: Before installing SFW or SFW HA, ensure that port 1556 is available.

Backup Exec 12.x fails to list the volumes and database instances of a clustered Microsoft SQL server (1879274)

On Windows Server 2003 x64 systems, Symantec Backup Exec 12.x fails to list the volumes and the database instances of a clustered Microsoft SQL server.

Workaround: The workaround is to restart the Backup Exec “Remote Agent for Windows Systems” services on the systems where the SQL instances are running. For information about how to restart the “Remote Agent for Windows Systems” service, see *Symantec Backup Exec 12.5 for Windows Servers Administrator's Guide*.

Veritas Storage Foundation

This section provides information on known Storage Foundation issues.

Enterprise Vault (EV) snapshots are displayed in the VEA console log as successful even when the snapshots are skipped and no snapshot is created (2142378)

When Enterprise Vault component's snapshot is created from the VEA console or using Vxsnap CLI, then the VEA console log displays the snapshot as being created successfully even when no snapshot is created and the snapshot operation fails. This issue is seen when there is a problem with remote communication.

Workaround: Make sure that the Scheduler service is configured with Domain admin credentials and restart the Symantec Plug-in Host service if remote communication is not working and delete any previously prepared snapshot mirrors. Perform a **Prepare** operation again and then take a snapshot of the Enterprise Vault components.

BSOD 0xCA during install of DDI-1 when array connected over iSCSI with MPIO (2082546)

Bluescreening of setup nodes while installing Device Driver Integration (DDI)-1 for Storage Foundation for Windows 5.1 Service Pack 1.

Workaround: Reconfigure MS iSCSI initiator without the MPIO option enabled and then install the Device Driver Integration (DDI-1) package.

On a Windows Vista x86 node, the VEA fails to launch with a "MSVCR71.dll not found" error (2059877, 2132462)

This issue occurs when the Veritas Enterprise Administrator (VEA) cannot find MSVCR71.dll under C:\Program Files\Veritas\Veritas Object Bus\bin" on the node.

Workaround: To launch the VEA successfully, copy MSVCR71.dll from "C:\Program Files\Veritas\Veritas Object Bus\eat\bin" to "C:\Program Files\Veritas\Veritas Object Bus\bin".

Takeover and Failback operation on Sun Controllers cause disk loss (2084811)

DSMs report IO errors in case of a takeover and failback operation leaving the volume degraded. This happens both for a standalone setup & clustered setup.

In a disk group with Thin Provisioning (TP) disks, deporting forcibly while reclaiming at the disk group level causes the reclaim operation to never return back (2138005)

Deporting forcibly while reclamation is at progress on a diskgroup having thin provisioning disks gives the error **Failed to complete the operation...**

V-76-58645-382: Dynamic disk group was deported with active I/O.

Workaround: Do a manual refresh to get the disk groups to a normal state.

SFW DSM for Huawei does not work as expected for Huawei S5600T Thin Provisioning (TP) LUNs (2725582)

In SFW 5.1 SP2, Thin Provisioning Reclaim support is available for Huawei S5600T arrays only if hotfix Hotfix_5_1_20051_87_2683797 is installed. This issue occurs after the hotfix installation.

In case the active paths are disabled, the I/O fails over to the standby paths. When the active paths are restored, the I/O should fail back to the active paths. But in case of Huawei S5600T TP LUNs, the I/O runs on both active as well as standby paths even after the active paths are restored. This issue occurs because Huawei S5600T TP LUN does not support A/A-A explicit trespass.

The SFW DSM for Huawei functions properly for Huawei S5600T non-TP LUNs.

Workaround: To turn off the A/A-A explicit trespass, run the following commands from the command line:

```
vxddmpadm setdsma lua explicit=0 harddisk5
```

```
vxddmpadm setarray lua explicit=0 harddisk5
```

On a clustered setup, split-brain might cause the disks to go into a fail state (2076136)

In a Cluster Environment, Split-brain might cause disks and volumes to go into a failing state.

During internal testing it is observed with HP MSAP2000 array that after split-brain, disks are going into a failing state. This is due to some of the SCSI reservation commands taking longer time than expected.

Workaround: Reactivate the volumes and disks from the VEA console manually and then online the ServiceGroup in case of a VCS setup and online the ApplicationGroup for MSCS from the clustered GUI console.

To avoid this in future, increase the value of registration time in the registry. Create a DWORD key with name `RegistrationTimer` and value should be calculated as below: "IF SCSI-3 is enabled from SFW {3 seconds for each disk in the disk group; number of disks in the disk group (DG) => sleeping reservation for the going to be online DG}". Value should be specified in Milliseconds. Default value of this key is 7000 (7Secs).

The Veritas Enterprise Administrator (VEA) console cannot remove the Logical Disk Management (LDM) missing disk to basic ones (1788281)

This issue is intermittently produced and there is no workaround for this issue.

After breaking a Logical Disk Manager (LDM) mirror volume through the LDM GUI, LDM shows 2 volumes with the same drive letter (1671066)

Volume state is properly reflected in Diskpart. Issue is seen only in disk management (diskmgmt) MMC.

Workaround for this issue is as shown below:

To reflect the proper volume state in the diskmgmt console

- 1 If disk management console is open, then close it.
- 2 Run the command `net stop vxvm`
- 3 Stop vds by running `net stop vds`
- 4 Restart the vxvm service by running `net start vxvm`.
- 5 Now, restart the disk management console .

Unable to failover between cluster nodes. Very slow volume arrival (2104970)

Slow disk import because of large number of COW snapshots. Significant amount of time is spent in comparing disks.

Workaround: Disable the COW processing on disk group Import by creating the following DWORD registry key

```
SOFTWARE\VERITAS\Vxsvc\CurrentVersion\VolumeManager\DisableCOWOnImport=1
```

Blue screening noticed after clussvc crash while creating a VSS snapshot (2118628)

While taking the VSS backups, the clussvc crashes and system blue screening is noticed.

Workaround: Install Microsoft KB at: <http://support.microsoft.com/kb/950267>

Snapshot operation might fail with "Invalid Arguments" Error (2115125, 2126918)

If Refresh or Rescan operations are performed when VSS snapshots or Scheduled snapshots are going on, then the resulting Snapshot might fail with error "**Failed to complete the operation... V-40-32775-87: Invalid arguments.**"

Workaround: Retry the snapshot operation.

VDS errors noticed in the event viewer log (2123491)

If a user performs a rescan or reboot operation on the passive node when storage is being mounted on the active node, then the following event is noticed in the event viewer "**Unexpected failure. Error code: AA@02000018**". Note that this issue does not cause any harm or unexpected behavior.

Removing the VMDg resources from a service group to available storage from the Failover Clustering MMC results in an 'Assertion Failed' error (2080714)

When the Volume Manager Disk Group (VMDg) resource is removed from a service group, then the delete operation throws an '**Assertion Failed**' error. Clicking on **Retry** may cause the entire Failover Clustering MMC to hang up.

Workaround: Fix for the above issue is to upgrade from Windows Server 2008 SP1 to Windows Server 2008 SP2 as this issue is specific to Windows Server 2008 SP1 only.

On a Windows Server 2008 R2 x64 setup, after destroying a Storage Foundation for Windows (SFW) disk group, cannot create a Logical Disk Manager (LDM) disk group on the same disks (1878059)

When moving disks that have just been removed from an SFW dynamic disk group to LDM dynamic disk group, or creating an LDM dynamic disk group from those disks, the following error is shown : Warning V-40-32775-87. Invalid arguments. Note that this only happens on a Windows Server 2008 R2 x64 setup.

Workaround: Run diskpart rescan and repeat the operation.

Restore with `-a` option for component-based snapshot fails for Exchange mailboxes on a VCS setup (1873821)

Create a component-based normal snapshot on, say for example on, `C:\ vxsnap -x witha.xml create writer="microsoft exchange writer" component=Final`. Now run the `vxssnap restore` command with the `-f` and `-a` option. Restore operation fails because it tries to restore mounted databases when used with the `-a` option.

Workaround: Do either of the following to avoid the restore operation from failing:

- Dismount the mailbox before the restore operation.
or
- To avoid this problem fully restart the storage agent service once after the service group is online after the initial setup.

An extra GUI Refresh is required to ensure that changes made to the volumes on a cluster disk group having the Volume Manager Disk Group (VMDg) resource gets reflected in the Failover Cluster Manager Console(2123496)

Workaround: To reflect the changes made to the cluster disk group, go to the Cluster name, right-click on it and perform a Refresh. The changes get reflected in the Failover Manager console.

DR wizard cannot create an RVG that contains more than 32 volumes (2010918)

For VVR replication, the DR wizard cannot create a Replicated Volume Group (RVG) that contains more than 32 volumes. If you select more than 32 volumes while running the DR wizard, the create RVG task fails when you reach the Implementation panel.

To configure DR when any RVG contains more than 32 volumes, use the following steps:

- 1 Run the DR wizard until the Application Installation panel is displayed and then exit the wizard.
- 2 Complete the application installation on the secondary nodes.
- 3 Using the Veritas Enterprise Administrator (VEA) console, create a replicated data set (RDS) with a Primary and Secondary RVG with only 32 volumes. Do not select more than 32 volumes in the create RVG operation.

For more information on creating an RDS, see the *Veritas Volume Replicator Administrator's Guide*.

- 4 Once the RVG is created, right click on the RDS name and select **Add Volume**. Using the Add Volume wizard, add the remaining volumes that are part of the RVG.
- 5 Finish running the DR wizard to complete the service group cloning, replication configuration, and global cluster option (GCO) configuration.
- 6 In the VEA, change the IP address in the replication settings to match what you entered for the replication IP in the DR wizard, as follows:
 - Open the VEA and connect it to a system on the primary site where the primary RVG is configured. From the same VEA GUI, connect to a system on the secondary site where the secondary RVG is configured.
 - Go to Replication Network View.
 - Right click on the secondary RVG and select **Change Replication Settings**.
 - Change the primary side IP address and secondary side IP address to the same values which you provided in the DR wizard on the Replication Attribute Settings panel.

Allow restore using the vxsnap restore command if mailbox is removed or missing (2013769)

If a mailbox database component is missing or deleted from an Exchange 2010 configuration, then use the `vxsnap restore` command to recover the missing or deleted database component.

To restore a missing database, perform the following steps:

- 1 Create mailbox with same name as that of the missing mailbox database and mention the same database file and log path.

Make sure to uncheck the **Mount this database** checkbox.

- 2 Set the database properties by right-clicking the database and enabling the checkbox **This database can be overwritten by a restore** option in the Exchange Management Console.

- 3 Now try to restore the missing database using the vxsnap restore command.

```
vxsnap -x <filename> [-f] [-b] [-r] [-a] restore  
restoreType=<PIT|POF> writer=<writername>  
[subComponent=<subComponentName>] [RSG=<Yes|No>]
```

Note that the subcomponent and RSG=Yes|No is not valid for Exchange 2010.

Scheduled VSS snapshots of an Exchange mailbox database configured under a VCS cluster setup starts with some delay of around 2 to 3 minutes (2021279)

Prepare and Create VSS snapshot operations starts with some delay and takes sometime to get launched, mostly 2 to 3 minutes.

Event viewer shows error message "Could not impersonate Veritas Scheduler Service login user" when VSS restore and snapback operations are performed (2028835)

In case of an Exchange 2010 VCS cluster setup, if the Scheduler Service is stopped then the user may get the following error message **Could not impersonate Veritas Scheduler Service login user. Make sure this service is started and configured with a domain user account** in the VEA console and Application event log.

Workaround: If a Fileshare resource is configured for a VCS cluster setup, ensure that the Veritas Scheduler Service is running and configured with an appropriate user account. If snapshot metadata files are stored on a local volume, then this error can be ignored.

For a cluster setup, configure the Veritas Scheduler Services with a domain user account

In case of a clustered (VCS or DAG/MSCS) setup with more than one node, on each node of the cluster you must configure the Veritas Scheduler Services with a domain user account that has administrative privileges.

Sometimes VSS snapshot schedules are not visible under the Exchange node in the VEA console tree-view but are visible on the right pane of the console (2028805)

Create VSS Snapshot Schedules for an Exchange 2010 mailbox database. Expand the **Scheduled Tasks > Exchange Node** on the left pane of the VEA tree-view. It is noticed that the schedules are not visible under the Exchange node on the left pane but on the right pane of the VEA GUI.

Workaround: Perform a VSS refresh. The snapshot schedules get displayed under the Exchange node in the tree-view on the left pane.

Snapshot metadata files are not deleted after VSS Snapback and PIT Restore operation (2030283)

For an Exchange 2010 VCS cluster setup that has a fileshare resource configured to store snapshot metadata files, it is noticed that after performing a VSS Point in Time (PIT) restore or snapback operation the snapshot metadata files are not deleted even though the restore or snapback operation completes successfully. These snapshot files are displayed in the VSS restore and snapback wizards.

Workaround: Manually delete the older snapshot metadata files or if there is requirement to use the same file name, then use the -o option with the vxsnap utility command.

For example if \\FSAP1\share\mb1.xml is the snapshot set file name specified during Create snapshot operation, then files with the names mb1.xml\$, mb1.xmlwmd, and mb1.xml should be deleted. They are present at the location \\FSAP1\share.

If an inaccessible path is mentioned in the vxsnap create CLI, the snapshot gets created and the CLI fails (2030292)

If a wrong path or path which is not accessible is specified during the VSS create snapshot operation, then the operation fails after actual snapshot of the volumes and while generating a snapshot metadata file.

Workaround: Perform manual snapback of the volumes which are part of a component and take a VSS snapshot again by specifying a valid and accessible path.

If snapshot set files are stored on a Fileshare path, then they are visible and accessible by all nodes in the VCS cluster

If snapshot metadata files are stored on a fileshare path, they are visible and accessible by all nodes in a VCS cluster. Hence, VSS restore and reattach operations should be performed only on a node where the Exchange mailbox is online.

If a VCS resource database is configured for an Exchange 2010 mailbox database, the same database node appears in the VEA console tree-view more than once (2028846)

Workaround: Perform manual vxsnap refresh operation to refresh the VEA console.

Storage Management issues

The following are Storage Management issues.

Mirrored volume in Microsoft Disk Management Disk Group does not resynchronize (1150292)

On Windows Server 2008, a mirrored volume in a Microsoft Disk Management Disk Group does not resynchronize when a failed mirror is reattached.

Workaround: Reactivate the disk and resynchronize the volume using Microsoft Disk Management.

Expand volume operation not supported for certain types of volumes created by Microsoft Disk Management (1128016)

The resize operation to expand a volume created by Microsoft Disk Management is not supported for mirror, stripe, or RAID-5 volumes. Also, extending a volume to more than one disk in a single operation is not supported. A volume can only be extended on one other disk during a resize operation. However, the resize operation can be repeated so that the volume can be extended to more than one disk.

Snapshot and Restore issues

The following are Snapshot and Restore issues.

Vxsnap restore CLI command fails when specifying a full path name for a volume (1897541)

Specifying a full path name for a volume in the `vxsnap restore` CLI command fails with an error message, "The volume is not present in the snapshot."

Workaround: Specify either the drive letter or the drive path of the volume in the `vxsnap restore` command instead of specifying the full path name of the volume.

Restoring COW snapshots causes earlier COW snapshots to be deleted (1864268)

On Windows Server 2008, when restoring all earlier COW snapshots in reverse chronological order (restoring the latest snapshot to the earliest snapshot) causes earlier COW snapshots to be deleted. These COW snapshots are deleted after the second COW snapshot is restored.

Workaround: This is a known Microsoft problem. Refer to Microsoft KB975803 for more information.

(<http://support.microsoft.com/default.aspx?scid=kb;EN-US;975803>)

COW restore wizard does not update selected volumes (1881148)

The COW restore wizard requires that the snapshot set (XML file) be specified for the restore operation. The specification of the snapshot set allows the wizard to display the volumes associated with the snapshot set.

When you specify the snapshot set, continue to view the volumes to restore, and then go back to specify a different snapshot set, the volumes associated with the new snapshot set are not displayed in the **Select Volumes** screen of the wizard. The volumes that are displayed are the volumes associated with the first snapshot set.

Workaround: Cancel the COW restore wizard and launch it again specifying the appropriate snapshot set.

Snapshot operation requires additional time (1872810)

On Windows Server 2008, creating a new snapshot volume by performing a snapshot operation (mirror break) on a volume that already has a COW snapshot volume, and then performing an operation on this snapshot volume (e.g. assigning a drive letter, restore, or a snapshot operation that assigns a drive letter) requires additional time to complete.

Subsequent operations on the snapshot volume do not require additional time.

Incorrect message displayed when wrong target is specified in vxsnap diffarea command (1879829)

Issuing the `vxsnap diffarea -c` CLI command with the wrong value for the target parameter results in the display of an incorrect error message in the VEA console and in the Windows Event Viewer. The incorrect message that is displayed is "Failed to remove shadow storage area". The correct message that should be displayed is "Failed to change shadow storage area".

However, the correct message is displayed in the CLI command window.

Restore operation specifying missing volume for SQL component fails (1876307)

The operation to restore an SQL component specifying a missing volume fails when the operation has completed and the drive letter of the restored volume is changed to the drive letter of the original volume.

Workaround: Change the drive letter of the snapshot volume to the drive letter of the original volume before starting the restore operation.

Restore operation fails in VCS environment (1873821)

In a VCS environment on Windows Server 2003, the restore operation, with the -a and -f options, fails. The operation fails because the database does not dismount.

Workaround: There are two workarounds for this issue. The first workaround is to dismount the Mailbox manually before starting the restore operation. The second workaround is to restart the VxVM service after the Exchange service group is available under VCS. (You have to restart the VxVM service after every reboot of the operating system.)

Taking a snapshot of a remote SharePoint component results in an error (1793064)

When a snapshot operation is performed from a SharePoint front-end server running on Windows Server 2003, the snapshot of a remote SharePoint component fails with a VSS_E_BAD_STATE error message.

Microsoft SharePoint only supports the snapshot of a remote component if local components/volumes is snapshot together with remote components running on a Windows Server 2003 system. Microsoft SharePoint on Windows Server 2008 does not have this limitation.

This is a known Microsoft problem. Refer to Microsoft KB 976461 for more information about this problem.

(<http://support.microsoft.com/default.aspx?scid=kb;EN-US;976461>)

An approach that can be used to avoid this issue is to use a Windows Server 2008 Web Front End server in the SharePoint farm to run the snapshot operation.

Snapshot operation of remote Sharepoint database fails when it resides on local SharePoint server (1847861)

After configuring a remote database with a separate machine name and IP address on the local SharePoint server, taking a snapshot of the database fails.

This situation creates a call-back loop and returns the error condition, snapshot operation already in progress.

Snapshot of Microsoft Hyper-V virtual machine results in deported disk group on Hyper-V guest (1859745)

Creating a dynamic disk group with SCSI disks on a Hyper-V guest machine and then taking a snapshot of the Hyper-V guest with the Hyper-V host causes the disk group to be deported.

Enterprise Vault restore operation fails for remote components (1729872)

The restore operation fails for an Enterprise Vault component, when a part of the component resides on the local server and a part resides on a remote server. An open handle may exist on a volume where one of the parts reside causing the operation to fail.

Workaround: Specify the Force option in the Enterprise Vault restore wizard or CLI command to allow the operation to proceed successfully.

Persistent shadow copies are not supported for FAT and FAT32 volumes (1779879)

A shadow copy is persistent when it is not deleted after a backup operation. A persistent shadow copy is only supported for NTFS volumes. They are not supported for FAT or FAT32 volumes. This is a known Microsoft problem. Refer to Microsoft technical support for more information about this problem. ([http://msdn.microsoft.com/en-us/library/aa384613\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa384613(VS.85).aspx))

Copy On Write (COW) snapshots are automatically deleted after shrink volume operation (1863910)

On Windows Server 2008, the operation to shrink a volume that contains a shadow storage area causes VSS to delete any shadow copies (COW snapshots) that reside on the volume.

Restore operation from a Copy On Write (COW) snapshot fails in VCS environment (1729872)

On a Windows Server 2003 system, after a failover in a VCS environment, restoring from a COW snapshot fails. The DiffArea settings on the failing node are not transferred to other nodes. This prevents restoring from a COW snapshot.

Workaround: There are two workarounds to address this issue. Either of these workarounds can be performed.

- One way is to transfer the DiffArea settings to another node so as to manually copy the registry entry for the DiffArea settings to the selected node.

