

Veritas Storage Foundation™ and High Availability Solutions Release Notes

Windows Server 2003, Windows Server 2008

5.1



Veritas Storage Foundation and High Availability Solutions Release Notes

Copyright © 2008 Symantec Corporation. All rights reserved.

Storage Foundation 5.1 for Windows HA

Document Version: 5.1.2

Symantec, the Symantec logo, Veritas, and Veritas Storage Foundation 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.

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.

THIS 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” and “commercial computer software documentation” as defined in FAR Sections 12.212 and DFARS Section 227.7202.

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

Third-party legal notices

Certain third-party software may be distributed, embedded, or bundled with this Symantec product or recommended for use in connection with its installation and use. Such third-party software is separately licensed by its copyright holder. For complete third-party licensing information for the product or products represented in this publication, see the Third-Party Licensing section in the *Release Notes*.

Licensing and registration

Storage Foundation for Windows and Storage Foundation HA for Windows are licensed products. See the *Storage Foundation and High Availability Solutions for Windows, Installation and Upgrade Guide* for license installation instructions.

Technical support

For technical assistance, visit <http://www.symantec.com/business/support/index.jsp> and select phone or email support. This site also provides access to resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and the Veritas customer email notification service. Use the Knowledge Base Search feature to access additional product information, including current and past releases of product documentation.

Contents

Introduction	12
New features and changes in this release	13
General support	13
Windows Server 2008 support	13
Windows Server 2008 Server Core support	13
Client support on Windows Vista	13
Microsoft Operations Manager (MOM)	13
New application support	13
VCS Management Console 5.1	14
Enhancements to the Solutions Configuration Center	14
Enhancements to the Solutions wizards	15
Installation	15
Configuration Checker enhancements	15
Veritas Storage Foundation	15
Storage Management	15
SmartMove	16
VSS snapshot wizard enhancements	16
Microsoft Exchange Server 2007	16
Microsoft clustering	16
iSCSI	16
Dynamic Multi-pathing (Veritas DMP)	17
Veritas Cluster Server	18
Microsoft Exchange Server 2007 support	18
Support for Microsoft Sharepoint Server 2007 in a disaster recovery configuration	18
Support for networks using DNS scavenging	18
VCW support for configuring VCS LLT over UDP	18
Support for Oracle on 64-bit Windows servers	18
EMC SRDF/Star enterprise agent	18
BlackBerry Enterprise Server support	18
Veritas Volume Replicator	19
VVR support for TCP Multi-Connection	19
VSS snapshot wizard enhancement	19
Application support	20

Requirements	22
Operating system requirements	22
SFW and SFW HA software for servers	22
SFW and SFW HA software for clients	23
Hardware requirements	23
Disk space	23
Memory	24
System processor	24
Storage device compatibility	24
Display	25
General requirements	25
Supported browsers	25
Anti-spyware, firewall and port availability requirements	25
Remote systems	25
Driver signing options	25
Network access	26
Single instance of SFW	26
VMWare ESX server support	26
No longer supported	27
Symantec License Inventory Management (SLIM)	27
Windows Server 2000	27
Language Pack for Japanese	27
Dynamic Multipathing Array Support Libraries	27
Dependent service groups with the DR wizard	27
NetBackup agents and wizards	27
Installation notes	28
Software limitations	29
Installation or upgrade	29
License management	30
SFW and SFW HA installation CLI does not support adding license keys after installation	30
Veritas Storage Foundation	30
Requirements for iSCSI or VDS-based functionality	30
Limitations on 64-bit systems	31
Limitations of SFW support for Dynamic Multi-pathing (DMP)	31
Limitations of SFW with Exchange and SQL	31
Other issues	32
Veritas Cluster Server	35
Windows Safe Mode boot options not supported (1234512)	35
Service group offline alerts remain unresolved on a MOM 2005 server (1217601)	35

File shares on Windows Server 2008 are not accessible using the virtual IP address (1214494) 35

Security issue when using the Cluster Manager (Java GUI) and default cluster admin credentials (1188218) 35

VCWSilent does not support LLT over UDP configuration 36

VCW does not support configuring broadcasting for UDP 36

For LLT over UDP, VCW does not support the Low Priority option for a network adapter (1260629) 36

Solutions wizard support in a 64-bit VMWare environment 36

Cluster Manager (Java Console) 36

All servers in a cluster must run the same operating system 36

Service group dependency limitations 37

Volume Shadow Copy Service is not supported 37

Incorrect updates to path and name of types.cf with spaces 37

Lock by third-party monitoring tools on shared volumes 37

VCS lock on shared volumes during Exchange recovery 37

Schedule backups on online nodes 38

Cannot rename nodes with Veritas Security Services 38

Undocumented commands and command options 38

Undefined behavior when using VCS wizards for modifying incorrectly configured service groups (253007) 38

MirrorView agent resource faults when agent is killed (508066) 39

Exchange virtual servers are shown as non-reachable in the Exchange Service Manager (333108) 39

Cluster address for global cluster requires resolved virtual IP 39

Systems in a cluster must have same system locale setting 39

Virtual fire drill not supported in Windows environments 39

Disaster Recovery Configuration Wizard 39

Veritas Volume Replicator 41

Resize Volume and Autogrow not supported in Synchronous mode (103613) 41

Expand volume not supported if RVG is in DCM logging mode ... 41

Solutions Configuration Center 41

The Solutions Configuration Center and its wizards have signature verification disabled by default to speed startup time 41

Quick Recovery wizard displays only one XML file path for all databases, even if different file paths have been configured earlier 42

Disaster Recovery, Fire Drill and Quick Recovery wizards fail to load unless the user has administrative privilege on the system 42