The registry path for the DiffArea settings is

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
```

```
VSS\Volumes\Associations.
```

- The second way is to create a VCS regrep resource for the key so that the key automatically replicates on the cluster nodes.

Create a VCS regrep resource for

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\  
VSS\Volumes\Associations.
```

Shadow storage settings for a Copy On Write (COW) snapshot persist after shrinking target volume (1592758)

On Windows Server 2008, the shadow storage (DiffArea) setting for the size of the target volume does not change after shrinking the size of the target volume to less than minimum size. The DiffArea settings for the size of the target volume reflect the DiffArea size of the target volume before the shrink operation.

Copy On Write (COW) shadow storage settings for a volume persist on newly created volume after breaking its snapshot mirror (1678813)

On Windows Server 2008, the shadow storage (DiffArea) settings for a volume are applied to the newly created volume after breaking the snapshot mirror. These shadow storage settings can be displayed with the `vxsnap refresh` CLI command.

Conflict occurs when VSS snapshot schedules or VSS snapshots have identical snapshot set names (1303549)

An XML file is created when a VSS snapshot is taken. This XML file contains database and snapshot volume metadata. If two snapshot schedules, or a snapshot schedule and a VSS snapshot, are created with the identical snapshot set name and directory path, the schedule that is launched later overwrites the XML file that was created by the schedule or VSS snapshot operation that was launched earlier.

Since the earlier XML file does not exist, subsequent VSS reattach/VSS restore operations for that schedule or snapshot fails.

Workaround: Ensure that snapshot set names are unique in a given directory path to avoid conflict with other VSS snapshot schedules or VSS snapshots.

Memory leak occurs during snapshot and snapback operations (1234278)

A memory leak occurs during snapshot and snapback operations when the Microsoft Virtual Disk Service (VDS) is called. VDS causes the memory leak.

This is a known Microsoft problem. Refer to Microsoft technical support for more information about this problem.

Microsoft Outlook 2007 Client (caching mode enabled) does not display restore messages after VSS Exchange restore operation completes (1287199)

After a VSS Exchange restore operation completes, restore messages are not displayed in the Outlook 2007 Client when caching is enabled.

For more information about this issue, refer to Microsoft Outlook 2007 technical support.

Volume information not displayed correctly in VSS Restore wizard (1179162)

If a subcomponent of Microsoft Exchange is configured to use more than one volume, then the last page of the VSS Restore wizard does not display the list of volumes correctly. This is only a display issue and does not affect the restore operation.

Vxsnap restore operation fails with "Pre-Restore failed by Writer" error (1253095)

SFW dismounts the Exchange 2007 stores before beginning the vxsnap restore operation. If it fails to dismount the stores, the restore operation fails with a "Pre-Restore failed by Writer" error.

This occurs when the Exchange Storage group is not offline/dismounted or when databases have not been set to overwrite by restore.

Workaround: Make sure to dismount the stores, manually set them to overwrite, and repeat the vxsnap restore operation.

VSS Writers cannot be refreshed or contacted (1275029)

VSS Writers cannot be refreshed or contacted as in the following:

- `Vxsnap refresh` CLI operation fails because VSS fails to gather data from the VSS Writers
- Windows Event Viewer encounters a VSS error, "An internal inconsistency was detected in trying to contact shadow copy service writer." (Event ID 12302)

These are known Microsoft problems.

Workaround: Refer to Microsoft KB940184 for steps to correct the issue.

Memory leaks occur during VSS snapshot operations (859058, 1239666)

During snapshot operations using VSS, memory leaks occur.

This is a known Microsoft problem (KB 933653).

Time-out errors may occur in Volume Shadow Copy Service (VSS) writers and result in snapshots that are not VSS compliant (633219)

In some circumstances, you may receive VSS errors showing that the volume shadow copy freeze timed out. As a result the snapshots that were created are not VSS compliant and the snapshot XML file used by the VSS-based wizards and `vxsnap` commands is not generated. Therefore, you cannot use any of the `vxsnap` commands or VSS-based wizards to restore or to reattach the snapshot. If the snapshot volumes have been scheduled for automatic updates with the Quick Recovery Configuration Wizard or VSS Snapshot Scheduler Wizard, the updates cannot occur.

For a detailed description of the problem, see:

<http://support.microsoft.com/kb/915331>

Workaround: If a snapshot fails with this error, you can use volume-based commands to manually snapback individual snapshot volumes. You can use the `vxassist snapback` command or the Snap Back command from the Volumes node in the Veritas Enterprise Administrator console. Once the volumes are reattached and resynchronization is complete, you can create a new snapshot manually or scheduled snapshots can resume.

In addition, Microsoft supplies a hotfix that you can install to resolve this issue. For additional information, see Microsoft Knowledge Base 915331:

The backup process may fail and a time-out error may occur in Volume Shadow Copy Service writers

<http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B915331>

The `vxsnapsql restore` CLI command may fail when restoring an SQL database (895239)

On an SFW HA system that is configured with VCS, VVR, and GCO options, using the `vxsnapsql restore` CLI command to restore a SQL database may fail with the following error message:

```
Recovering production volumes from Snapshot Backup set ...
Can not reattach a mirror to a volume that is in use by another
application. Please close applications, consoles, Explorer windows,
or third-party system management tools accessing the volume and
then retry the operation. The SQL command failed after it was
initiated. The operation failed.
```

Workaround: The workaround for this problem is to first offline all the SQL server and MountV resources for the volume which contains the SQL database and Logs on VCS and then to bring them back online.

The `vxsnapsql restore` CLI command works correctly after performing this procedure.

VSS objects may not display correctly in VEA (307402)

On systems running both SFW and Microsoft Exchange, VSS objects may not be displayed in VEA after a reboot. Also, VSS objects may not display correctly as a result of changes to storage groups or databases in Exchange.

Workaround: Select **Refresh** from the **Action** menu of the VEA menu bar (or use the `vxsnap refresh` CLI command). Refreshing VEA displays these VSS objects.

The `vxsnapsql start` and `vxsnapsql create` commands fail with sp4 on 64-bit SQL Server 2000 (354767)

After installation of Service Pack 4 (SP4) on 64-bit Microsoft SQL Server 2000, the `vxsnapsql start` and `vxsnapsql create` commands fail. The commands fail because the Microsoft SQL Server 2000 file, `MSVCR71.dll`, is deleted during installation of SP4. See Microsoft Knowledge Base article 902150 for more information.

Workaround: Copy `MSVCR71.dll` to a temporary folder before installing SP4. After the installation is complete, move the `dll` file to the folder `\ProgramFiles(x86)\Microsoft SQL Server\80\Tools\Bin`.

VSS Snapshot of a volume fails after restarting the VSS provider service (352700)

The Veritas VSS Provider Service contacts the Microsoft VSS service to complete the snapshot operation. Restarting the Veritas VSS Provider Service disables the contact to the Microsoft VSS service.

Workaround: Restart Microsoft VSS service after restarting the Veritas VSS Provider Service.

Restoring SQL databases mounted on the same volume (258315)

When you restore a Microsoft SQL database that resides on a volume that contains another SQL database, the `vxsnapsql` utility restores both databases.

Workaround: Avoid this situation by configuring each SQL database on its own separate dynamic volume.

Mirror attach operation hangs and does not complete (406420)

The mirror reattach operation may not finish and hangs at 99% complete. Although the operation appears not to finish, the volume is healthy and it is accessible.

Workaround: The workaround is to issue a rescan to signal the completion of the operation.

Snapshot operation fails if components with the same name exist in different Exchange virtual servers (508893) (1104325)

If multiple Exchange virtual servers are online on the same server, snapshot operations may fail. This can occur when using the `vxsnap start` and `vxsnap create` commands or the Quick Recovery Configuration Wizard.

Workaround: Use the **VSS Snapshot Wizard** (VEA GUI) to take a snapshot in an environment with two virtual Exchange servers, when both have a storage group with the same name. To use the Quick Recovery Configuration Wizard, rename any storage groups with the same name, as follows:

- For Exchange 2003, in Exchange System Manager, right-click the storage group that you want to rename and click **Rename**.
- For Exchange 2007, in the Exchange Management Console, right-click the storage group that you want to rename and click **Properties**. In General Properties, change the name in the editable box and click **Apply**.

CLI command, `vxsnap prepare`, does not create snapshot mirrors in a stripe layout (839241)

When using the `vxsnap prepare` command, specifying the layout type as stripe should create snapshot mirrors in a stripe layout. However, if the number of columns is not also specified in the `vxsnap prepare` command, then snapshot mirrors with a concatenated layout are created.

After taking a snapshot of a volume, the resize option of the snapshot is disabled (866310)

After performing a snapshot operation on a volume, the volume might be designated as read-only, which means the Resize Volume option is disabled. (Right-click the volume in tree view and in the menu, Resize Volume... is disabled).

Workaround: In the volume properties page, deselect the **Read Only** check box. When you right-click the volume in tree view, **Resize Volume > Expand** is now enabled.

If the snapshot plex and original plex are of different sizes, the snapback fails (867677)

When a snapshot volume and the original volume are of different sizes, the snapback fails.

Workaround: Make the snapshot volume read-write manually, increase the size of the snapshot volume to match the size of the corresponding original volume, and then reattach.

Snapshot scheduling issues

The following are Snapshot scheduling issues.

Snapshot schedule fails as result of reattach operation error (1280848)

On Windows Server 2008, a snapshot schedule fails when the reattach operation fails during a snapshot procedure on mounted volumes. A "volumes are in use, cannot reattach" error occurs for the reattach operation. Subsequent snapshot schedules fail with the same error. The reattach operation fails as a result of a known Microsoft volume lock problem (SRX080317601931).

Workaround: Snapshotted volumes that do not have assigned drive letters do not encounter this error. When creating snapshot schedules, select the "no driveletter" for the snapshotted volumes.

Next run date information of snapshot schedule does not get updated automatically (930269)

When selecting a snapshot schedule object in the VEA GUI, information about the next run date is displayed.

If the next run date changes, such as after a scheduled run, the new next run date information is not automatically updated in the VEA GUI.

Workaround: Reselecting the snapshot schedule in the VEA GUI updates the display of the next run date information.

Changes related to Daylight Savings

Time Impact of the United States Energy Policy Act of 2005. Beginning Spring 2007, daylight saving time (DST) start and end dates have been changed. DST dates in the United States:

- Start three weeks earlier (2:00 A.M. on the second Sunday in March)
- End one week later (2:00 A.M. on the first Sunday in November).

To address this change, Microsoft provides patches for Windows Server 2003.

These patches are available at:

<http://support.microsoft.com/kb/928388>

The SFW Snapshot Scheduler relies on the Windows system clock and does not function correctly without the application of the Microsoft DST patch.

VEA GUI may not display correct snapshot schedule information after Veritas Scheduler Service configuration update (1260683)

In a cluster environment, the Veritas Scheduler Service needs to be configured on each node with domain administrator privileges. This configuration change requires that the scheduler service be restarted on each node to enable the new settings. This is done to ensure that the schedule information is reflected on all the nodes in the cluster in case of failover. However, the VEA GUI may not show the correct schedule information after the service is restarted.

Workaround: To ensure that the VEA GUI displays the correct schedule information, the Storage Agent Service also needs to be restarted after the Scheduler Service is restarted. In this way, the Storage Agent Service is able to receive any changes in the schedule information from the Veritas Scheduler Service. Alternatively, to get the correct schedule information, you must perform a VSS refresh command with the VEA GUI or a `vxsnap refresh` CLI command every time you want to display the correct schedule information.

Scheduled snapshots do not occur at correct times after installing patch for Daylight Savings Time (999290, 999316)

After applying the Microsoft patch for daylight savings time (DST), the times for scheduled snapshots are not corrected by the patch and do not occur at the correct times. Also logs for the snapshot scheduler are not corrected by the patch and contain invalid time entries.

Workaround: After applying the Microsoft DST patch, restart the "Veritas Scheduler Service" for the changes in the patch to become effective.

Scheduled snapshots affected by transition to Daylight Savings Time (929625)

The transition from Standard Time to Daylight Savings Time (DST) and the transition from Daylight Savings Time to Standard Time affects the Snapshot Scheduler.

- On the first day of DST, any snapshots scheduled during 2:00 A.M.- 2:59 A.M. are taken during 3:00 A.M.- 3:59 A.M. DST.
- On the last day of DST, any snapshots scheduled during 1:00 A.M. - 1:59 A.M. are taken 1:00 A.M. - 1:59 A.M. Standard Time.
- If during 1:00 A.M. - 1:59 A.M. on the last day of DST the Veritas Scheduler Service is started/restarted or a VSS refresh occurs, some snapshots scheduled for this period are not taken. For example, if a VSS refresh occurs at 1:30 A.M. on the last day of DST, then any snapshots scheduled during 1:00 A.M. - 1:29 A.M. are not taken

In a cluster environment, the scheduled snapshot configuration succeeds on the active node but fails on another cluster node (800772)

In a VCS cluster environment, in some cases configuring a snapshot schedule fails on one or more of the cluster nodes and the Quick Recovery Wizard or VSS Snapshot Scheduler Wizard displays an error message to that effect. In that case, the schedule succeeds on the active node but in the case of a failover, scheduled snapshots do not occur.

Workaround: Start the Quick Recovery Configuration Wizard from the Solutions Configuration Center (**Start>Run>sc**). Continue through the wizard until the **Synchronizing Schedules** panel shows that synchronization between cluster nodes is complete. Click **Finish** to exit the wizard.

After a failover occurs, a snapshot operation scheduled within two minutes of the failover does not occur (798628)

When a failover occurs and the disk group is imported on the active node, the scheduler waits for two minutes. Then the schedule-related information is refreshed. If a snapshot operation, such as a mirror preparation or a snapshot, is scheduled within those two minutes, it does not occur at that time. The schedule starts working with the next scheduled snapshot operation. If the mirror preparation operation was skipped, it is performed at the time of the next scheduled snapshot.

Unable to create or delete schedules on an MSCS cluster node while another cluster node is shutting down (894830)

If you are creating or deleting a snapshot schedule on an MSCS cluster node while another node in the cluster is shutting down, the schedule creation or deletion fails. You can no longer create or delete schedules on the original node until the Veritas Storage Agent (vxvm service) is restarted on the original node. However, any existing schedules continue to run, and you can create or delete schedules from other nodes in the cluster.

Workaround: Restart the Veritas Storage Agent (vxvm service) on the node on which you attempted to create or delete the schedule.

Quick Recovery Wizard schedules are not executed if service group fails over to secondary zone in a replicated data cluster (1209197)

In a replicated data cluster configured with primary and secondary zones, Quick Recovery snapshot schedules are not executed if the service group fails over from the primary zone to the secondary zone.

On Windows Server 2008, a scheduled snapshot operation may fail due to mounted volumes being locked by the OS (1205743)

A Windows Server 2008 issue causes the operating system to intermittently lock mounted volumes. This can result in a failure in a scheduled snapshot operation, if the user specified mount points or mount paths for the snapshot volumes or manually mounted the snapshot volumes after a snapshot operation completed. If the operating system locks mounted volumes, when the scheduler tries to do the next scheduled operation, it fails with the error "volumes are in use". The error can be found in the .sts file corresponding to the schedule.

Workaround: Check if any programs or processes are holding a lock on the storage groups and take the necessary steps to release the lock on the relevant volumes. Remove the mount for the volume before the next scheduled snapshot.

Quick Recovery Configuration Wizard issues

The following are Quick Recovery Configuration Wizard issues.

Quick Recovery Wizard allows identical names to be assigned to snapshot sets for different databases (1090276)

The Quick Recovery Configuration Wizard lets you edit the snapshot set names and XML file names. If you select multiple databases during one run of the wizard, the wizard validates the names you assign to ensure that they are unique across all databases and snapshot sets. However, if you specify different databases during different runs of the wizard, the wizard is unable to validate that the names assigned during the later run are different from the names assigned earlier. If you later run the wizard to modify both databases at the same time, the wizard recognizes the names are the same and will not proceed further.

Workaround: Select both databases in a single run of the wizard when configuring for the first time, so that the wizard can validate the names, or ensure that you specify unique names. If you have already assigned the same names by running the wizard multiple times for multiple databases, select the databases on different runs in modify mode as well.

VEA Console issues

The following are VEA Console issues.

Reclaim storage space operation may not update progress in GUI (1955322)

Performing a reclaim operation may not allow the GUI to automatically update the progress of the operation. In this situation, the progress of the operation does not change.

Workaround: Perform a rescan operation to allow SFW to obtain the progress about the operation and to refresh the GUI.

SFW Agents are slow to appear in VEA GUI (1858587)

After system reboot, the SFW Agents do not appear immediately in the VEA GUI. The SFW Agents may appear after many minutes.

Workaround: Add a key to the Windows registry, USE_RT_TIMEOUT, to allow the SFW Agents to appear more quickly. USE_RT_TIMEOUT has value = 0 and is of type DWORD.

The registry path for 32-bit systems:

```
HKEY_LOCAL_MACHINE/software/veritas/VRTSobc/pal33/agents /__defaults
```

The registry path for 64-bit systems (x86 and IA64):

```
HKEY_LOCAL_MACHINE/software/wow6432node/veritas/VRTSobc/  
pal33/agents/__defaults
```

After adding the key to the Windows registry, restart all the SFW Agents or reboot the system to make the settings effective.

VEA GUI fails to log on to iSCSI target (1287942)

On a Windows Server 2008 system, the operation to log onto an iSCSI target fails when selecting the initiator adapter and the source portal (using the "Advanced settings" option). The failure of the operation is not obvious. However the connection object displayed in the VEA GUI for the logon session shows an invalid IP address of 0.0.0.0.

Workaround: When it is necessary to specify the initiator adapter and source portal during logon of an iSCSI target, you can use the Microsoft iSCSI Initiator Applet to successfully perform the operation.

VEA GUI incorrectly displays a new iSCSI disk as online (1362395)

In Windows Server 2008, when a new iSCSI disk is presented, the VEA GUI incorrectly displays the disk as being online.

Workaround: Perform a rescan to correctly display the new iSCSI disk as being offline.

Dell Virtual Floppy USB Device displayed by VEA GUI (1362215)

Dell Servers provide a virtual USB device, the Dell Virtual Floppy USB Device. The VEA GUI displays this device as a disk drive. SFW 5.1 does not manage this device and operations involving this disk, such as adding this disk to a dynamic disk group, are not supported.

The display of the Dell Virtual Floppy USB Device in the VEA GUI can be disabled in the setup operation for the Dell HBA.

VEA does not display properly when Windows color scheme is set to High Contrast Black (1225988)

Launching the VEA GUI and then changing the color scheme in the Appearance settings of Windows to High Contrast Black causes the VEA GUI not to display properly.

Workaround: To enable the VEA GUI to display properly, close the VEA GUI and launch it again.

VEA displays objects incorrectly after Online/Offline disk operations (1196813, 1200302, 1202847, 1204590, 1205352)

On Windows Server 2008, after performing online/offline disk operations on disks that belong to the Microsoft Disk Management Disk Group, the VEA GUI may display objects related to this disk group incorrectly. Missing disk or duplicated volume objects may be displayed in the VEA GUI. Generally, performing a rescan operation corrects this issue. However, a rescan may not be effective and may possibly cause the Veritas Storage Agent Service to terminate abnormally. This situation may also occur when the dynamic disk in the Microsoft Disk Management Disk Group is disabled and then enabled with the Device Manager.

Workaround: To have the VEA GUI display objects related to the Microsoft Disk Management Disk Group correctly, restart the Storage Agent Service. However, after the Storage Agent has restarted, performing some operations on the disk group (such as write signature or create simple volume) using SFW may fail. In this situation, perform a rescan operation after the Storage Agent Service has restarted.

Disks displayed in Unknown disk group after system reboot (1138080)

If all disks in a dynamic disk group are brought online after a server is booted, the disks are incorrectly displayed in the Unknown disk group.

Workaround: Perform a rescan to display the disk group correctly.

Device type displayed for a disk may not be accurate (291887)

The device type displayed for a disk in the VEA may not be accurate.

When the device type is displayed as FIBRE for a disk, the device type may be a different type, such as SCSI. SFW obtains the device type value from a Microsoft API. This issue has been sent to Microsoft for investigation.

Internationalization issues

The following are Internationalization issues.

VEA GUI cannot show double-byte characters correctly on (English) Windows operating system (1238207)

VEA GUI relies on the font setting of the Windows operating system to be enabled to display double-byte characters after enabling East Asian Languages in the **Windows Regional and Language Options** dialog box. The default font setting for the (English) Windows operating system cannot display double-byte characters.

Workaround: The following procedures enable the display of double-byte characters.

To enable display in Windows Server 2003 or Windows XP

- 1 Right click on the desktop.
- 2 Select **Properties > Appearance** tab.
- 3 In the window that appears, click **Advanced**.
- 4 Select "Message Box" from the Item drop-down list.
- 5 Select a font from the Font drop-down list that supports double-byte characters. (For example: "MS Mincho".)
- 6 Click **OK** to complete the setting.

To enable display in Windows Server 2008 or Windows Vista

- 1 Right click on the desktop.
- 2 Select **Personalize**.
- 3 Select Windows Color and Appearance.
- 4 In the window that appears, click **Advanced**.
- 5 Select "Message Box" from the Item drop-down list.
- 6 Select a font from the Font drop-down list that supports double-byte characters. (For example: "MS Mincho".)
- 7 Click **OK** to complete the setting.

VEA can't connect to the remote VEA server on non-English platforms (804330, 861289)

When connecting to the remote VEA server on non-English platforms, you might see a VEA error that says "Request to server has timed out".

Workaround: Set up the target server's subnet in the DNS Reverse Lookup Zone. For example, if the remote VEA server is 10.198.91.111, set the target server's subnet to 10.198.91.* in the DNS Reverse Lookup Zone.

Note that setting the DNS Reverse Lookup Zone Configuration is a network requirement for VEA and VVR. When setting up your network, verify the availability of DNS Services. AD-integrated DNS or BIND 8.2 or higher are supported. Make sure that a reverse lookup zone exists in the DNS.

Dynamic Multi-pathing (DMP) issues

The following are Dynamic Multi-pathing (DMP) issues.

Bug check may occur when adding DMP DSM option (1251851)

After installing SFW, adding the DMP DSM option, with Windows Add or Remove Programs, may result in bug check 0xD1. This issue has been reported to Microsoft (SRZ080421000462).

DMP DSM operations are not currently supported by vxdmpadm (1287130)

DMP DSM operations are not currently supported by the `vxdmpadm setattr dsm` command. The `vxdmpadm setattr dsm` command is not available in this release.

Workaround: Use the `vxdmpadm setattr array` command to manage DMP DSMs.

Changes made to a multipathing policy of a LUN using the Microsoft Disk Management console, do not appear on the VEA GUI (1859745)

DMP DSMs do not manage the load balance settings made with the Microsoft Disk Management console. So changes made to a multipathing policy using the Microsoft Disk Management console do not appear on the VEA GUI.

Changing the load balance settings for DMP DSMs must be done using the SFW VEA GUI or CLI.

Symantec does not appear as the digital signer for DMP DSMs (1892280)

On Windows Server 2008 R2 for IA64, the property of a Symantec DSM in the System Devices GUI of the Windows Device Manager does not show Symantec as the digital signer. This is a problem with Windows Server 2008 R2 for IA64 and has been reported to Microsoft.

Microsoft Systems Center Operations Manager 2007 (OpsMgr 2007) issues

The following are Microsoft Systems Center Operations Manager 2007 (OpsMgr 2007) issues.

Performance Graph for MPIO does not display data (914312)

When monitoring the performance activity of a volume using MPIO Path Performance counters, the performance data is displayed as the number of reads, number of writes, bytes read, and bytes written. The counter can increment to a point where the graph appears to level off or becomes negative. This condition continues until the affected counter rolls over to zero, at which time an accurate graph is displayed.

When deleting the last RVG or moving an RVG, the VVR state view is not updated (1051217, 1051220)

The **VVR State** view > **Detail** view is not updated in OpsMgr 2007 when the last RVG is deleted or when an RVG is moved. This is due to OpsMgr 2007 being unable to recognize the empty collection of item sent by discovery workflows.

Other issues

The following are other issues.

SFW volume operations fail on Windows Server 2008 (1093454)

On Windows Server 2008, SFW operations on a volume may fail with a message stating that the volume is already in use. This is caused by Windows not releasing an open handle. This is a known Microsoft problem. (KB952790)

Sharing property of folders not persistent after system reboot (1856737)

On Windows Server 2008, folders that reside on a volume in a dynamic disk group and were set up as shared folders are no longer shared after a system reboot. The following is the workaround procedure for this issue.

Note: Perform the following before system reboot.

To work around the sharing property issue

- 1 Enable the dynamic disk group that contains the shared folders for latestart.

For example use the CLI command:

```
vxdg -gDiskGroup1 latestart on
```

- 2 In regedit, navigate to

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanserver
```

- 3 Right-click the lanmanserver node and select **New > Multi-String Value** to enter a new REG_MULTI_SZ entry.

- 4 Name the Multi-String Value as DependOnService and enter the service name for the Veritas DG Delayed Import Server name in the Data field. (The default name for this service is VxDgDI.)
- 5 Reboot the system.

Microsoft Disk Management console displays an error when a basic disk is encapsulated (1601134)

On a Windows Server 2008 with the Microsoft Disk Management console launched, adding a basic disk that contains a primary partition/extended partition with a logical drive to an SFW dynamic disk group using the VEA GUI, may cause a pop-up error message on the Microsoft Disk Management console. The pop-up error message on the Microsoft Disk Management console is not meaningful and can be ignored.

bcdedit fails after installing SFW 5.1 SP1 (1839598)

On Windows Server 2008 R2, when the system volume is not the same volume as the boot volume and the system volume does not have a drive letter, bcdedit fails after installing SFW 5.1 SP1.

Workaround: Add a drive letter to the system volume before running bcdedit. The drive letter can be removed later, after working with bcdedit.

Results of a disk group split query on disks that contain a shadow storage area may not report the complete set of disks (1797049)

When performing a disk group split query command on a set of disks that contain a shadow storage area of volumes on disks having mirrored volumes, the resulting report may not be comprehensive. In this case, the report does not indicate the complete set of disks for split closure.

Extending a simple volume in Microsoft Disk Management Disk Group fails (1596070, 1834611)

On Windows Server 2008, while extending a simple volume in a Microsoft Disk Management disk group, the operation fails with the error message, "Fail to grow volume.". This issue also affects the automatic volume growth operation when resizing a volume in a Microsoft Disk Management disk group. This is a known Microsoft problem (KB975680).

Unable to add a shared folder in Microsoft Failover Cluster environment (1233387)

After creating a cluster disk group and VMDG resource (dynamic volume) in a Microsoft Failover Cluster environment on Windows Server 2008, the dynamic volume cannot be found when trying to add a shared folder with the "Provision

a shared folder Wizard". This is a problem with Windows Server 2008 and has been reported to Microsoft.

Workaround: Moving the VMDG resource to each of the nodes in the cluster environment, one node at a time, allows adding the dynamic volume as a shared folder with the "Provision a shared folder Wizard" in the last node.

After the VMDG resource reaches the last node, the "Provision a shared folder Wizard" works correctly when the VMDG resource is moved back to any of the other nodes.

Volume automatically assigned a drive letter after dynamic disk group deport/import operations (1282891)

On Windows Server 2008, the operations of deporting and then importing a dynamic disk group that contains a volume that does not have an assigned drive letter results in the assignment of a drive letter to the volume. In addition, the drive letters of other volumes in the dynamic disk group may change. This is a Windows Server 2008 problem and has been reported to Microsoft.

Workaround: Manually remove the automatically assigned drive letter of the volume after importing the dynamic disk group. Also adjust the drive letters of the other volumes in the dynamic disk group as needed.

SFW cannot merge recovered disk back to RAID5 volume (1150262)

For a Microsoft Disk Management RAID5 volume on Windows Server 2008, a recovered disk is displayed by SFW as a RAID 5 volume, however the volume has a degraded status. SFW is not enabled to perform a reactivate operation on the volume to change the volume to a healthy status.

Workaround: Use Microsoft Disk Management to reactivate the disk or the RAIDS 5 volume to resynchronize the plexes in the RAID5 volume and change the volume to a healthy status.

Request for format volume occurs when importing dynamic disk group (1109663)

During the import of a dynamic disk group, or other operation that involves mounting a volume, that has an unformatted volume with a drive letter or assigned mount point, a pop-up window appears that requests formatting the volume. Avoid completing the formatting operation if there is any existing data on the volume.

Port conflict when using PBX_exchange.exe in MSCS (1194658)

The default port for PBX is 49162. In certain environment configurations, a conflict for this port may occur.

Workaround: Change the port range for PBX to resolve the port conflict. To configure the port range for PBX, a Windows registry key must be added for vxsvc and agents.

- For vxsvc, add the registry key under
 \HKEY_LOCAL_MACHINE\Software\Veritas\VxSvc\CurrentVersion\Network\Params\Security
with the following:
 - type = REG_SZ
 - name = CLIENT_PORT_RANGE
 - value in the form X-Y, where X and Y are numeric values and Y > X.
- For agents, add the registry key under
 \HKEY_LOCAL_MACHINE\Software\Veritas\VRTSobc\pal33\Agents\<agentname>\Network\Params\Security
where <agentname> is the name of the agent, such as StorageAgent, gridnode, actionagent, etc.

Note: If the registry key is not present, then port range 49162-65535 is assumed.

Logging on to SFW as a member of the Windows Administrator group requires additional credentials (1233589)

On Windows Server 2008, by design, logging on to SFW as a member of the Windows Administrator group should allow access to SFW without additional credentials. However, only the Administrator userid is allowed access to SFW in this way. Other members of the Administrator group are not allowed access unless additional credentials are given.

Workaround: Other members of the Administrator group should provide their Windows userid and password when prompted to gain access to SFW.

Removing a cluster disk group causes an error message (1233398)

On Windows Server 2008, removing a cluster disk group causes an error message describing that an Assertion Failed. However, in this case, the remove cluster disk group operation has completed successfully and this message can be ignored. Click the **Ignore** button at the bottom of the message window to continue. This is a known Microsoft problem (KB953402).

Certain operations on a dynamic volume cause a warning (1093454)

On Windows Server 2008, operations on a dynamic volume (such as change drive letter, delete, or shrink) result in a warning message stating that the volume is currently in use. This is a known Microsoft volume lock problem (SRX080317601931).

Workaround: If no applications are utilizing the volume, complete the operation by responding to the warning message to perform the operation with force.

Avoid encapsulating a disk that contains a system-critical basic volume (1180702)

On Windows Server 2008, if a disk contains a system-critical basic volume (as determined by VSS), then the disk should not be encapsulated by SFW. The disk needs to be managed by Microsoft Logical Disk Manager (LDM) so that in a recovery situation it can be recovered by ASR. Encapsulating the disk would not allow recovery by ASR.

Sharing property of folders in clustering environment is not persistent (1195732)

In a clustering environment on Windows Server 2008, the sharing property of folders is not persistent when first the cluster disk group is deported and the system is rebooted, and then the cluster disk group is imported back to the system. Also, the sharing property is not persistent when the cluster disk group is deported to another node. In addition, the file share property of a volume is not persistent when it arrives after system boot up.

Access violation error occurs when performing simultaneous rescan operations (1219999)

On a Windows Server 2008 system, performing two rescan operations simultaneously, one in SFW and one in Microsoft Disk Management, results in an access violation error.

Workaround: Ensure that the Veritas Storage Agent service and the Virtual Disk Service (VDS) are both stopped; and then restart both services.

Fileshare cannot be created using Failover Cluster Management (1159620, 1195732)

In a clustering environment on Windows Server 2008, a fileshare cannot be created by using Microsoft Failover Cluster Management. An alternate way to create the fileshare is to use Windows Explorer. In addition, connecting to the fileshare using the virtual IP address is not possible.

To connect to the fileshare, use the virtual name of the fileshare, not the virtual IP address.

Installation of SFW or SFW HA into a non-default installation directory results in the creation of duplicate files and directories (861852)

If you choose to specify an installation directory instead of accepting the default directory, duplicate files, and directories are created. This does not affect the function of the product.

Entries under Task Tab may not be displayed with the correct name (797332)

Tasks displayed under the Task tab of the VEA GUI console may appear as an entry labeled as "NoName". These labels are not harmful and refer to a task that is running.

Attempting to add a gatekeeper device to a dynamic disk group can cause problems with subsequent operations on that disk group until the storage agent is restarted (864031)

If your storage array has a gatekeeper device (disk), do not add this disk to a dynamic disk group. The operation to include this disk in a dynamic disk group fails, and subsequent operations on the disk group, such as snapshot operations, fail until the storage agent is restarted.

Workaround: Remove any gatekeeper devices from the dynamic disk group and restart the Veritas Storage Agent (vxvm service).

Installing SFW in a non-default path causes an abnormal termination (829850)

An abnormal termination occurs when installing SFW in a location that is not the default installation path. This is due to a problem with Microsoft Virtual Disk Service (VDS). This is a known Microsoft problem (SRX061018602975).

ASR fails to restore a disk group that has a missing disk (844084)

When a disk group is missing a disk or a volume, you should not perform an ASR backup and restore procedure, as that action is not supported.

Use only U.S. ASCII characters in the SFW or SFW HA installation directory name (858913)

Using non-ASCII characters in the SFW or SFW HA installation directory may result in the creation of duplicate directories and files.

Workaround: No workaround. Use only U.S. ASCII characters in directory names.

Unable to create an MSCS Volume Manager Disk Group resource type on the active node (301263)

In a two node MSCS cluster, you cannot create an MSCS Volume Manager Disk Group resource type on the active node after SFW has been uninstalled on the standby node.

This issue occurs when the Volume Manager Disk Group resource type does not already exist in the cluster before uninstalling SFW on the standby node.

Workaround: The workaround is to run ClusReg.cmd on the active node after uninstalling SFW on the standby node and before trying to create the Volume Manager Disk Group resource.

ClusReg.cmd is located in the VM5INF folder and is in the path where SFW has been installed. For example, if SFW has been installed on a 64-bit server using the default path, then VM5INF is located at `C:\Program Files(x86)\VERITAS\VERITAS Volume Manager 4.3\VM5INF`

Veritas Cluster Server

This section provides information on known Veritas Cluster Server issues.

File Share Configuration Wizard may create dangling VMDg resources (2097155)

This issue occurs if you use folder mounts for creating file share service groups. The VCS File Share Configuration Wizard successfully creates file share service groups, but may fail to configure dependency for one or more VMDg resources. The VMDg resources are configured correctly but may not be part of the overall service group resource hierarchy.

Workaround:

You may have to manually configure the dependency for such dangling VMDg resources. VMDg resources are typically configured as child of MountV resources in VCS service groups.

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

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

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

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

Workaround

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

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

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

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

SharePoint 2010 resource faults with an initialization error

After configuring the SharePoint service group, the VCS SharePoint 2010 agent resource (SharePointServer) may fault.(2102270)

The SharePoint 2010 agent log may contain the following messages:

```
VCS ERROR V-16-10051-13583
```

```
SharePointServer:<SharePointcomponentname>:monitor:Provider Initialization failed [4, 0x800705AF]
```

```
VCS ERROR V-16-20083-105
```

```
SharePointServer:<SharePointcomponentname>:monitor:Provider Initialization failed [4, 0x800700A4].
```

Workaround

From the Windows Services MMC snap-in, restart the Windows Management Instrumentation (WMI) service and then probe the SharePoint 2010 resource.

This is a known Microsoft issue and a hotfix was not available at the time of this release.

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

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

The MSMQ agent log may contain the following message:

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

The Windows Event Viewer may display the following message:

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

Workaround

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

VCS services do not start on systems where Symantec Endpoint Protection 11.0 MR5 version is installed (1710556)

This issue occurs on Windows Server 2008 systems.

The VCS High Availability Engine (HAD) may fail to start if you install and configure VCS on systems where Symantec EndPoint Protection (SEP) version 11.0 MR5 is already installed.

The following error may be displayed:

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

Workaround: Disable Symantec EndPoint Protection (SEP) on all the systems where you have installed VCS and then configure the VCS cluster.

After completing the cluster configuration tasks, enable SEP on all the systems.

Exchange 2007 database fails to mount after performing a database restore operation using Backup Exec 12.5 (1674378)

This issue occurs if you are using Backup Exec (BE) 12.5 on Windows Server 2008 systems where Exchange 2007 is configured with VCS.

When the **Mount database after restore** option is enabled in the Restore Properties Settings for Exchange, after performing a database restore operation using Backup Exec (BE) 12.5 the Exchange 2007 database fails to mount on the cluster node.

Global group fails to come online on the DR site with a message that it is in the middle of a group operation (1795151)

When the node that runs a global group faults, VCS internally sets the MigrateQ attribute for the group and attempts to fail over the global group to another node

within the local cluster. The MigrateQ attribute stores the node name on which the group was online. If the failover within the cluster does not succeed, then VCS clears the MigrateQ attribute for the groups. However, if the groups have dependencies which are more than one-level deep, then VCS does not clear the MigrateQ attribute for all the groups.

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

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

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

To bring the global group online on the DR site

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

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

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

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

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

where:

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

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

- 3 Bring the service group online on the remote cluster.

Type the following on the command prompt:

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

Unable to access SQL Server 2008 databases upon failover (1876562)

When you create a SQL 2008 database from a cluster node, only the Local Administrators group and the SQL Users group created on that node have permissions to that database. As a result, when the SQL service group is switched over to another cluster node, you cannot access that database from that node.

Also, the SQL service may fail to start after switching over the service group on alternate nodes. This occurs if the SQL service user account specified during SQL installation does not have local administrative privileges on all the cluster nodes.

Workaround: Ensure that the user account for the SQL service is a domain user and a member of the Local Administrators group on all the cluster nodes.

Cannot log on to the Cluster Manager (Java Console) after upgrading to Service Pack 2 (1871939)

You may not be able to log on to the VCS Cluster Manager (Java Console) after upgrading to Service Pack 2. This issue occurs if you have configured a secure cluster and are upgrading your systems from SFW HA 5.1 AP1 to SFW HA 5.1 SP2.

Workaround: Start the Symantec Product Authentication Service and then log on to the Cluster Manager (Java Console). Type the following at the command prompt:

```
net start vrtsat
```

Storage agent resources may go into an unknown state after upgrading Windows Server 2008 SP1 systems (1786188, 1835035, 1835031)

If you upgrade the Windows Server 2008 SP1 operating system on SFW HA 5.1 SP1 cluster nodes, the storage agent resources (VMDg and MountV) in the cluster may go into an UNKNOWN state and the storage agent service (vxvm) may fail to start.

This issue occurs if you upgrade Windows Server 2008 SP1 to Windows Server 2008 SP2 or Windows Server 2008 R2.

Workaround: Complete the following steps depending on the upgrade case:

To perform Windows Server 2008 SP1 to Windows Server 2008 SP2 upgrades:

- 1 Stop the Veritas High Availability Engine (HAD) on all the cluster nodes.
Type the following at the command prompt:

```
hastop -all -force
```
- 2 From the command prompt, run %vmpath%\FixVDSKey.bat on all the cluster nodes.

%vmpath% is the default installation directory for Veritas Volume Manager, typically, C:\Program Files\Veritas\Veritas Volume Manager 5.1. (C:\Program Files (x86)\Veritas\Veritas Volume Manager 5.1 on 64-bit systems)
- 3 Reboot all the cluster nodes.
- 4 Verify that the Veritas High Availability Engine (HAD) is running on all the cluster nodes.
Type the following at the command prompt:

```
hasys -state
```


The status should display as RUNNING.
If HAD is not running, start it.
Type the following at the command prompt:

```
hastart
```

To perform Windows Server 2008 SP1 to Windows Server 2008 R2 upgrades

- 1 From the Windows Control Panel, launch **Add or Remove Programs**.
- 2 Click **Service Pack 2 for SFW 5.1, SFWHA 5.1, and VCS 5.1 for Windows** and then click **Change**.
- 3 On the **Symantec Product Installer Selection** panel, click **Repair**, and then click **Next**.
- 4 On the **Validation** panel, click **Next**.
- 5 On the **Summary** panel, click **Repair**.
- 6 After the installer completes, click **Next** and then click **Finish**.
- 7 Reboot the systems.

VCW is unable to configure the VCS HAD Helper service user account in a domain having a Windows 2000 domain controller

While configuring the cluster on Windows Server 2008 R2 systems, the VCS Cluster Configuration Wizard (VCW) fails to configure the VCS HAD Helper Service user account because it is unable to add the user account to the local Administrator's group on the cluster nodes. The VCW logs display the following error:

```
Error=000006FD.  
00000968-00000666: Failed to add the user to administrators group.
```

This issue occurs on Windows Server 2008 R2 systems that are part of a domain that has a Windows 2000 domain controller.

While taking volume-based snapshots using the VEA console, the Exchange 2007 service group fails over (1727397)

While taking volume-based snapshots from the Veritas Enterprise Administrator (VEA) console on a node where an Exchange 2007 service group is online, the VSS Exchange writer crashes causing the MExchangeIS resource to fault. This results in the Exchange 2007 service group to fail over to another cluster node. This happens if the snapshots are taken of volumes that belong to an Exchange 2007 storage group.

This issue is applicable to Exchange Server 2007 Service Pack 1 running on 64-bit Windows Server 2008 Service Pack 2 systems.

Workaround: Install Update Rollup 9 for Microsoft Exchange Server 2007 Service Pack 1.

See: <http://support.microsoft.com/kb/970162>

SQL instance running on 64-bit machine is not discovered by MOM 2005 server (1449804)

A SQL Server instance running on a 64-bit cluster node is not discovered by MOM 2005 Server. This problem occurs because the MOM 2005 agent is 32-bit while the SQL instance is 64-bit.

Workaround: Depending on your SQL server version, create the following registry key on the 64-bit cluster nodes that host the SQL instance: For SQL Server 2008:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\  
CurrentVersion\Uninstall\Microsoft SQL Server 10
```

For SQL Server 2005:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\  
Microsoft SQL Server\Instance Names\SQL
```

You need not create any registry value under this key. After adding the registry key, the MOM server detects the SQL instances.

Version conflict error while importing the VCS 5.1 SQL management pack for MOM 2005 (1471181)

A management pack version conflict error occurs when you try to import the VCS 5.1 management pack for SQL server in a Microsoft Operations Manager 2005 monitoring environment. This occurs if you have already imported the Microsoft SQL Server 2008 management pack before you import the VCS management pack.

The following error is displayed:

```
Version of Rule Group 'State Monitoring and Service  
Discovery' - '09.0.3043.0000' should be newer than  
'10.1.0001.0000'.
```

Workaround: You can ignore the error and click **Continue** to proceed with the VCS management pack import process. There is no change in the SQL 2005 monitoring scripts included in the Microsoft SQL management pack version 10.1.0001.0000. The VCS management pack file (VCS_SQL2005_MOM2005.akm) version 09.0.3043.0000 works as it is with Microsoft SQL management pack version 10.1.0001.0000.

VCS cluster configuration fails if Symantec Endpoint Protection 11.0 MR3 version is installed (1455690)

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

The following error is displayed:

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

Perform the following workaround to resolve this error.

To resolve error message

- 1 Create a custom rule in the SEP firewall rules table. Specify the following details for the rule:
 - Rule type: Application
 - Application name: llt.sys

- Action: allow
- 2 Move this rule to the top of the firewall rules table and then apply the firewall policy again.
- 3 Ensure that the SEP clients on the systems receive this policy and then proceed with the cluster configuration task.

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

Memory leak occurs in the VCS agent for SQL 2008 (1466183)

A memory leak occurs in the VCS agent for SQL Server 2008. This issue is observed when DBList based SQL database detail monitoring is configured. In this mode of detail monitoring, the VCS agent for SQL 2008 uses Microsoft ActiveX Data Objects (ADO) to access the SQL databases. The memory leak occurs due to the ADO connections made by the agent to each database configured in the DBList agent attribute. The amount of memory leak is negligible and should not cause any adverse effects on the SQL Server operations in the cluster.

Currently there is no fix available for this issue.

Contact Symantec technical support for more information.

SQL Server 2008 Analysis and Agent service resources may go in to an unknown state (1466012)

The SQL Server 2008 Analysis service and SQL Server 2008 Agent service resources may go in to an UNKNOWN state when you bring the SQL Server 2008 service group online. The following error is logged on the GenericService agent log:

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

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

Issue while configuring a secure cluster (1466003)

While configuring a secure cluster you may get the following error on the **Configure Security Service Options** panel of the **VCS Cluster Configuration Wizard** (VCW):

Symantec Product Authentication Service Configuration utility failed. Exit Code : 11

As a result, you may not be able to configure a secure cluster.

Workaround: Note the following requirements before configuring a secure cluster:

- Disable Windows Firewall, if it is enabled.
- While specifying the root broker details in the VCW panel, specify the physical host name (instead of the IP address) of the root broker system.

If the error persists, perform the following steps:

To fix persistent error

- 1 From the command prompt, navigate to the following directory on the cluster system:

```
C:\Program Files\Veritas\Security\Authentication\bin
```

For 64-bit systems the path is as follows:

```
C:\Program Files(x86)\Veritas\Security\Authentication\bin
```

Here, C:\Program Files (C:\Program Files(x86) for 64-bit) is presumed to be the installation directory for VCS.

- 2 Run the following command from the command prompt:

```
"vssregctl.exe -s -l -b  
"Security\Authentication\AuthenticationBroker\AtPlugins\vx" -k  
"ABAuthSourceLocation" -v "C:\Program  
Files\Veritas\Security\Authentication\systemprofile\A  
BAuthSource" -t string"
```

For 64-bit systems, the command is as follows:

```
"Security\Authentication\AuthenticationBroker\AtPlugins\vx" -k  
"ABAuthSourceLocation" -v "C:\Program  
Files(x86)\Veritas\Security\Authentication\systemprofile\A  
BAuthSource" -t string"
```

- 3 Proceed to configure a secure cluster using VCW.

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

While configuring a cluster, the VCS Cluster Configuration Wizard (VCW) may fail to ping systems that are selected to be a part of the cluster. As a result, you

cannot configure the cluster. This may happen in case Symantec Endpoint Protection (SEP) client is installed on the selected systems. VCW uses Internet Control Message Protocol (ICMP) to ping systems and ICMP traffic is blocked in SEP, by default.

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

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

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

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

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

The VCS commands may also fail with the following error:

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

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

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

If the network adapters cannot ping each other, the cluster nodes may not get GAB membership

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

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

```
gabconfig -a
```

If no port membership information is returned it indicates that GAB is not operating. This issue can be addressed in either of the following methods:

To address this issue using method 1

- 1 Reboot the cluster nodes that do not have GAB membership.
- 2 Verify the GAB operation in the cluster.

Type the following on the command prompt:

```
gabconfig -a
```

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

To address this issue using method 2

- 1 Stop the LLT service in the cluster.

Type the following on the command prompt:

```
:net stop llt
```

- 2 Delete the cluster using VCW.
- 3 Ensure that the network adapters can ping each other and then re-create the cluster using VCW.

MountV resource takes time to offline on Windows Server 2008 systems (1189260, 1235123)

The MountV resource may take considerable amount of time to go offline on Windows Server 2008 systems. The MountV agent log displays the following message:

```
VCS WARNING V-16-10051-9023 MountV:<servicegroupname>-MountV:offline:  
Failed to lock  
volume [2:5]
```

Workaround: Symantec recommends that on Windows Server 2008 systems, set the value of the MountV attribute ForceUnmount to NONE. The MountV agent forcibly dismounts the volume irrespective of the type of access an application has to that volume.

File share service group may fail to come online on Windows Server 2008 systems (1204865)

While configuring file shares if you select Bring the service group online option on the **File Share Configuration Wizard Completion** panel, the file share service group may fail to come online. The following message appears in the log:

```
VCS ERROR V-16-10051-10506
FileShare:fs-FileShare:online:Unknown error for folder
<sharename>
```

This issue occurs on Windows Server 2008 systems.

To work around this file share service group issue

- 1 Flush the file share service group.
 - From the Java Console, click the cluster in the configuration tree, click the **Service Groups** tab, and right-click the service group icon in the **View** panel.
 - Click **Flush**, and then click the appropriate system from the menu.
- 2 Bring the file share service group online.

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

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

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

AutoStart may violate limits and prerequisites load policy

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

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

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

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

Trigger not invoked in REMOTE_BUILD state

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

Some alert messages do not display correctly (612268)

The following alert messages do not display correctly:

- | | |
|-------|---|
| 51030 | Unable to find a suitable remote failover target for global group %s. Administrative action is required. |
| 51031 | Unable to automatically fail over global group %s remotely because local cluster does not have Authority for the group. |
| 50913 | Unable to automatically fail over global group %s remotely because clusters are disconnected and ClusterFailOverPolicy is set to %s. Administrative action is required. |
| 50914 | Global group %s is unable to failover within cluster %s and ClusterFailOverPolicy is set to %s. Administrative action is required. |
| 50916 | Unable to automatically failover global group %s remotely due to inability to communicate with remote clusters. Please check WAN connection and state of wide area connector. |
| 50761 | Unable to automatically fail over global group %s remotely because ClusterList values for the group differ between the clusters. Administrative action is required. |
| 50836 | Remote cluster %s has faulted. Administrative action is required. |
| 51032 | Parallel global group %s faulted on system %s and is unable to failover within cluster %s. However, group is still online/partial on one or more systems in the cluster |
| 51033 | Global group %s is unable to failover within cluster %s and AutoFailOver is %s. Administrative action is required. |

Issues related to the VCS engine

The following issues relate to the VCS engine.

Engine may hang in LEAVING state

When the command `hares -online` is issued for a parent resource when a child resource faults, and the `hares -online` command is followed by the command

`hastop -local` on the same node, then the engine transitions to the LEAVING state and hangs.

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

Timing issues with AutoStart policy

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

Issues related to Cluster Manager (Java Console)

The following issues relate the Cluster Manager (Java Console)

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

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

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

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

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

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

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

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

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

Exception when selecting preferences (585532)

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

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

Java Console errors in a localized environment

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

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

Common system names in a global cluster setup

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

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

Agent logs may not be displayed (643753)

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

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

Table 1-14 `bmc` and `bmcmap` file location

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

Service group dependency limitations

The following are service group dependency limitations.

Online local firm dependency violation

If the parent group and the child group are online on node 1, and if the child group faults, VCS begins to take the parent group offline. However, this occurs at the same time the child group is failing over to node 2. If the parent group fails to go

completely offline and the child group goes online on node 2, then a dependency violation results.

Online remote firm dependency violation

If the parent group is online on node 1 and the child group is online on node 2 and faults, the child group selects node 1 as its failover target. This scenario results in a dependency violation because the parent group fails to go offline on node 1.

Concurrency violation trigger cannot offline service group with online firm dependencies

The concurrency violation trigger cannot offline a service group if the group has a parent online on the system with local firm dependency. The concurrency violation continues until the parent is manually taken offline.

Workaround: In this situation, VCS sends notification that the violation trigger failed to offline a service group that is in concurrency violation. The administrator can manually offline the parent group and then the child group.

Secure clusters

The following issues relate to secure clusters.

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

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

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

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

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

To work around this upgrading a secure cluster issue

- 1 Restart the Veritas High Availability Engine (HAD).

Type the following at the command prompt:

```
net stop had
net start had
```

- 2 Verify that HAD is running.

Type the following at the command prompt:

```
hasys -state
```

The state should display as RUNNING.

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

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

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

Global service groups

The following are global service groups issues.

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

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

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

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

Group does not go online on AutoStart node

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

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

Cross-cluster switch may cause concurrency violation

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

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

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

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

Workaround: To bring a global group online on a remote cluster, 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.

Fibre Channel adapters may require modified settings

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

Emulex Fibre Channel adapters

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

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

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

To workaround this issue

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

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

<http://entsupport.symantec.com>.

QLogic Fibre Channel adapters

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

To workaround this issue

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

VCS with Microsoft Exchange Server

The following issues apply to VCS with Microsoft Exchange Server.

Permission issues after upgrading an Exchange cluster (1364867)

The following issues may occur after you upgrade an Exchange cluster:

- You cannot log on to the Veritas Enterprise Administrator (VEA).

The following error is displayed:

```
VEA veaconfig ERROR V-40-49444-54 User does not have sufficient privilege.
```

- The `vxsnap` command may fail with the following error: V-40-49152-9: .

```
Your user account does not have the privileges required to perform the operation
```

Workaround: After the upgrade is complete, you must manually assign the VEA administrative privileges to the admin user and the Administrators group on each cluster node. Perform the following steps on all the cluster nodes, one node at a time.

To work around this issue

- 1 Take the Exchange service group offline or fail over to another node in the cluster.
- 2 On the node on which the Exchange service group is offline, type the following at the command prompt:

```
veaconfig -c add_user -r Administrator -n Administrator@<EVS_Name>.<Domain_Name>.nt -o localhost
```

Here, *<EVS_Name>* is the Exchange virtual server name. *<Domain_Name>* is the fully qualified domain name. Ensure that the command is successful.

- 3 On the node on which the Exchange service group is offline, type the following at the command prompt:

```
veaconfig -c add_user -r Administrator -n Administrators@<EVS_Name>.<Domain_Name>.com.nt -g -o localhost
```

Ensure that the command is successful.

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

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

This issue occurs when RPC over HTTP is deployed in an Exchange Server 2003 environment with a front-end/back-end configuration, and the Exchange back-end

server is clustered with VCS. The front-end server is Exchange 2003 SP2 and the back-end server is Exchange 2003 SP1.

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

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

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

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

To make changes in the registry keys

- 1 Bring the Exchange service group online.
- 2 Click **Start** and then click **Run**.
- 3 In the dialog box, enter regedit and click **OK**.
- 4 In the Registry Editor, locate the following subkey in the registry:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan
- 5 In the right pane, double-click **Enabled**.
- 6 Click **Decimal**, enter 0, and then click **OK**.
- 7 On the **File** menu, click **Exit** to quit Registry Editor.

Error while performing Exchange post-installation steps (1211491)

After installing Exchange and rebooting the node, the Veritas High Availability Engine (HAD) may fail to start. As a result, while performing the Exchange post-installation tasks, the Exchange Setup Wizard may either fail to launch or may display the following error message:

```
Failed to get the cluster information. Make sure that VCS
Engine (HAD) is in running state. Start HAD and click Retry
to continue. Click Cancel to exit the wizard.
Error V-16-13-4207
```

This issue may occur in a secure cluster environment.

To work around this issue

- 1 Restart the Veritas High Availability Engine (HAD).

Type the following at the command prompt:

```
hastop -local -force hastart
```

- 2 Verify that HAD is running.

Type the following at the command prompt:

```
hasys -state
```

The state should display as RUNNING.

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

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

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

To work around this issue

- 1 Take all the ExchService resources in the Exchange 2003 service group offline.
- 2 From the Services MMC snap-in, restart the WMI service.
- 3 Run VCW to perform the required tasks.
- 4 Bring the ExchService resources online.

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

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

```
Server name mismatch Server: EVS1
```

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

You can ignore this error and proceed with the analysis.

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

The Exchange Setup Wizard does not allow a node to be rebuilt, and fails during installation. This is because the wizard stores all the information about the Exchange Virtual servers (EVS) that can fail over on a node, in the ExchConfig registry hive. The path in the registry hive is `HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\VCS\EXCHCONFIG`.

Even if any of the failover nodes die, the corresponding entry still exists in the system list of the EVS. During installation, the Exchange Setup Wizard refers to this incorrect registry entry and fails.

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

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

To work around this issue

- 1 To open the Registry Editor, click Start > Run, type `regedit`, and then click OK.
- 2 In the registry tree (on the left), navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\VCS\EXCHCONFIG`
- 3 From the Exchange Virtual Server keys, delete the keys representing the nodes that are being rebuilt.
- 4 Repeat steps 1 to 3 for the Exchange virtual server on all the nodes in the cluster.
- 5 Exit the Registry Editor.

Resource for Exchange Information Store may take time to online

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

As a default behavior, the enterprise agent for Exchange waits in the Online entry point and returns only when the IS resource starts or when the start operation fails. When IS service is delayed, the enterprise agent for Exchange logs the following message:

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

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

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

To work around this issue

- 1 Open the Registry Editor..
- 2 From the navigation pane, go to

```
\\hkey_local_machine\software\veritas\vcs\  
exchconfig\parameters\msexchangeis
```
- 3 On the **Edit** menu, select **New**, and then click **DWORD Value**.
- 4 Name the value ForceExit.
- 5 Right-click the value and select **Modify**.
- 6 In the **Edit DWORD Value** dialog box, specify the value data as '1'.
Click **OK**

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

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

Metabase update for Exchange may take a longer time (499727)

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

Workaround: Increase the metabase update timeout value. For more information, see:

<http://www.symantec.com/docs/TECH36558>

VCS with Oracle

The following issues apply to VCS with Oracle

Oracle Enterprise Manager cannot be used for database control (364982)

In this release, you cannot use Oracle Enterprise Manager for database control.

For more information, see TechNote 277440 at:

<http://seer.entsupport.symantec.com/docs/277440.htm>

VCS Hardware Replication Agent for EMC MirrorView

The following issues apply to VCS Hardware Replication Agent for EMC MirrorView.

MirrorView resource cannot be brought online because of invalid security file (769418)

If a configured MirrorView resource cannot be brought online successfully, the problem may be an invalid security file. Review the steps for executing the `addArrayuser` action in the *Veritas Cluster Server Hardware Replication Agent for EMC MirrorView, Configuration Guide* and verify that the steps were followed correctly. If you did not specify a password as an Action Argument when executing the `addArrayUser` action, an invalid security file for the SYSTEM user is created on the local and remote arrays. Executing the `addArrayuser` action again with a valid password does not overwrite the invalid security file.

To resolve this issue, you must modify the `addArrayUser.pl` action script and re-execute it to remove the invalid security file. The `addArrayUser.pl` script is located in the directory, `%ProgramFiles%\Veritas\cluster server\bin\MirrorView\actions`.

Make a copy of the original `addArrayUser.pl` script before you make any changes to the script.

The following procedure removes the security file created for the SYSTEM user.

To remove the security file created for the SYSTEM user

- 1 In the `addArrayUser.pl` script, replace the line:

```
my $cmd = "\" . $java_home . "\\java\" -jar \"" . $NaviCliHome  
. "\\navicli.jar\" -h " . $LocalArraySPNames[$i] . "  
-AddUserSecurity -Password $arrayPasswd -Scope 0";
```

with the line:

```
my $cmd = "\" . $java_home . "\\java\" -jar \"" . $NaviCliHome  
. "\\navicli.jar\" -h " . $LocalArraySPNames[$i] . "  
-RemoveUserSecurity";
```

- 2 In the `addArrayUser.pl` script, replace the line:

```
my $cmd = "\" . $java_home . "\\java\" -jar \"" . $NaviCliHome  
. "\\navicli.jar\" -h " . $RemoteArraySPNames[$i] . "  
-AddUserSecurity -Password $arrayPasswd -Scope 0";
```

with the line:

```
my $cmd = "\" . $java_home . "\\java\" -jar \"" . $NaviCliHome  
. "\\navicli.jar\" -h " . $RemoteArraySPNames[$i] . "  
-RemoveUserSecurity";
```

- 3 After you have modified the `addArrayUser.pl` script, save the changes.
- 4 Execute the `addArrayUser` action to remove the invalid security file. Consult the *Veritas Cluster Server Hardware Replication Agent for EMC MirrorView, Configuration Guide* for more details on executing the `addArrayUser` action. You do not need to specify an Action Argument.
- 5 The action should complete successfully. If an error is returned, verify that the changes to the `addArrayUser.pl` script were made correctly and verify that the script is in the correct location.
- 6 After the invalid security file has been removed, revert the modified `addArrayUser.pl` script back to the original script, and follow the procedure for executing the `addArrayUser` action again.

Disaster Recovery Configuration Wizard

The following are Disaster Recovery Configuration Wizard issues.

The DR Wizard does not provide a separate “GCO only” option for VVR-based replication (1184660)

The Disaster Recovery Configuration Wizard provides a “GCO only” option for hardware array-based replication only, not for VVR-based replication. If this option is selected, before proceeding to GCO configuration, the wizard creates a storage and service group configuration intended for use in hardware array-based replication and incorrect for a VVR configuration. For VVR replication you should instead choose the option to configure both VVR Replication and GCO. If you do not want the wizard to configure the VVR replication but only GCO, you do the following:

To configure GCO only

- 1 Select the option **Configure Veritas Volume Replicator (VVR)** and the **Global Cluster Option (GCO)**
- 2 Exit the wizard after configuring the service group.
- 3 Configure VVR replication without using the wizard.
- 4 Restart the wizard and select the same VVR and GCO replication option.

The wizard recognizes that the VVR replication settings are complete, and enables you to proceed to GCO configuration.

The Disaster Recovery Wizard fails if the primary and secondary sites are in different domains or if you run the wizard from another domain (853259)

The Disaster Recovery Wizard requires that the primary and secondary sites be in the same domain. In addition, you must launch the wizard from within the same domain as the primary and secondary sites.

Otherwise, when you select the secondary site system, the wizard returns the error that it was unable to perform the operation and that it failed to discover Veritas Cluster Server.

The Disaster Recovery Wizard may fail to bring the RVGPrimary resources online (892503)

During the final stage of disaster recovery configuration with the Disaster Recovery Wizard, the last action is to bring the RVGPrimary resources online. In some cases, the wizard displays an error on its final panel and notifies you to bring the resources online manually.

Workaround: Use the Cluster Manager (Java console) to manually bring online the RVGPrimary resources of the selected application service group and any dependent group.

The Disaster Recovery Wizard requires that an existing storage layout for an application on a secondary site matches the primary site layout (781923)

The Disaster Recovery Configuration Wizard is designed to use for a new installation on the secondary site. Because it clones the storage, you do not need to configure the storage at the secondary site.

If you configure disk groups and volumes at the secondary site and install the application before you run the Disaster Recovery Wizard, the following limitations apply:

The wizard recognizes the storage at the secondary site only if it exactly matches the layout on the primary site. If there is a mismatch in volume sizes, the wizard can correct this. Otherwise, if the layout does not match, the wizard will not recognize that a storage layout already exists.

If it doesn't find a matching storage layout, the wizard will clone the storage from the primary site, if there is enough disk space. The result is two sets of disk groups and volumes:

- The set of disk groups and volumes that you created earlier
- The different set of disk groups and volumes that the wizard created by cloning the primary storage configuration

Workaround: If you have already created the storage layout at the secondary site and installed the application, use the Disaster Recovery Wizard only if the layout exactly matches the layout on the Primary site.

Otherwise, if the wizard creates a different set of disk groups and volumes than what you have created earlier, you must set up the application to use the disk groups and volumes created by the Disaster Recovery Wizard before you can continue with the wizard.

The Disaster Recovery Wizard may fail to create the Secondary Replicator Log (SRL) volume (896581)

If the VMDg resource is not online on the selected Secondary system, the Disaster Recovery Wizard fails to create the SRL volume. This can occur if the disk group for the selected service group has not been imported on the selected secondary system so that the VMDg resource is not online.

Workaround: Exit the wizard. Bring the VMDg resource for the selected service group online at the secondary node where you are configuring replication. Then run the Disaster Recovery Wizard again.

The Disaster Recovery Wizard may display a failed to discover NIC error on the Secondary system selection page (893918)

The Disaster Recovery Wizard may display a failed to discover NIC error on the secondary system selection page. This can occur if it encounters a problem with the Windows Management Instrumentation (WMI) service on one of the cluster nodes.

Workaround: Exit the wizard and check if the Windows Management Instrumentation (WMI) service is running on the node identified in the error message. If not, start the service and restart the wizard.

If the error repeats, you can troubleshoot further by checking if there is a problem with the WMI repository on the node. To check for problems, use the WMI test program `wbemtest.exe` to enumerate instances of `Win32_NetworkAdapterConfiguration` and `Win32_NetworkAdapter`. If they do not enumerate successfully, fix the problem with the WMI repository before restarting the wizard.

Service group cloning fails if you save and close the configuration in the Java Console while cloning is in progress (1216201)

While the Disaster Recovery Wizard is cloning the service group, if you save and close the configuration in the Java Console while cloning is still in progress, the cloning fails with an error.

Workaround: Delete the service group on the secondary site. Run the wizard again to clone the service group.

If RVGs are created manually with mismatched names, the DR Wizard does not recognize the RVG on the secondary site and attempts to create the secondary RVG (1214003)

The Disaster Recovery Wizard configures VVR replication for you. However, if you choose to configure the replication outside of the DR Wizard, ensure that you use the same names for the RDS and RVG on both sites. Otherwise, if the secondary site has a different RVG name than the primary, when you run the wizard, the wizard finds the primary site RVG information but does not recognize the misnamed secondary site RVG. On the replication action page, creation of the secondary RVG fails.

Workaround: Rename the misnamed RVG on the secondary site to match the primary site. You can run the wizard again and continue with GCO configuration. Refer to the *Veritas Volume Replicator Administrator's Guide* for more information on implementing VVR manually.

Cloned service group faults and fails over to another node during DR Wizard execution resulting in errors (1177650)

After service group cloning is complete, a resource fault may occur in the service group on the secondary site, causing the cloned service group to fault and fail over to the other cluster node. As a result, when the wizard proceeds to the replication Implementation stage, implementation actions may fail because the resource is online on the other node.

Workaround: If you discover that the cloned service group has failed over to another node resulting in any failure of the actions shown on the wizard Implementation page, delete the cloned service group completely and run the DR Wizard again.

DR wizard may display database constraint exception error after storage validation in EMC SRDF environment (1127959)

The DR wizard storage validation on the secondary site may result in a constraint exception error (duplicate database objects) shown on the Storage Validation page of the wizard. This error can occur because the array information and the Volume Manager information cached in the VEA are not in synch. This error is most likely to happen in an EMC SRDF environment. Rescanning the storage on the secondary node to update the Volume Manager information can often resolve this error.

Workaround: Check the storage configuration on the secondary site for any errors. Using the VEA, rescan the storage on the secondary node on which the error occurred.

On Windows Server 2008 R2 and SP2, DR wizard creation of secondary RVGs may fail due to mounted volumes being locked by the OS (1299615)

A Windows Server 2008 issue causes the operating system to intermittently lock mounted volumes. Microsoft released a hotfix for this issue, included in Windows Server 2008 SP1, but the issue is still seen in Windows Server 2008 R2 and Windows Server 2008 SP2. This volume lock issue can result in the DR wizard failing to create secondary RVGs. This issue is more likely to occur if there are many disk groups and volumes in the configuration. In such a case the wizard may successfully complete configuring some but not all RVGs. If the wizard is then run again to complete the RVG configuration, the wizard is unable to complete setting up the RLINKs for the RVGs that were configured earlier.

Workaround: Offline all mountV resources at the secondary site before using the wizard to configure replication and GCO. If a failure occurs while configuring secondary RVGs, delete any existing secondary site RVGs before you re-run the wizard.

Fire Drill Wizard

The following are Fire Drill Wizard issues.

Fire Drill Wizard may fail to recognize that a volume fits on a disk if the same disk is being used for another volume (893398)

When using the Fire Drill Wizard to prepare the fire drill configuration, you can assign disks for the snapshot volumes. If you assign more than one volume to the same disk, the Fire Drill Wizard requires that the disk size be large enough to accommodate the size of both volumes combined, even if one of the volumes is being assigned to another disk as well. For example, if you have a 10-GB volume assigned to disk A and disk B, and a 5-GB volume assigned to disk B, the Fire Drill Wizard only allows this assignment if disk B has at least 15 GB free.

Workaround: Assign volumes to separate disks or ensure that if more than one volume is assigned to a disk then it is large enough to accommodate all the volumes assigned.

Fire Drill Wizard may time out before completing fire drill service group configuration (1296532)

In some larger application service group configurations with many resources, the Fire Drill Wizard may time out before it is able to complete the fire drill service group configuration.

Workaround: The default value for the wizard time-out is 600000 milliseconds, the equivalent of 10 minutes. If the wizard times out, you can reset the default time value in the Windows registry to a longer time, for example to 20 minutes.

For a 32-bit OS, modify the following registry setting:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\winsolutions\TimeLimit
```

For a 64-bit OS, modify the following registry setting:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Veritas\winsolutions\TimeLimit
```

RegRep resource may fault while bringing the fire drill service group online during "Run Fire Drill" operation

Occasionally, when you run a fire drill using the Fire Drill Wizard, the RegRep resource faults and the fire drill service group fails to come online. This occurs due to a VCS error (V-16-10051-5508).

To work around this issue

- 1 Stop the Fire Drill Wizard.
- 2 In the VCS Java Console, bring the fire drill service group offline.

- 3 In the fire drill service group, bring online the MountV resource on which the RegRep resource depends.
- 4 Copy the contents of the primary RegRep volume to the secondary RegRep volume.
- 5 Bring online the entire fire drill service group. If no other problem exists, the service group comes online.
- 6 Run the Fire Drill Wizard again, selecting the **Restore to Prepared State** option. You can then select the **Run Fire Drill** option to run the fire drill again.
- 7 Proceed as during a normal run of the Fire Drill Wizard.

Fire Drill Wizard in an HTC environment is untested in a configuration that uses the same horcm file for both regular and snapshot replication (1703762)

In a Hitachi TrueCopy hardware replication environment, the Fire Drill Wizard has only been tested using two separate `horcm` files on the secondary site for the snapshot replication. In other words, it has been tested in a configuration with four `horcm` files as follows:

- Two matching `horcm` files on the primary and secondary site used for replication
For example, a `horcm10.conf` on the primary site and an identical `horcm10.conf` on the secondary site
- Two additional `horcm` files (`horcm11.conf` and `horcm12.conf`) on the secondary site, used for the fire drill snapshot replication. The `horcm11.conf` file is the same as `horcm10.conf` except that it uses the secondary site IP address.

This configuration has been tested on the following array:

- Hitachi Thunder 9570 (Micro Code version – 065F/D)

The following snapshot configuration has not been tested and therefore results are unknown:

- Two matching `horcm` files (for example, `horcm10.conf`) on the primary and secondary site used for replication
- One additional `horcm` file (`horcm11.conf`) used along with the `horcm10.conf` file on the secondary site for the fire drill snapshot replication

Other issues

The following are other issues.

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

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

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

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

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

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

```
hagrpl -offline service_group -sys system_name -clus cluster_name
```

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

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

VCS wizards may fail to probe resources (1318552)

While creating resources and service groups using VCS wizards, if you choose to bring the resources or service groups online, the wizards may fail to probe the resources. The following error is displayed:

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

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

Backup Exec 12 installation fails in a VCS environment (1283094)

If you try to install Backup Exec 12 on systems where VCS is already configured, the installation may fail. This failure happens on 64-bit systems.

Workaround: Stop the Veritas High Availability Engine (HAD) on all the cluster nodes and then proceed with the Backup Exec installation.

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

While running the VCS Cluster Configuration Wizard (VCW), the options to retrieve a list of systems and users in the domain on the **Domain Selection** panel are available only for the first time you run the wizard. If you click **Next** and then click **Back** to go back to the panel, all or some of these options appear disabled.

Workaround: Exit and launch the wizard again.

If VCS upgrade fails on one or more nodes, HAD fails to start and cluster becomes unusable (1251272)

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

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

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

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

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

To workaround this issue

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

Type the following on the command prompt:

```
net stop had
```

```
net stop llc
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 4 From the Windows Services snap-in, change the startup type of the Veritas High Availability Engine (HAD) service to Manual.
- 5 Repeat step 2, step 3, and step 4 on all the nodes on which VCS was upgraded successfully.
- 6 On one of the nodes on which VCS was upgraded successfully, open the VCS configuration file `main.cf` in a text editor and remove the entries of all the cluster nodes on which the VCS upgrade failed.

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

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

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

Type the following on the command prompt:

```
net start had
```

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

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

Contact Symantec Technical Support for more information.

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

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

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

Changes to referenced attributes do not propagate

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

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

For example, the `ArgList` of the `MountV` resource contains the `DiskGroupName` attribute of the `VMDg` resource. If you change the `VMDg` resource name or the `SystemList`, the VCS engine does not communicate the change to the `MountV` agent, causing it to fault. In such a situation, you can reconfigure the `MountV` agent using one of the following methods:

- Refresh the `VMDgResName` attribute for the `MountV` resource. Set the attribute to an empty string "" first, then reset it to the new `VMDg` resource name.
- Stop and restart the `MountV` agent on the system.

ArgListValue attribute may not display updated values

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

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

MountV resource comes online with drive letter mapped to network share (254586)

On systems running Windows Server 2003, a MountV resource can be mounted and brought online using a drive letter that is already mapped to a network share.

Known behavior with disk configuration in campus clusters

The campus cluster configuration has the same number of disks on both sites and each site contains one plex of every volume. Note that an environment with an uneven number of disks in each site does not qualify as a campus cluster.

If a site failure occurs in a two-site campus cluster, half the disks are lost. The following cases may occur:

- The site in which the service group is not online fails.
- The site in which the service group is online fails.

The behavior and possible workarounds for these conditions vary.

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 -local -force` command to stop the cluster or node where any such group is online. This workaround is not required if the cluster or node is stopped without the force option.

VCS Simulator installation may require a reboot (851154)

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

Unable to output correct results for Japanese commands (255100)

When the Veritas Command Server starts up on a Windows setup, it runs as a Windows service on a local system. A Windows service generally runs in the same

locale as the base Operating System's locale, and not the systems locale. For example, if a system is running an English version of Windows with a Japanese locale, then the CmdServer service runs in an English locale and not Japanese. Thus, when user commands are issued in Japanese the command server is confused when performing the Uniform Transformation Format (UTF) conversions and is unable to output the correct results.

Veritas Volume Replicator

This section provides information for Veritas Volume Replicator known issues.

On a DR setup, if Replicated Data Set (RDS) components are browsed for on the secondary site, then the VEA console does not respond

If RDS and RVG items are browsed for on the secondary site on a DR setup, then the Veritas Enterprise Administrator (VEA) console hangs up and does not respond. This is noticed only on the secondary site and not on the primary site.

Workaround: Create reverse lookup entries in the DNS for VVR IP and physical host.

Secondary host is getting removed and added when scheduled sync snapshots are taken (2010491)

Schedule a synchronized snapshot on the secondary host. It is noticed that sometimes when a synchronized snapshot happens on the secondary, the secondary gets removed and added. This is because the snapshot operation is taking too long to complete. To avoid this, increase the AE_TIMEOUT value in the registry to one minute. Its default value is set to 30 secs.

Windows Server 2003 SP1 Firewall

Windows Server 2003 SP1 has a firewall at the NIC level. If this firewall is enabled for after Windows Server 2003 SP1 is installed, it disrupts the communication between VVR Primary and Secondary.

Workaround: On a server with Windows Server 2003 SP1, either disable the Windows Firewall or configure the firewall to support VVR. For details refer to the *Veritas Volume Replicator Administrator's Guide*.

Replication may stop if the disks are write cache enabled (343556)

In some hardware configurations, if the standard Windows write back caching is enabled on the Secondary, replication may stop for prolonged time periods. In such cases, update timeout messages appear in the primary system event log. Because the Secondary is slow to complete the disk writes, a timeout occurs on the Primary for acknowledgment for these writes.

Workaround: Before setting up replication, disable write caching for the disks that are intended to be a part of the RDS. You can configure write caching through Windows Device Manager by right-clicking the disk device under the Device drives node and selecting **Properties > Policies**.

Discrepancy in the Replication Time Lag Displayed in VEA and CLI (299684)

When the Secondary is paused, you may note a discrepancy in replication time lag reported by the `vxrlink status` command, the Monitor view, and the `vxrlink updates` command. The `vxrlink status` command and the Monitor view display the latest information, while the information displayed by the `vxrlink updates` command is not the latest.

The vxrlink updates command displays inaccurate values (288514)

When the Secondary is paused and is behind the Primary, the `vxrlink updates` command may show inaccurate values. While the Replicator Log is receiving writes, the status displayed remains the same as before the pause. However, if the Replicator Log overflows and the Data Change Map (DCM) are activated, then the `vxrlink updates` command output displays the correct value by which the Secondary is behind. In DCM mode, the Primary reconnects the Secondary RLINK and sends updated information, including the time associated with the last update sequence number on the Primary.

Some VVR operations may fail to complete in a Cluster Environment (309295)

If an RVG is a part of a VCS cluster and the cluster resource for this RVG exists, then VVR fails the Delete RDS, Delete Secondary RVG, Delete Primary RVG, Disable Data Access, Migrate, or Make Secondary operations with the following error:

```
Cannot complete operation. Remote node closed connection
```

This issue is a timing issue. The VVR VRAS module times out before completing the check to determine if the RVGs participating in the operation already have a resource created.

Workaround: To prevent the timeout, make the following change on all cluster nodes of the Primary and Secondary cluster:

To change the timeout value

- 1 Open the registry editor using the command, `regedit`.
- 2 Navigate to the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\VRTSobc\pal33\Agents\  
StorageAgent\constants
```

- 3 Modify the registry DWORD value for the `AE_TIMEOUT` entry, from the default value of 30 seconds to 60 seconds or higher.

On 64-bit systems the `AE_TIMEOUT` key is located at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VERITAS\VRTSobc\  
pal33\Agents\StorageAgent\constants\version\constants
```

- 4 In order for the registry key change to take effect, at the command prompt type:

```
vxassist refresh
```

IBC IOCTL Failed Error Message (496548)

At times, the `vxibc register` or the `vxibc unregister` command may display the following error message:

```
Error V-107-58644-932: IBC IOCTL failed
```

Workaround: Verify that you have specified the correct RVG or disk group name with the command.

Pause and Resume commands take a long time to complete (495192)

At times, the pause and resume operation can take a long time to complete due to which it appears to be hung.

Workaround: Wait for some time till the operation completes, or manually disconnect and reconnect the network that is used for communication to enable the operation to complete.

Replication keeps switching between the pause and resume state (638842, 633834)

In a setup that is configured for Bunker replication, if a failure occurs at the primary site, then the Bunker is used to replay the pending updates to the secondary. Later, when the primary node becomes available again, the Bunker can be deactivated and replication can be started from this original primary to the secondary. However, performing any other intermittent operations such as detaching or attaching the RLINK, before starting replication from the original primary can cause the replication to switch between the pause and resume state.

Workaround: Recreate the Secondary RVG.

Replicating vxcache enabled volumes may display data corruption messages (700107)

Including vxcache enabled volumes as a part of an RDS may cause the following messages to be displayed, repeatedly. These errors are harmless and do not cause any data corruption.

```
vxio Warning Disk 57 N/A DELLS106 The system failed to flush
data to the transaction log. Corruption may occur.
vxcache Error None 19 N/A DELLS106 Fail irp: 89D870B8
status:c0000185
vxcache Error None 11 N/A DELLS106 Error in backend io irp:
878249E0 master irp:89D870B8 status:c0000010
```

VEA GUI has problems in adding secondary if all NICs on primary are DHCP enabled (860607)

When VEA is connected to the Primary host using "localhost" as the hostname and all the NICs on the primary server have DHCP enabled on them, then the Add Secondary Wizard fails to identify that it is connected to the Primary host and does not proceed further.

Workaround: To avoid this issue, connect to the Primary host using either the hostname or the IP address of the server.

Pause secondary operation fails when SQLIO is used for I/Os (1278144)

Pausing replication with checkpoints from the secondary host may fail for heavy I/Os and low-bandwidth network. If the secondary's request for RLINK checkpoint for Pause to primary times out before the primary's acknowledgment to the request, the pause operation would fail.

Workaround: To avoid this issue, perform one of the following procedures:

- Pause the secondary RVG by selecting the Pause Secondary option from the secondary RVG right-click menu. If it fails, slow down the I/O to the Primary host and retry. Secondary initiated pause lets you specify a checkpoint and maintains the connection between Primary and Secondary.
- Select the Pause Secondaries from Primary option from the Primary RVG right-click menu. If it succeeds, it can be used instead of using the pause replication from the Secondary host. In a Primary initiated pause, the Secondary host gets disconnected and checkpoints cannot be specified.

Performance counter cannot be started for VVR remote hosts in perfmon GUI (1284771)

Performance monitoring cannot be started if the file is saved under **Performance Logs and Alerts > Counter Logs**.

Performance counters can be started as follows:

To start performance monitoring

- 1 To start the file from the details pane, right-click and select the **Properties** dialog box. Then, select the **General > Run As** option.
- 2 In the **Run As** text box enter a username that has administrative privileges on your local computer. Select the **Set Password** tab to enter the password. If your computer is connected to a domain, then use the Domain Admin Group privileges.

Vxcache settings at volume level are lost while migrating the VCS MS Exchange 2003 service group between primary and secondary sites (1320795, 1322771)

On role change of primary and secondary nodes either through the Migrate or Takeover operation, VVR provider disables vxcache for the volumes in a replicated volume group. On subsequent role change from new secondary to primary, the VVR provider enables vxcache on that node if the policy is set to do caching. However, it is noticed that after enabling the vxcache for the volume, the “vxcache cacheinfo” does not reflect the true status.

Workaround: Run the `vxassist refresh` command from the CLI to refresh system information and get the desired output.

VVR Graphs get distorted when bandwidth value limit is set very high (1801004)

When bandwidth value is set to a very high value, VVR graphs get distorted.

BSOD seen on a Hyper-V setup (1840069)

When a virtual machine resource group is failed over, BSOD is noticed on Hyper-V.

Workaround: Run the cluster tunable command as shown. Symantec recommends that you set the value of x to 1:

```
cluster/cluster:clustername/prop HangRecoveryAction=x
```

Here x can take the following values:

- 0=disables the heartbeat and monitoring mechanism.
- 1= logs an event in the system log of the Event Viewer.
- 2=terminates the cluster services.
- 3=causes a Stop error (Bugcheck) on the cluster node.

Log volume and RDS volume on a clustered setup is missing after upgrading SFW HA from 5.1 to 5.1 SP1 on a Windows Server 2008 x64 SP1 setup (1795107)

After upgrading SFW HA from 5.1 to 5.1 SP1, it is noticed that the log volume and corresponding RDS volume is missing after system reboot and on making the service group online.

Workaround: The clustered disk group should be offlined and then onlined after completing the upgrade process and system reboot.

Unable to start statistics collection for VVR Memory and VVR remote hosts object in Perfmon (1670543)

Using Perfmon's alerts and counter logs, try to create a new log by selecting VVR memory or VVR remote hosts as objects. The log gets created; however, when we try to start statistics collection by selecting the log, it does not start.

Workaround: Use Perfmon's System Monitor page to directly add the VVR counters.

Bunker primary fails to respond when trying to perform stop replication operation on secondary (1544680)

If there are pending writes along with IBC messages on a bunker host that has multiple secondaries, then while replaying the pending writes from the bunker to the secondary site, the bunker host can experience a hang-like situation.

Workaround: Stop replication from the bunker host and either do a takeover on the secondary or synchronize with the existing primary by restarting replication.

Software fixes and enhancements in 5.1 SP2

Fixed issues and software enhancements are referenced by Symantec incident number and described briefly below for the 5.1 Service Pack 2 release.

Veritas Storage Foundation

[Table 1-15](#) describes the SFW issues that were fixed for the 5.1 SP2 release.

Table 1-15 Storage Foundation for Windows (SFW) fixed incidents for 5.1 SP2

Fixed Incidents	Description
1463998	Storage Agent (vxvm) crashes upon starting due to mount provider (mount.dll). Storage Agent requires a page file on all 64 bit versions of Windows Server 2008.
2148649	Storage related operations in a clustered environment fail due to the Microsoft Hotfix 982802
1739726	Disk regions pane is not cleared if there is no data to display
1788853	vxddmpadm allperf fails on HDS AA array
1794385	Event:1067: Storage Agent process terminated unexpectedly. If the ddlprov.dll (DDL provider)provider has corrupted the memory, it causes the Storage Agent service to crash. Disabling or renaming it prevents the Storage Agent service to load the provider and avoiding the crash.
1803180	Failover issue with VMDg and MountV

Table 1-15 Storage Foundation for Windows (SFW) fixed incidents for 5.1 SP2
(continued)

Fixed Incidents	Description
1840786	Adding a DRL to a 9TB mirrored volume causes 8-10 second file access delay. Without the DRL, there is no delay in file access. The DRL was added and removed few times and issue was clearly identified to be related to DRL.
1861896	Storage Agent terminates due to EMC Invista devices
1863354	Two LUNs from an IBM 2180XIV are claimed by both VEMCSYMM and VXIV Device specific Modules (DSMs)
1864647	Server XSVSQL03 with active SQL server instance unable to communicate with Active Directory (AD) Domain controllers. Unable to login into server when it was hung.
1882296	Storage Agent terminates due to VDID Hitachi.dll
1915142	Windows Server 2008 Failover Cluster cannot offline Volume Manager Disk Group (VMDg) resources after running for 48 hours
1919142	Unable to import SCOM 2007 Management Pack, Symantec.SFW.mp version 5.1.1.0 on SCOM 2007 SP1
1920075	VMDg resource creation in MSCS fails with 'attempting to add pages from the extension.dll error
1920541	Storage agent terminates due to ddlprov/vdid
1923059	Windows Failover Cluster encounters issues and RHS points at vxres.dll
1927505	Disks are not visible in the VEA after upgrading to 5.1 SP1 using vibmaad.sys DMP DSM

Table 1-15 Storage Foundation for Windows (SFW) fixed incidents for 5.1 SP2
(continued)

Fixed Incidents	Description
1928963	<p>Unable to reserve majority of disks after upgrading SFW 5.1 to SFW 5.1 Service Pack 1 (SP1).</p> <p>Passive node was upgraded to SFW 5.1 SP1 but unable to failover the service group to the upgraded node.</p>
1931195	Server hangs when VVR secondary is disconnected.
1932717	<p>MSA2012fc disks missing in SFW 5.1 Service Pack (SP1).</p> <p>After upgrading or clean install to SFW 5.1 Service Pack 1 (SP1), LUNs from MSA2012fc are not seen using the "vxdisk list" even though they can be seen on the Device Manager which works as expected on SFW 5.1.</p>
1939313	MSCS Cluster Service is unable to start when an user moves the Quorum from the basic disk to dynamic causing the resource monitor (resrcmon) to crash unexpectedly.
1955572	NBU Advance Client process takes 40-50 minutes to complete, even with no data changes occurring . This is caused by lengthy SFW rescans on the off-host server.
1959339	During first cluster service startup after reboot Quorum resource is taking too long to come online
1961245	<p>Windows Cluster 2008 MSDTC resource fails to come online when dependent on VMDG resource.</p> <p>MSDTC resource dependent on Physical Disk resource online correctly. MSDTC resource dependent on VMDG resource with files on dynamic volume can be configured, but does not online again once taken offline.</p>

Table 1-15 Storage Foundation for Windows (SFW) fixed incidents for 5.1 SP2
(continued)

Fixed Incidents	Description
1971818	VSS snapshot fails with "VSS Provider reached an unexpected provider error"
1992881	Volumes taking long time to arrive
1994874	VMDg resources timeout during online due to volume arrival issue even though it appears the volume arrives successfully from Pnp
1998592	Unable to pass Microsoft cluster validation check when VMDg resource is present.
2002204	The 5.x Capacity Monitor rule cannot pass volume name to script as it did in the 4.x product
2019623	DMP DSM Disk 7 and Disk 9 path report incorrect information
2020749	SFW commands fails with error V-77-57616-2 Server Initialization failed when the user name contains special characters
2022740	When attempting to perform a VSS snapshot, a warning is received in the Sys Event Log stating: Event ID 7 vxio: kernel log full: volume <volume name> detached
2024086	Vxio.sys crashes with bugcheck ID 0x3b
2024551	Storage Agent crashes when adding a new LUN to the system
2029224	Installer needs to add new and update existing Track Aligned Value (TAV) settings. Track aligned value was set to 96 by VM.msi which is an incorrect value and should be set to 128.

Table 1-15 Storage Foundation for Windows (SFW) fixed incidents for 5.1 SP2
(continued)

Fixed Incidents	Description
2037388	Server blue screen after failover. BugCheck7E - SYSTEM_THREAD_EXCEPTION_NOT_HANDLED
2042439	Cluster failure due to resource monitor (resrcmon) crash
2051334	Storage Agent crash due to vssprov interaction with SQL Writer
2051864	VMDg resources in a Windows Failover Cluster fail to come online until a rescan is performed on the cluster node in the VEA console
2052875	During Failover tests, the Volume Manager Disk group (VMDg) resources failed to come online due to disk group import issues During Failover tests, the VMDg resource failed to online due to DG import issues - DG_FAIL_NO_MAJORITY
2056039	Allow cluster resource to offline volumes before offlining disk group
2073785	In IBM DS8000, DMP adds two unrelated disks to single MPIO object (VIBMAADS)
2081736	After installation of DDI-1 on X64 SFW 5.1 Sp1 vxdmpadm.exe does not work anymore.
2082736	Adding disks from an XIV array causes bluescreen with bug check ID 0xCA
2104970	Unable to failover between cluster nodes. Very slow volume arrival.
2131084	Enclosures are not created and volumes are shown in a stopped state after reboot following the uninstallation of CCStore

Veritas Cluster Server

[Table 1-16](#) describes the issues that were fixed in the 5.1 SP2 release.

Table 1-16 Fixed issues for Veritas Cluster Server 5.1 SP2

Fixed incidents	Descriptions
1297012	<p>Disk time out value not reset during SFW uninstall</p> <p>When SFW is installed in an MSCS or VCS environment, the disk time out value in the Windows registry is changed to 60 seconds. During the uninstall of SFW in this environment, the disk timeout value in the Windows registry is not reset to its original value.</p> <p>After completing the uninstall of SFW, you may restore the original disk time out value by accessing the Windows registry (HKEY-LOCAL-MACHINE\SYSTEM\CurrentControlSet\Services\Disk) and manually change the TimeOutValue key.</p>
1803383, 2007447	<p>LLT protocol driver on windows did not handle plug-n-play messages from underlying NIC card. As a result, when underlying NIC card was removed or disabled, LLT protocol service caused machine to hang. This change allows LLT to unbind from the NIC card, when a plug-n-play message indicating NIC removed is received.</p>
1850959, 1867937, 1993047	<p>The following issues have been fixed in the HTC agent:</p> <ul style="list-style-type: none"> ■ If the horctakeover command times out or encounters an error condition, the service group is frozen in the cluster, and a critical message is logged in the engine log. The message indicates that there is manual recovery operation that needs to be performed on the array before you can switch/failover the service group to another node in the cluster. ■ The HTC agent's open function no longer starts the Hitachi RAID manager as in the previous versions of the agent. ■ The HTC agent does not require specifying the User, Domain, and Password attributes to freeze the group on the remote cluster. ■ The agent supports replication status monitoring and trap generation with LinkMonitor=2 in Replicated Data Cluster (RDC) environments. ■ The agent validates that the value of OnlineTimeout for the HTC type is >= 10 seconds. If this value is set to less than 10 seconds, the agent logs an appropriate error message. Symantec recommends that you set the OnlineTimeout value to 10 seconds or more. ■ HTC service group concurrency violation issue in secure clusters

Table 1-16 Fixed issues for Veritas Cluster Server 5.1 SP2 (*continued*)

Fixed incidents	Descriptions
1872419	When a large number of MountV resources (typically more than 100) are configured in a service group, it is observed that the VCSAgDriver process utilizes a high amount of processor time (upto 100% CPU usage) while the service group is online. The CPU spike was observed during the MountV agent's monitor function. This issue occurs on Itanium systems.
1876562	SQL service user account specified during SQL Server 2008 installation does not have local administrative privileges on all the cluster nodes.
1882383	The VCS MountV agent is modified to include the following change: Depending upon the ForceUnmount attribute value the agent unmounts the volumes either gracefully or forcefully, irrespective of the type of access applications have on the volumes.
1882687	Microsoft Outlook clients configured to use RPC over HTTP are unable to connect to Exchange Server 2003 configured under VCS.
1916965	Fix in the Mirrorview agent for Consistency group support for sync. mode and "Invalid mix of states" error handled.
1926484	The RegRep agent stores the registry changes at a different location than what is specified in the configuration. This happens whenever the service group system list is modified (either a node is added or removed) when the RegRep resource is online in the cluster.
1927325	When the system level attribute "CPUUsageMonitoring" is enabled, the VCS engine (HAD) logs display the following message: VCS ERROR V-16-1-50120 Error in enabling CPUUsage monitoring: -1073738810 VCS fails to enable the attribute and as a result is not able to monitor the CPU usage on the cluster nodes.
1929104	This issue occurs where Exchange 2007 is clustered with VCS. Users are unable to access their Exchange mailboxes using Outlook Web Access. The following URL fails to redirect to the Exchange 2007 Client Access Server. http://EVS/Exchange The workaround mentioned in the following technote solves the issue only for an Active-Passive Exchange configuration. In an Any-to-Any Exchange setup, the GenericService resources show a probe error on the nodes where the Exchange 2007 service group is offline. http://www.symantec.com/docs/TECH71937

Table 1-16 Fixed issues for Veritas Cluster Server 5.1 SP2 (*continued*)

Fixed incidents	Descriptions
1933048	In MSCS/FOC cluster, drive letter assignment for volume1 is not maintained after same drive letter is used for volume2 and is deported.
1937380	<p>After updating the VCS management pack (Symantec.SFW.HA.mp, ver 5.1.10000.1) and the VCS Library Management Pack (Symantec.VCS.Library.mp, ver 5.1.10000.2) the Helper Process utility (MOMHelper.exe) keeps terminating and the following error is observed:</p> <p>Forced to terminate the following process started at <time> because it ran past the configured timeout 60 seconds.</p>
1940265	<p>This issue occurs when the IIS FTP service is clustered using VCS.</p> <p>In an IIS service group, a VCS IIS resource is configured for the FTP Publishing Service (MSFtpsvc). However, this VCS IIS resource fails to probe.</p> <p>The IIS agent log displays the following message:</p> <p>VCS ERROR V-16-10051-13504 IIS:testftp-MSFTPSVC-IIS:monitor:Failed to find the service object. Please check the "SiteType" attribute. (MSFTPSVC)</p>
1943088	Performance issues with VCS when you configure service groups that contain a large number of MountV and VMDg resources (typically over 20 disk groups and over a 100 MountV resources).
1943534	<p>On Windows Server 2008, the MSMQ resource fails to come online due to a permissions issue.</p> <p>The following errors are observed in the agent log:</p> <ul style="list-style-type: none"> ■ VCS ERROR V-16-10041-17059 ■ MSMQ:<servicegroupname>-MSMQ:online:SetFileSecurity error! (rc=5) ■ VCS ERROR V-16-10041-17062 ■ MSMQ:<servicegroupname>-MSMQ:online:Failed to set permissions to the MSMQ storage. Error 5. <p>The MSMQ agent runs in the local system context. The MSMQ agent assigns the MSMQ service SID with full control privileges to the MSMQRootPath. If there is any change in the permissions such that the local system account does not have privileges on the file system, then the MSMQ agent is unable to assign the MSMQ service SID with full control privileges to the MSMQRootPath. Without the required permissions, the MSMQ resource fails to come online.</p> <p>On Windows Server 2008, the MSMQ virtual server queues failed to be seen from a remote system.</p>

Table 1-16 Fixed issues for Veritas Cluster Server 5.1 SP2 (*continued*)

Fixed incidents	Descriptions
1943578	<p>This issue occurs where Exchange 2007 is clustered with VCS. After failing over the Exchange 2007 service group, the ExchService2007 resource configured for the MExchangeMailSubmission service reports Event ID 39 and the internal mail flow stops working.</p> <p>This does not affect external SMTP-based mail delivery.</p> <p>This issue occurs only on service group failover.</p>
1951924	<p>SQL Server 2008 user databases are not accessible after a failover if the SQL service user account specified during SQL Server 2008 installation does not have local administrative privileges on all the cluster nodes.</p>
1919993, 1957237	<p>The following issue was observed with the VCS MountV agent:</p> <p>MountV agent is unable to offline the volumes if non-clustered applications have open handles to those volumes.</p>
1960076	<p>Process agent resources fault while trying to start the configured processes with the configured user credentials.</p> <p>The Process agent log displays the following messages:</p> <ul style="list-style-type: none"> ■ VCS ERROR V-16-2-13120 Thread(1748) Error receiving from the engine. Agent(Process) is exiting. ■ VCS ERROR V-16-10051-6531 Process:GenProc:online:Failed to get the password. ■ VCS ERROR V-16-2-13066 Thread(2572) Agent is calling clean for resource(GenProc) because the resource is not up even after online completed. ■ VCS ERROR V-16-2-13068 Thread(2572) Resource(GenProc) - clean completed successfully. ■ VCS ERROR V-16-2-13071 Thread(2572) Resource(GenProc): reached OnlineRetryLimit(0). <p>This issue is observed only on SFW HA 5.1 SP1.</p>
1960699, 1960731	<p>Improves failover performance of cluster disk groups when used with VCS.</p>

Table 1-16 Fixed issues for Veritas Cluster Server 5.1 SP2 (*continued*)

Fixed incidents	Descriptions
1962243	<p>The VCS SQL agent resources fault while trying to start the SQL service in the context of the configured user credentials.</p> <p>The SQL 2000 agent log displays the following message:</p> <pre>VCS ERROR V-16-20020-48 SQLServer2000:<servicegroupname>-SQLServer2000:monitor:Failed to decrypt the password. Error = -2.</pre> <p>The SQL 2005 agent log displays the following message:</p> <pre>VCS ERROR V-16-20050-40 SQLServer2005:SQL192-SQLServer2005:monitor:Failed to get the password attribute. Error = -2.</pre> <p>This issue is observed only on SFW HA 5.1 SP1.</p>
1979764	<p>The IP agent is unable to probe IP addresses if the first three octets and the first two digits of the fourth octet match those of the IP address manually assigned to the network adapter.</p> <p>The IP agent log contains the following message:</p> <pre>VCS WARNING V-16-10051-4008 IP:csg_ip:monitor:IP (<VirtualIPaddress>) is Admin IP</pre>
2005859	<p>The VCS Cluster Manager (Java Console) is unable to load the group templates.</p> <p>The following error is displayed:</p> <pre>VCS ERROR V-16-10-65: Could not load :- Hacf</pre> <p>This issue typically occurs if in the cluster configuration file, main.cf, references to types configuration files are specified using the absolute path.</p> <p>For example, if the entry for ClusterConnectorConfigType.cf file in the main.cf appears as follows:</p> <pre>include "C:\Program Files\Veritas\Cluster Server\conf\config\ClusterConnectorConfigType.cf"</pre> <p>The hacf utility creates temporary files before loading the templates. Absolute paths are not handled by hacf, therefore it fails to create the required temporary files and is unable to load the templates. In some cases, the hacf utility may also crash.</p>
2009727	<p>The SRDF agent does not perform failover correctly in SRDF/A environment with dynamic role-swap capable devices.</p>

Table 1-16 Fixed issues for Veritas Cluster Server 5.1 SP2 (*continued*)

Fixed incidents	Descriptions
2012768	<p>After bringing the file share service group online, the file share resource faults and fails over to the next available system in service group's system list. After coming online on the next system, the resource again faults on that system and fails back to the original system or to an alternate system. This fault and failover activity repeats itself in a cyclic manner.</p> <p>This issue typically occurs on multi-node (two or more nodes) file share service groups configured on Windows Server 2008 (SP2 and R2) systems.</p>
2017551	<p>VCW support for more than 2 network cards to create 2-8 private network links while configuring LLT over UDP.</p>
2018404	<p>VCS agents fail to convert the first argument of the arglist from UTF8 to OS encoding.</p> <p>This issue is seen when a system is set to a locale that has got multiple dot (".") characters in the locale name.</p> <p>The engine and the agent logs (of all the agent type resources configured) contains the following message:</p> <p>VCS ERROR V-16-2-13346 (<system_name>) Resource(<resource_name>): Failed to convert arglist attribute(<attribute_name>) from UTF8 to OS encoding</p> <p>For example: The locale, "Chinese (Traditional)_Hong Kong S.A.R." has got multiple dot characters and will cause the agent framework to fail to convert the agent arglist from UTF8 to OS encoding.</p>
2020013	<p>This issue occurs in a multi-node (e.g. 10 nodes) cluster environment where there is a temporary disruption in the VCS private network links configured in the cluster.</p> <p>When the private network links connection is restored, the VCS GAB may cause a panic on the nodes where there is an error in the gap sequence protocol that GAB uses to establish the cluster membership.</p> <p>This may result in a BSOD (0xbad400000 crash dump) on those nodes.</p>
2040049	<p>VCWSilent does not support LLT over UDP configuration</p> <p>VCS provides a silent configuration utility, VCWSilent.exe, that can be used to configure a new cluster. However, the VCWSilent.exe does not support configuring LLT over UDP.</p>

Table 1-16 Fixed issues for Veritas Cluster Server 5.1 SP2 (*continued*)

Fixed incidents	Descriptions
2066365	<p>This issue is seen when a considerable number of IIS sites (typically more than 10) are configured and the IIS wizard is used to configure these sites under VCS.</p> <p>While configuring the IIS service group, the IIS site discovery leads to a memory corruption and the wizard fails to discover the IIS sites. The IIS wizard may either hang or may fail to complete.</p> <p>The following Application Error event is generated in the Windows Event Viewer:</p> <p>"Faulting application hadiscover.exe"</p>
2077386	<p>On non-English operating system installations, after upgrading SFW HA 5.0 RP2 or later versions to SFW HA 5.1 SP1 the VCS resource types on the node are not updated.</p> <p>Agents, agent type definitions and default values that are introduced or modified in 5.1 SP1 are therefore not available after the upgrade. As a result, the existing VCS service groups may fail to probe or may not come online.</p>
2081131	<p>In some cases, when a user runs the hagetcf.exe diagnostic utility to gather the logs from a VCS node, havol.exe registers a process crash failing to return the complete information of the volumes of the node.</p> <p>The process crash occurs because hagetcf.exe invokes havol.exe in order to determine the drive and volume information of a node.</p> <p>An error similar to the following is logged:</p> <p>Event ID: 1000 Source: Application Error Description: Faulting application havol.exe, version 5.0.0.386, faulting module havol.exe, version 5.0.0.386, fault address 0x00044292.</p>
2088587	<p>The simconfig.txt file (symconfig in UNIX) which lists the cluster configurations, has an internal size limit of 4KB. Further, the error message does not adequately highlight the reason for the failure (the 4 kB limit).</p> <p>Due to this limitation, if you add a large number of cluster configurations to a VCS Simulator, then it may fail to start certain cluster configurations.</p> <p>The VCS Simulator may display the following error:</p> <p>V-16-1-49003 Cannot gather Simulator port configurations for cluster <clusname>.</p>

Table 1-16 Fixed issues for Veritas Cluster Server 5.1 SP2 (*continued*)

Fixed incidents	Descriptions
2110910	<p>Agents using perl scripts for monitoring fail to probe when the file perl is present in c:\Program files\Veritas\VRTSPerl\bin</p> <p>If you have created a file named "perl" without an extension in the folder where perl.exe is located, and you probe a resource using an agent that uses Perl scripts for agent functions, then the agent will fail to probe the resource and report an UNKNOWN state and fail to come ONLINE.</p> <p>This happens because there are two files with the same name while the agent was calling the "perl" file, and not "perl.exe" file.</p> <p>An error similar to the following is logged:</p> <p>VCS ERROR V-16-2-13038 Thread(448) Resource(VCSweb): Error executing the program (C:\Program Files\Veritas\Cluster Server\bin\VRTSWebApp\monitor.pl).</p> <p>This issue was observed only on SFW HA 5.1 and SFW HA 5.1 AP1</p>

Veritas Volume Replicator

[Table 1-17](#) describes the VVR issues that were fixed in 5.1 SP2 release.

Table 1-17 Veritas Volume Replicator (VVR) fixed Incidents for 5.1 SP2

Fixed incidents	Description
2053938	Frequent BSODs that are referencing vxio.sys 0x000000D5
2095754	Server blue screens after a failover operation is performed
2093478	Fix code in rpioctl.c duringnmcom_sender thread create which may cause a deadlock

Software fixes and enhancements in 5.1 SP1AP1

Fixed issues and software enhancements are referenced by Symantec incident number and described briefly below.

Veritas Storage Foundation

[Table 1-18](#) lists the SFW issues those were fixed in this Application Pack 1 release:

Table 1-18 Fixed issues for Storage Foundation for Windows

Incident Number	Description
1919142, 1925491	Unable to import the latest SCOM 2007 Management Pack due to Strong Name verification.
1959339	During first cluster service startup after a reboot, Quorum resource comes online after a long time.

Veritas Cluster Server

[Table 1-19](#) lists the VCS issues those were fixed in this Application Pack 1 release:

Table 1-19 Fixed issues for Veritas Cluster Server

Incident Number	Description
2012768	<p>After bringing the file share service group online, the file share resource faults and fails over to the next available system in service group's system list. After coming online on the next system, the resource again faults on that system and fails back to the original system or to an alternate system. This fault and failover activity repeats itself in a cyclic manner.</p> <p>This issue typically occurs on multi-node (two or more nodes) file share service groups configured on Windows Server 2008 (SP2 and R2) systems.</p>

Software fixes and enhancements in 5.1 SP1

Fixed issues and software enhancements are referenced by Symantec incident number and described briefly below for the 5.1 Service Pack 1 release.

Installation and licensing

[Table 1-20](#) describes the issues that were fixed in the 5.1 SP1 release.

Table 1-20 Fixed issues for installation and licensing

Incident number	Description
1442162	For an SFW 5.1 setup, running the Configuration Checker post-installation may display an invalid license and status failure message.
1481741	Unable to install or reinstall SFW or SFW HA 5.1, if Microsoft SQL 2008 is installed on the system or systems. If SFW or SFW HA 5.1 is installed after an SQL Server 2008 installation, or if you have installed SQL Server 2008 and need to reinstall SFW 5.1, then the installation may fail.
1521305	SFW HA 5.1 AP1 installation using the CLI and a non-standard install path may fail.

Veritas Storage Foundation

[Table 1-21](#) describes the issues that were fixed for SFW in the 5.1 SP1 release.

Table 1-21 Fixed issues for Veritas Storage Foundation

Incident	Description
1361969	Synchronization of missing schedule entries sometimes fails in multi-node clustered environment
1363774	In a multi-node cluster environment, Quick Recovery Configuration Wizard sometimes fails to create schedules on passive nodes
1368925	SFW scheduler service authentication vulnerability
1388819	Storage Agent terminates unexpectedly while running SFW HA
1427101	Quick Recovery Configuration Wizard does not display Storage Group volumes because folder mounts are not supported.
1431636	Installation fails when quorum does not reside on basic disk
1471343	After installing SFW 5.1 on Russian localized Windows, SFW services fail to start unless Windows locale setting is changed to US-English
1473350	Starting system after power off, mirror resynch operation does not complete
1501305	Abnormal termination after disk group import or deport
1505561, 1803180, 1828495	Missing or unarrived volumes cause VMDg agent and MountV agent to hang

Table 1-21 Fixed issues for Veritas Storage Foundation (*continued*)

Incident	Description
1508742	During system boot, PBX service fails to start (service-specific error 22 (0x16))
1517749	Quick Recovery Configuration Wizard was not able to identify Exchange 2007 in different root domain-child domain Exchange installation scenario.
1527445	Rule manager does not accept a hyphen in a domain name
1533045	The <code>vxdisk list</code> command does not display EMC storage devices (except Symmetrix)
1536740	VEA fails when using a policy to redirect the Windows desktop
1542971	Transportable snapshot support for Windows Server 2003
1555723, 1589601	After importing disk group, volume reported as missing or offline
1589012	VSS snapshot volumes mounted at time of snapshot
1591716	Volume/database corruption after create or break mirror operations
1596950	Request for <code>vxvol</code> command to provide volume GUID
1632428	Diskpart utility does not return correct dynamic disk information
1634370	Request for utility to provide PID, VID, and LUN Serial numbers
1650449	When adding disks to diskgroup, VMDg resource in MSCS cluster fails
1654592	Volumes missing in VEA after <code>vxvm</code> service restarted
1671998, 1702902	Creating rules with VEA fail with error V-52589-50102-29
1701858	In VEA, disk has no properties
1704638	Unable to take more than three snapshots of three Exchange Storage Groups simultaneously
1707031	Disk group deport results in excessive rescan operations
1723526	VSS snapshot operation creates duplicate snapshot volume names
1742444	File system corruption after evacuating disks
1764487	Unable to remove disk from Microsoft Disk Management disk group
1788460, 1836283	In VCS environment, MountV resource hangs during failover

Table 1-21 Fixed issues for Veritas Storage Foundation (*continued*)

Incident	Description
1790842	Missing pagefile causes Storage Agent to abnormally terminate
1794385	During system start up, storage agent does not start due to failed SCSI inquiry
1805877	Upgrading to SFW 5.1 AP1 results in earlier hotfix being overwritten
1832737	After installing a new disk, performing a rescan results in abnormal termination of Storage Agent

Veritas Cluster Server

[Table 1-22](#) describes the issues that were fixed in the 5.1 SP1 release.

Table 1-22 Fixed issues for Veritas Cluster Server 5.1 SP1

Fixed incidents	Descriptions
1200960	The VMGetDrive utility fails to complete on cluster nodes where there are a large number of disk groups imported.
1229217	The Lanman resource faults when it tries to perform the DNS refresh and one of the DNS servers is not available.
1262548, 1486465	Memory leak in IIS agent.

Table 1-22 Fixed issues for Veritas Cluster Server 5.1 SP1 (*continued*)

Fixed incidents	Descriptions
1276432	<p>This issue occurs where SQL Server is configured with VCS. While reindexing databases, SQL Server reports I/O errors messages of the following type are displayed in the Windows Application logs and the SQL logs:</p> <pre> INFORMATION 833(0x40000341) MSSQL\$CPSPRD01 NJIPWCPSDB01 SQL Server has encountered 1 occurrence(s) of I/O requests taking longer than 15 seconds to complete on file [<Database file name>] in database [<Database name>] (5). The OS file handle is 0x00000000000007D4. The offset of the latest long I/O is: 0x0000002b120000 </pre> <p>This issue may be related to the file system access function (CheckFSAccess) of the MountV agent. When file system access monitoring is enabled, the MountV agent checks the accessibility of the mounted volume. This may cause the I/O errors for SQL database operations.</p>
1296465, 1499225	<p>This issue occurs in cases where the VCS Global Cluster Option (GCO) is configured in a disaster recovery setup.</p> <p>If the ClusterService group (with the Wide Area Connector resource) and a global service group are online on the same cluster node at a multi-node primary site and that node fails or is shut down, the service group tries to fail over locally. However, if there is not a suitable failover node at the primary site, the service group does not fail over to a node on the secondary site (DR site). Thus global failover is unsuccessful.</p> <p>The VCS engine logs the following error:</p> <pre> VCS NOTICE V-16-1-52604 Global group <service group name> is no longer completely faulted in cluster. Canceling retry of cross-cluster failover. </pre>

Table 1-22 Fixed issues for Veritas Cluster Server 5.1 SP1 (*continued*)

Fixed incidents	Descriptions
1298362	<p>When a disk group is imported and the MountV resource is brought online, sometimes there may cases where volumes fail to arrive or may go missing. In such cases the MountV resource goes into an UNKNOWN state and the service group is unable to fail over. The following new agent behavior fixes this issue.</p> <p>If the MountV agent detects missing or unarrived volumes during online or other operations, the MountV resource faults and this initiates a service group failover. Also to provide more information at the disk group level, the VMDg agent detects missing or unarrived volumes during detail monitoring and logs the issue.</p>
1298649, 1486196	<p>If the volumes configured for Exchange are mounted as folder mount points, the Exchange Setup Wizard for VCS may fail to discover such volumes and crash intermittently.</p>
1316917	<p>The DR Wizard fails to create RVG, if the name of volume that is being replicated is assigned as a label to another volume.</p>
1363677	<p>The DR Wizard that failed to create primary RVGs after running the QR wizard on the primary site</p>
1369751, 1486518	<p>After configuring a print share service group with printers added in the virtual server, subsequent deletion of printers is not reflected upon failover to another nodes.</p> <p>This issue occurs due to RegRep agent's behavior of not processing the keys that are deleted. The printers are stored under a registry hive and the hive corresponding to the deleted printer is ignored by RegRep agent.</p>

Table 1-22 Fixed issues for Veritas Cluster Server 5.1 SP1 (*continued*)

Fixed incidents	Descriptions
1371162	<p>This issue occurs when Exchange is deployed in an Any-to-Any configuration with a front-end/back-end scenario, and the Exchange back-end server is clustered with VCS.</p> <p>When the Calendaring options for the Exchange protocols (POP3 and IMAP4) are configured to use the Exchange front-end server (Calendaringtab > Use front-end server option), VCS fails to bring the Exchange Protocol resources online.</p> <p>The Exchange Protocol agent log may display the following message:</p> <pre>VCS DBG_21 V-16-50-0 ExchProtocol:V03-IMAP4SVC-1: online:_UpdateMetabaseInformation() returned 100, 0x00000003 ExchProtocolRes.cpp:CExchProtocolRes::Online[207]</pre>
1372034, 1486465	<p>While upgrading to 5.0 RP1a, if the IIS agent attribute Site Type is set to APPPOOL, the IIS resource cannot be probed.</p>
1382400	<p>A node cannot be added to a cluster which has ClusterService service group configured and the node has only 1 public NIC enabled using HP NIC teaming software.</p>
1383348, 1486528	<p>After configuring a Process resource inside a service group and bringing it online, the Process agent memory usage increases with each offline, online, offline monitor operation. The memory usage pattern indicates leakage in these entry points. This leakage is observed only on Windows IA64 and Windows X64 based systems.</p>
1422649	<p>The File Share Configuration Wizard does not allow an existing or a new fileshare that has a space in the name.</p>
1423166	<p>The SQL Server 2005 Configuration Wizard sets the Lanman attributes ADUpdateRequired and ADCriticalForOnline to True even if the ADUpdateRequired check box is unchecked while running the wizard</p>
1426957	<p>The IP agent creates false DNS entries when IP resources are brought online in a VCS cluster.</p>
1427895	<p>Disaster Recovery Configuration Wizard failed with the error V-52410-49479-116 after specifying primary system name.</p>

Table 1-22 Fixed issues for Veritas Cluster Server 5.1 SP1 (*continued*)

Fixed incidents	Descriptions
1436651, 1452919	In a MOM 2005 SP1 monitoring environment, when a service group is taken offline from online state or online from offline state, if the VCS MOM script is called during the service group transition period, the state monitoring script generates alerts.
1437841	The Print Share Configuration Wizard is unable to detect externally modified printshare service groups in the modify mode. This happens due to the presence of unrecognized resources inside the printshare service group.
1445497	The Veritas Cluster Configuration Wizard (VCW) fails to recognize Network Interface Cards (NIC) on IBM eServer systems if NIC teaming
1451314	The RemoteGroup resource generates large number of VCSAgDriver.exe process handles.
1455173	Memory leaks in Veritas High Availability Engine (had.exe).
1461328	The Veritas Hitachi TrueCopy agent has been enhanced to include additional monitoring and reporting capabilities. You can now configure the agent to generate notifications depending on the state of the configured HTC devices.
1472638	Lanman attempts to update a DNS server other than the one that it is configured to update.

Table 1-22 Fixed issues for Veritas Cluster Server 5.1 SP1 (*continued*)

Fixed incidents	Descriptions
<p>1479886, 1484131, 1665485</p>	<p>A RegRep resource faults if the attribute ReplicationDirectory is modified when the RegRep resource is online in the cluster. This issue occurs if the registry replication directory on the shared disk is mounted using volume mount points. The following error messages are logged:</p> <pre>VCS NOTICE V-16-10051-5802 RegRep:RegRep:attrchanged:TRACE: Attribute changed: ReplicationDirectory VCS ERROR V-16-10051-5503 RegRep:RegRep:monitor:Directory does not exist (or) could not create (directory=<directory path>) VCS DBG_1 V-16-50-0 RegRep:RegRep:clean:Internal api failure (API=OpenFileMapping, Info=MAIN_SHARED_MEMORY) (Windows Error Code = 2) RegSharedMemory.c: RequestSharedMemory[36]</pre> <p>The RegRep agent creates corrupt registry file names.</p> <p>The RegRep agent fails to replicate registry key deletion changes made on a node on to the failover nodes in the cluster. For example, after configuring a print share service group with printers added in the virtual server, subsequent deletion of printers is not reflected upon fail over to another node. This issue occurs due to RegRep agent's behavior of not processing the keys that are deleted.</p>
<p>1480415</p>	<p>The following errors were fixed in the VCS Process Agent:</p> <ul style="list-style-type: none"> ■ Concurrency violation occurs as resource is brought online outside of VCS control on the passive cluster node. ■ Resource faults on the active Node because the resource is taken offline outside of VCS control. ■ Multiple processes running on the same server.
<p>1481743</p>	<p>The Process agent fails to probe when the configured user account password contains spaces. The following error is logged:</p> <pre>VCS ERROR V-16-10051-6531 Process:monitor:Failed to get the password</pre>

Table 1-22 Fixed issues for Veritas Cluster Server 5.1 SP1 (*continued*)

Fixed incidents	Descriptions
1483145	<p>The following errors were reported while switching service groups to the remote site in a VCS Global cluster environment:</p> <pre>VCS ERROR V-16-1-50101 Command (haclus -add remotecluster1 IP) failed. Cluster Administrator privilege required VCS ERROR V-16-1-50101 Command (hahb -modify ... -add Icmp ClusterList remotecluster1) failed. Cluster Administrator privilege required</pre> <p>This issue occurred because the user name contained "!" as the first character. VCS does not support certain characters for user accounts. In a secure cluster setup, this issue occurs even after setting up trust between the root brokers.</p>
1484011	<p>The ExchProtocol agent fails to start, stop, or monitor the Exchange Protocol servers POP3 and IMAP4 after these services were renamed and the Calendar tab modified from the Exchange System Manager.</p>
1510627	<p>This fix includes a disk filter driver (VxSCSIFilter) that enables VCS support for clustered disk groups created on internal disks attached to a Dell PERC6i storage controller. You must use the vxclus utility to set the conditions required to create clustered disk groups on internal disks. Refer to the Veritas Storage Foundation Administrator's Guide for more information about the vxclus utility.</p> <p>Limitations:</p> <ul style="list-style-type: none"> ■ This driver supports internal disks only. ■ This driver supports SCSI2 reservations only. SCSI3 is not supported. ■ This driver is supported on all flavors of Windows Server 2003 only.

Table 1-22 Fixed issues for Veritas Cluster Server 5.1 SP1 (*continued*)

Fixed incidents	Descriptions
1515403	<p>The VCS agent dlls were corrupted on one of the cluster nodes. As a result, service groups cannot be failed over to the affected node. The following error was displayed:</p> <pre>VCS ERROR V-16-1-1-195: Agent(s) for group <servicegroupname> failed on system <systemname>.</pre> <p>The agent logs contained the following message:</p> <pre>VCS ERROR V-16-2-13061 Thread(4252) Agent(MountV) is exiting because it could not load the agent library (C:\Program Files\Veritas\Cluster Server\bin\<agentname>\<agentname>.dll).</pre> <pre>VCS ERROR V-16-2-13120 Thread(3432) Error receiving from the engine. Agent(agentname) is exiting.</pre> <p>The service group fail over problem persisted even after the affected node was added back to the cluster after reinstalling VCS. This issue occurred because the agent's resource attribute "AgentFailedOn" retained the affected node name on which the agent dlls were initially corrupted. As this attribute was not cleared even after the affected node was rebuilt, the VCS engine considered that the agents on that node failed and hence the service groups cannot be failed over.</p>
1540399	<p>While configuring a SQL 2008 service group the SQL Server 2008 Configuration Wizard may crash when you click Next on the User Databases List panel.</p>
1544338	<p>After configuring the Print Share service group, the printer associated with the service group cannot be listed in the Active Directory Domain Services, even when the "List in the directory" option was enabled in the Printer Properties.</p>

Table 1-22 Fixed issues for Veritas Cluster Server 5.1 SP1 (*continued*)

Fixed incidents	Descriptions
1587279	<p>If there is a resource fault while taking a service group offline on a node, VCS fails to update the service group state details in the internal configuration. As a result, if that node is faulted, VCS triggers a local failover and brings the service group online on an alternate node.</p> <p>This failover is unintentional and should not have occurred as the service group was taken offline intentionally, either for modifying the resources or for some other maintenance purpose.</p> <p>This problem exaggerates in a global cluster (GCO) environment, when the global group is being taken offline on the primary site to bring it online on the secondary site. The group remains in offline state at the primary site and online at secondary site until the node at the primary site is in RUNNING state.</p> <p>As soon as the primary site node is faulted the service group comes online at the primary site. This results in a concurrency violation and possible data corruption.</p>
1596215	The timestamp for Solution wizard logs is not intuitive enough
1596233	While configuring the Enterprise Vault service group on 64-bit systems, the VCS Enterprise Vault Cluster Setup Wizard does not take into account the EV Wow6432 registry keys (HKLM\Software\Wow6432Node\Enterprise Vault) for replication.
1634310	Process agent resources after running for a period of time go into an unknown state and fail to come online.
1635911	<p>While configuring a SQL 2008 service group, the SQL Server 2008 Configuration Wizard may fail to enumerate the SQL databases and may crash when you click Next on the Instance Selection panel. This issue occurs because the wizard uses the logged-on user account context to connect to the databases. If the logged-on user does not have adequate privileges, the wizard may crash.</p> <p>If the logged on user account does not have the required privileges, the wizard displays an appropriate error and allows the user to proceed with the service group configuration.</p>
1650451	Reliability and security issue with Symantec Veritas VRTSweb.
1652239	If the VCS agent for SRDF Star is configured without any parent resources, rebooting the node where the resource is online may cause a concurrency violation when the node restarts.

Table 1-22 Fixed issues for Veritas Cluster Server 5.1 SP1 (*continued*)

Fixed incidents	Descriptions
1705162	The VCS print share and file share configuration wizards cannot detect externally modified print share and file share service groups when the wizards are run in the modify mode. This issue happens because of the presence of additional resources (apart from the default resources) in the service group.
1735775	The VCS SRDF agent on Windows now supports the SwapRole functionality. You can configure whether or not to swap the roles of the dynamic devices at the time of failover.
1737176	The VCS SQL 2008 Configuration Wizard is unable to detect externally modified SQL Server 2008 service group when the wizard is run in the modify mode. This happens because of the presence of additional resources (apart from the default resources) in the service group.
1737305	SQL Server 2008 monitoring is not supported with System Center Operations Manager 2007, if SQL Server 2008 is clustered with VCS.
1737309, 1751756	On Windows Server 2008, the 64-bit MOM helper utility generates errors during initialization.
1739675	The VCS <code>hasys -display</code> command lists information about the various systems in a cluster. However, in the command output the cluster node names are not separated with a "#" character.
1745782	When performing a move or a failover of the application service group to the DR site, the SRDF state shows 'Failed Over' instead of 'Synchronized' indicating that the Role Swap did not complete properly. This requires manual intervention to complete the Role Swap outside of VCS.
1766172	LLT on Windows NT padded llt packets to 64-byte size before transmission. This padding operation did not match allocated buffer size, causing incorrect buffer size reporting to NDIS, which in-turn caused the NIC card driver fail with bugcheck 0xD1.
1803180	When a disk group is imported and the MountV resource is brought online, sometimes there may cases where volumes fail to arrive or may go missing. In such cases the MountV resource goes into an UNKNOWN state and the service group is unable to fail over.

Table 1-22 Fixed issues for Veritas Cluster Server 5.1 SP1 (*continued*)

Fixed incidents	Descriptions
1803872	If there is a resource fault while taking a service group offline on a node, VCS fails to update the service group state details in the internal configuration. As a result, if that node is faulted, VCS triggers a local failover and brings the service group online on an alternate node. This failover is unintentional and should not have occurred as the service group was taken offline intentionally, either for modifying the resources or for some other maintenance purpose. This problem exaggerates in a global cluster (GCO) environment, when the global group is being taken offline on the primary site to bring it online on the secondary site. The group remains in offline state at the primary site and online at secondary site until the node at the primary site is in RUNNING state. As soon as the primary site node is faulted the service group comes online at the primary site. This results in a concurrency violation and possible data corruption.
1807359	The VCS agent for SRDF fails to determine dynamic RDF capabilities of array because symconfigure returns incorrect values.
1809463	Distributed Transactions fail when MSDTC is clustered with SQL Server 2005 on Windows Server 2008.
1843417	The Lanman resource fails to online if any of the DNS servers mentioned in the AdditionalDNSServers attribute are not reachable. Additionally, the Lanman resource faults during the DNSRefresh interval if any server in the AdditionalDNSServers attribute are not reachable when the refresh occurs.
1844266	SQL 2008 MSDTC does not work when under SFW HA 5.1 AP1 control.
1876899	SRDF agent entry points fail when creation of short file name is disabled on the system.

Veritas Volume Replicator

[Table 1-23](#) describes the issues that were fixed in the 5.1 SP1 release.

Table 1-23 Fixed issues for Veritas Volume Replicator

Fixed incidents	Description
1544666	Diskgroup autoimport fails if VVR objects are present on the diskgroup.

Table 1-23 Fixed issues for Veritas Volume Replicator (*continued*)

Fixed incidents	Description
1544669	SQL data was found to be stale after doing a failover to the other node.
1544673	System crash due to vxio.sys
1544677	"Duplicate virtual device number(s)" message logged on the system event log due to vxboot error on start-up.
1544678	If two disk groups are imported on the same node, data volumes of the second disk group never arrive.
1544686	Memory leak in storage agent (VVR provider and VRAS module)
1839444	VVR secondary server may crash when the VVR disk group is imported.

Software fixes and enhancements in 5.1 AP1

Fixed issues and software enhancements are referenced by Symantec incident number and described for the 5.1 Application Pack 1 release.

Veritas Cluster Server

[Table 1-24](#) describes the issues that were fixed in the 5.1 AP1 release.

Table 1-24 Fixed issues for Veritas Cluster Server 5.1 AP1

Incident number	Description
1298649	The VCS Exchange wizards may crash when folder mount points are present on the regrep volume.
1319212	Provide the Windows Active Directory dialog box to select and search Organizational Unit in the Exchange Setup Wizard for VCS.
1398535	The VCS SQL Configuration Wizard always sets Lanman attributes ADUpdateRequired and ADCriticalForOnline to 'TRUE', no matter what the user specifies.

Software fixes and enhancements in 5.1

This section describes the software fixes and enhancements in 5.1.

Veritas Storage Foundation

Table 1-25 describes the issues that were fixed for SFW in the 5.1 release:

Table 1-25 Fixed issues for Storage Foundation for Windows

Incident number	Description
342776	Restoring Exchange subcomponent that spans more than one volume is not supported.
511754	The <code>vxsnap restore</code> command fails when using the <code>-a</code> option to dismount volumes.
621856	The Quick Recovery Wizard does not update the screen that shows available disks for snapshot volumes while the wizard is running.
630138	Scheduled snapshots fail if volumes have the same name.
649092	The <code>vxsnap prepare</code> command cannot accept more than one hard disk per volume.
796211	For Exchange Server 2007 environments, manually dismount Exchange database stores before doing the VSS Restore.
818798	VSS Restore Wizard may not list the Quick Recovery snapshot XML file required to restore a snapshot set.
836802	Support for VSS snapshots.
839241	CLI command, <code>vxsnap prepare</code> , does not create snapshot mirrors in a stripe layout.
841623	Some registry entries created by the Quick Recovery Wizard remain after the schedule is deleted using the VEA console.
843076	The Quick Recovery Wizard may return an SFW discovery error if run after failover to another cluster node.
845637	MPIO parameters are not persistent after rebooting.
848908	The Quick Recovery Wizard fails to disable the settings for disk assignment once mirror preparation is complete.
850332	After upgrading 64-bit systems to SFW HA 5.1, the Vxbridge service fails to register.
862074	The DSM Balanced Path load balancing policy becomes unusable after a system reboot.

Table 1-25 Fixed issues for Storage Foundation for Windows (*continued*)

Incident number	Description
866516	The Quick Recovery Wizard is unable to discover a SQL instance on a system if the system is running a default SQL instance that is part of an MSCS cluster.
884205	Memory leaks occur during VSS snapshot operations.
915091, 915208	Extra spaces are inserted in Rule Manager alert topics.
1023357	VVR performance counters are not displayed in Ops Mgr 2007.
1145176	CLI support for Logical Disk Manager and Microsoft Disk Management.
1163778	VEA GUI does not enforce limits for task throttling.
1194685	SCSI settings for MSCS.
1215141	Storage Agent abnormally terminates when Capacity Monitoring is enabled.
1219357	Snapshot of SFW volume may fail when Microsoft Disk Management Disk Group exists on system.
1219391	Powering off or disconnecting DMP paths of the active node in a cluster environment does not result in failover of VMDG resources.
1219755	Cluster disk groups cannot be imported after system reboot.
1227740	Diskpart does not display dynamic volumes as Readonly
1598933	Incorrect CHAP status of iSCSI initiator displayed on VEA GUI.

Veritas Cluster Server

[Table 1-26](#) describes the issues that were fixed in the 5.1 release.

Table 1-26 Fixed issues for Veritas Cluster Server 5.1

Incident number	Description
493266	Lanman resources fail to come online if multiple Lanman resources depend on the same IP resource.
506454	VCW configures the cluster with both upper and lower case of the same system name

Table 1-26 Fixed issues for Veritas Cluster Server 5.1 (*continued*)

Incident number	Description
704021	With the Disaster Recovery wizard, storage cloning does not complete if the disks that are on the non-shared bus are selected
837702	The Fire Drill Wizard does not delete the DCO log volume when deleting a fire drill configuration.
843076	The Fire Drill Wizard may give an SFW discovery error if the replication service group has been switched between systems on the secondary site.
855170	With the Disaster Recovery wizard, Secondary RVG fails if you specify the same name for the Primary and Secondary RLINK.
864671	A user in a user group does not receive Cluster Administrator rights.
893550	With the Disaster Recovery wizard, storage cloning may time out on a large mirrored volume and fail to create any subsequent volumes.
894979	Cannot use the same NIC resource to configure Notifier and Web Console using VCW.
	Concurrency violation with online firm dependencies

Veritas Volume Replicator

[Table 1-27](#) describes the issues that were fixed in the 5.1 release.

Table 1-27 Fixed issues for Veritas Volume Replicator

Incident number	Description
1022623	The <code>vxprint</code> command output is not correct
1067545	Secondary going into Activating state on a cluster setup
1074533	System crash due to <code>vxio.sys</code>
1086439	The <code>vxedit</code> command does not work if <code>diskgroup</code> is not specified
1091010	VVR-Vxrsync with configuration file fails to synchronize secondary
1091064	VRAS should print version number of target host whenever an error message “version mismatch” is displayed
1107083	RVG resource properties show garbage values for RLINK attribute on a VVR-MSCS setup

Table 1-27 Fixed issues for Veritas Volume Replicator (*continued*)

Incident number	Description
1109346	Prevent flooding of system Event Viewer with message, "Readback memory pool request failed for RLINK. Readback pool size should be increased."
1123805	Memory leak in HA Server
1240812	Multiple periodic RLINK disconnects seen, typically 30 or less.
1243208	During synchronized snapshots and snapbacks, Secondary RLINK gets disconnected and connected multiple times.
1262343	Creation of RDS fails on the Primary with error "The configuration server may be busy or down."

Documentation changes

The information in this section updates information provided in the product documentation for Veritas Storage Foundation 5.1 Service Pack 2 for Windows and Veritas Storage Foundation HA 5.1 Service Pack 2 for Windows.

Veritas Storage Foundation for Administrator's Guide

This refers to Chapter 14, *Microsoft Clustering Support* in the guide This chapter contains a note in the section *Create a dynamic mirrored quorum resource* on page 769. The note appears as:

"If you are planning to create a dynamic mirrored quorum for your Volume Manager Disk (VMDG) resource, then make your ClusSvc resource dependent on the VxBridge service. Refer to Microsoft documentation for details on creating resource dependencies. This dependency is required only in cases when you will reboot all the cluster nodes at the same time."

The above note is incorrect.

The correct text for this note should be: "If you are planning to configure a dynamic mirrored volume of Volume Manager Disk (VMDG) resource as a Quorum, then make your 'Clusvc' service dependent on the 'VxBridge' service. This dependency is required only in cases when you will reboot all the cluster nodes at the same time."

This note is also documented in the following guides:

- Veritas Storage Foundation and High Availability Solutions Microsoft Clustering Solutions Guide for Microsoft SQL 2008 and 2008 R2
Refer to Chapter 6 *Implementing a dynamic mirrored quorum resource > Changing the quorum resource to a dynamic mirrored quorum resource* section on page 81.
- Veritas Storage Foundation and High Availability Solutions Solutions Guide
Refer to Chapter 17 *Deploying SFW with MSCS > Implementing a dynamic quorum resource* section on page 638.

Documentation

Storage Foundation for Windows documentation is included on the product software discs for Veritas Storage Foundation and High Availability Solutions 5.1 SP2 for Windows in Adobe Portable Document Format (PDF). Explore the \Docs directory of the software disc and double-click the file name to view a document.

Note: The information in the Release Notes supersedes the information provided in the product documents. You can download the latest version of this document from the Symantec Support website.

[Table 1-28](#) displays the Veritas Storage Foundation and High Availability Solutions documentation set.

Table 1-28 Veritas Storage Foundation and High Availability Solutions

Title	File Name
<i>Veritas Storage Foundation and High Availability Solutions Getting Started Guide</i>	SFWHA_GettingStarted.pdf
<i>Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide</i>	SFWHA_InstallUpgrade.pdf
<i>Veritas Storage Foundation and High Availability Solutions Release Notes</i>	SFWHA_ReleaseNotes.pdf
<i>Veritas Storage Foundation 5.1 for Windows SP2 WinLogo Certification Readme File</i>	SFW_HA_WinLogo.pdf
<i>Veritas Storage Foundation and High Availability Solutions Solutions Guide</i>	SFW_Solutions.pdf

Table 1-28 Veritas Storage Foundation and High Availability Solutions
(continued)

Title	File Name
<i>Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL 2000 and 2005</i>	SFW_HA_DR_SQL_Solutions.pdf
<i>Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL 2008</i>	SFW_HA_DR_SQL2008_Solutions.pdf
<i>Veritas Storage Foundation and High Availability Solutions Quick Recovery Solutions Guide for Microsoft SQL 2008</i>	SFW_QR_SQL2008_Solutions.pdf
<i>Veritas Storage Foundation and High Availability Solutions Microsoft Clustering Solutions Guide for Microsoft SQL 2008</i>	SFW_MSCS_SQL2008_Solutions.pdf
<i>Veritas Storage Foundation and High Availability Solutions Quick Recovery and Microsoft Clustering Solutions Guide for Microsoft SQL</i>	SFW_QR_MSCS_SQL_Solutions.pdf
<i>Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange 2003</i>	SFW_HA_DR_Exch2003_Solutions.pdf
<i>Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange 2007</i>	SFW_HA_DR_Exch2007_Solutions.pdf
<i>Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange 2010</i>	SFW_HA_DR_Exch2010_Solutions.pdf
<i>Veritas Storage Foundation and High Availability Solutions Quick Recovery and Microsoft Clustering Solutions Guide for Microsoft Exchange</i>	SFW_QR_MSCS_Exch_Solutions.pdf

Table 1-28 Veritas Storage Foundation and High Availability Solutions
(continued)

Title	File Name
<i>Veritas Storage Foundation and High Availability Solutions Quick Recovery Solutions Guide for Microsoft Exchange 2010</i>	SFW_QR_Exch2010_Solutions.pdf
<i>Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Enterprise Vault</i>	SFW_HA_DR_EV_Solutions.pdf
<i>Veritas Storage Foundation Quick Recovery Solutions Guide for Enterprise Vault</i>	SFW_QR_EV_Solutions.pdf
<i>Veritas Storage Foundation Quick Recovery Solutions Guide for Microsoft Office SharePoint Server 2007</i>	SFW_QR_SharePoint_Solutions.pdf
<i>Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SharePoint Server 2003 and 2007</i>	SFW_HA_DR_SharePoint_Solutions.pdf
<i>Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SharePoint Server 2010</i>	SFW_HA_DR_SharePoint2010_Solutions.pdf
<i>Veritas Storage Foundation and High Availability Solutions Management Pack Guide for Microsoft System Center Operations Manager 2007</i>	SFW_VVR_OpsMgr2007.pdf
<i>Veritas Storage Foundation and High Availability Solutions Management Pack Guide for Microsoft Operations Manager 2005</i>	SFW_VCS_MOM_2005.pdf

[Table 1-29](#) displays the Symantec Product Authentication Service documentation set.

Table 1-29 Symantec Product Authentication Service

Title	File name
<i>Symantec Product Authentication Service Administrator's Guide</i>	SPAS_AT_Admin.pdf

Table 1-29 Symantec Product Authentication Service (*continued*)

Title	File name
<i>Symantec Product Authentication Service Release Notes</i>	SPAS_AT_ReleaseNotes.pdf
<i>Veritas Storage Foundation and High Availability Solutions Quick Start Guide for Symantec Product Authentication Service</i>	SPAS_QuickStart.pdf

[Table 1-30](#) displays the Veritas Storage Foundation documentation set.

Table 1-30 Veritas Storage Foundation

Title	File name
<i>Veritas Storage Foundation Administrator's Guide</i>	SFW_Admin.pdf

[Table 1-31](#) displays the Veritas Volume Replicator documentation set.

Table 1-31 Veritas Volume Replicator

Title	File name
<i>Veritas Storage Foundation Volume Replicator Administrator's Guide</i>	VVR_Admin.pdf
<i>Veritas Volume Replicator Advisor User's Guide</i>	VVR_Advisor.pdf

[Table 1-32](#) displays the Veritas Cluster Server documentation set.

Table 1-32 Veritas Cluster Server

Title	File name
<i>Veritas Cluster Server Administrator's Guide</i>	VCS_Admin.pdf
<i>Veritas Cluster Server Agent Developer's Guide</i>	VCS_AgentDev.pdf
<i>Veritas Cluster Server Bundled Agents Reference Guide</i>	VCS_BundledAgents.pdf
<i>Veritas Cluster Server Agent for Microsoft Exchange 2003 Configuration Guide</i>	VCS_Exch_Agent.pdf

Table 1-32 Veritas Cluster Server (continued)

Title	File name
<i>Veritas Cluster Server Database Agent for Oracle Configuration Guide</i>	VCS_Oracle_Agent.pdf
<i>Veritas Cluster Server Database Agent for Microsoft SQL Configuration Guide</i>	VCS_SQL_Agent.pdf
<i>Veritas Cluster Server Application Note: HA and Disaster Recovery for BlackBerry Enterprise Server</i>	Recovery for BlackBerry Enterprise Server VCS_AppNote_BlackBerry.pdf
<i>Veritas Cluster Server Agent for EMC SRDF Configuration Guide</i>	VCS_SRDF_Agent.pdf
<i>Veritas Cluster Server Agent for EMC SRDF/Star Installation and Configuration Guide</i>	VCS_SRDFStar_Agent.pdf
<i>Veritas Cluster Server Agent for EMC MirrorView Installation and Configuration Guide</i>	VCS_MirrorView_Agent.pdf
<i>Veritas Cluster Server Agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access Installation and Configuration Guide</i>	VCS_TrueCopy_Agent.pdf
<i>Veritas Cluster Server Agent for IBM Metro Mirror Installation and Configuration Guide</i>	VCS_MetroMirror_Agent.pdf
<i>Veritas Cluster Server Management Pack Guide for Microsoft System Center Operations Manager 2007</i>	VCS_MgmtPack_SCOM2007.pdf
<i>Veritas Cluster Server Application Management Pack Guide for Microsoft System Center Operations Manager 2007</i>	VCS_AppMgmtPack_SCOM2007.pdf
<i>Veritas Cluster Server Library Management Pack Guide for Microsoft System Center Operations Manager 2007</i>	VCS_LibraryMgmtPack_SCOM2007.pdf

[Table 1-33](#) displays the legal notices for the documentation set.

Table 1-33 Third-party Legal Notices

Title	File name
<i>Third-party Legal Notices</i>	Legal_Notices.pdf

PDF copies of the product guides are also available on the Symantec Support website at:

<http://www.symantec.com/business/support/index.jsp>

Documentation feedback

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions to sfwha_docs@symantec.com. Include the title and part number of the document (located in the lower left corner of the title page), and chapter and section titles of the text on which you are reporting. Our goal is to ensure customer satisfaction by providing effective, quality documentation.

For assistance with topics other than documentation, visit:

<http://www.symantec.com/business/support/index.jsp>

Acronyms

The following table defines the acronyms used in the SP1 release notes.

Table 1-34 Acronym list

Acronym	Definition
ALUA	Asymmetric Logical Unit Access
AP	Application Pack
BES	BlackBerry Enterprise Server
COW	Copy on write
DCM	Data change map
DMP	Dynamic MultiPathing
DR	Disaster Recovery
GAB	Global Atomic Broadcast
HAD	High Availability Daemon
HBA	Host bus adapters
HCL	Hardware compatibility list
IIS	Internet Information Services

Table 1-34 Acronym list (*continued*)

Acronym	Definition
MOM	Microsoft Operations Manager
MPIO	Multipath I/O
MSCS	Microsoft Cluster Services
MSDE	Microsoft Database Engine
MSMQ	Microsoft Message Queuing
NPP	Non-paged pool
RDP	Remote Desktop Protocol
RVG	Replication Volume Group
SCC	Solutions Configuration Center
SCL	Software compatibility list
SCOM	Systems Center Operations Manager
SFW	Storage Foundation for Windows
SFW HA	Storage Foundation for Windows High Availability
SP	Service Pack
TCP	Transmission Control Protocol
VCS	Veritas Cluster Server
VEA	Veritas Enterprise Administrator
VVR	Veritas Volume Replicator
VHD	Virtual Hard Drive
VAM	Veritas Application Manager
VCW	VCS ClusterConfigurationWizard
UDP	User Datagram Protocol