Known issues	43
Installation, upgrades, and licensing	43
Disk time out value not reset during SFW uninstall (1297012) ...	43
SFW HA installation may fail on x64 systems (635814)	43
After upgrade to SFW HA 5.1 on 64-bit system, the Symantec Product Authentication Service menu does not work (1251282)	44
Uninstalling after upgrade to SFW HA 5.1 does not delete all files from the system (1263431)	44
Log on to remote nodes before installation (106013)	44
Software installs registry keys with read-write permission for Power Users group (964870)	44
Internationalization issues	44
Timestamp in Veritas Cluster Management Console logs reflects Pacific Standard Time (PST) or Pacific Daylight Time (PDT) (847646)	45
Only U.S. ASCII characters are supported in file paths (862762, 860579, 860186)	45
The installation directory for the VRTSWebApp service must include only U.S. ASCII characters (864183)	45
Language preference in Veritas Enterprise Administrator (VEA) must be set to English (United States) or Japanese (Japan) (849497)	45
General issues	46
Troubleshooting errors (766137)	46
VMDg resource may not failover in a cluster environment (774442)	46
Symantec PBX installation proceeds even when reserved port is occupied (801671)	46
Veritas Storage Foundation	47
Storage management issues	47
Snapshot and Restore issues	47
Snapshot scheduling issues	52
Quick Recovery Configuration Wizard issues	56
VEA Console issues	57
Internationalization issues	59
Dynamic Multi-pathing (DMP) issues	60
Microsoft Systems Center Operations Manager 2007 (Ops Mgr 2007) issues	60
Other issues	61
Veritas Cluster Server	67
Symantec Endpoint Protection security policy may block the VCS Cluster Configuration Wizard (1315813)	67

- Reconfiguring the root broker multiple times may cause issues in a secure cluster (1260632) 67
- If the network adapters are unable to ping each other, the cluster nodes may not get GAB membership 68
- MountV resource takes time to offline on Windows 2008 systems (1189260, 1235123) 68
- File share service group may fail to come online on Windows 2008 systems (1204865) 69
- Saving large configuration results in very large file size for main.cf (616818) 69
- AutoStart may violate limits and prerequisites load policy 70
- Trigger not invoked in REMOTE_BUILD state 70
- Some alert messages do not display correctly (612268) 70
- Issues related to the VCS engine 71
- Issues related to Cluster Manager (Java Console) 71
- Service group dependency limitations 73
- Secure clusters 74
- Global service groups 75
- Fibre Channel adapters may require modified settings 76
- VCS with Microsoft Exchange Server 77
- VCS with Oracle 82
- VCS Hardware Replication Agent for EMC MirrorView 82
- Disaster Recovery Configuration Wizard 83
- Fire Drill Wizard 88
- Other issues 89
- Veritas Volume Replicator 95
 - General Issues 95
- Software fixes and enhancements 99
 - Veritas Storage Foundation 99
 - Veritas Cluster Server 101
 - Veritas Volume Replicator 101
- Documentation changes 103
 - Veritas Storage Foundation and High Availability Solution Quick Recovery and Microsoft Clustering Solutions Guide for Microsoft Exchange 103
 - Veritas Storage Foundation and High Availability Solutions Quick Recovery and Microsoft Clustering Solutions Guide for Microsoft SQL 103
 - Veritas Storage Foundation and High Availability Solutions, Solutions Guide 104

Veritas Storage Foundation and High Availability Solutions	
HA and Disaster Recovery Solutions Guide	
for Microsoft Exchange	104
Exchange pre-installation on first node (secondary site)	
(page 603)	104
Veritas Storage Foundation and High Availability Solutions	
HA and Disaster Recovery Solutions Guide	
for Microsoft Exchange 2007	105
Exchange pre-installation on first node (secondary site)	
(page 599)	105
Veritas Storage Foundation Administrator's Guide	105
Location of New Volume tool on the VEA GUI toolbar	
(page 59)	105
Setting up a dynamic boot and system volume on	
Windows Server 2008 (page 68)	105
Appearance of Snapshot Volume tab	
(page 95)	106
Appearance of Alerts tab	
(page 95)	106
Right-click computer icon to view all drive paths	
(page 157)	106
Right-click computer icon to destroy dynamic disk group	
(page 182)	106
Renaming a cluster disk group	
(page 185)	106
Veritas Storage Foundation Volume Replicator	
Administrator's Guide	107
Read-only access given to volumes under RVG	
when RVG is stopped (page 306)	107
Enhancements made for vxio logging	107
Enhancements done in VRAS logging	107
Miscellaneous logging enhancements	108
Veritas Cluster Server Administrator's Guide	108
Setting the checksum option (page 691)	108
Configuring BlackBerry Enterprise Server in a	
VCS environment (page 406)	108
Veritas Storage Foundation and High Availability Solutions	
Installation and Upgrade Guide	109
Upgrading an Exchange Server cluster (Chapter 5)	109
Documentation	110
Documentation feedback	112

Veritas Storage Foundation and High Availability Solutions Release Notes

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

Introduction

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

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

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

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

<http://www.symantec.com>

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

<http://entsupport.symantec.com/docs/303042>

For information about Microsoft certification for Veritas Storage Foundation (Windows Server 2003: Microsoft Certified For Windows Certification; Windows Server 2008: Certified for Windows Server 2008), see the SFW WinLogo Readme that is included with the SFW product documentation on the product media.

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

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

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>

This release also supports Veritas Cluster Server Management Console. Related Release Notes are located on the installation media for that product.

New features and changes in this release

The changes described below are introduced in Veritas Storage Foundation for Windows and Storage Foundation HA for Windows version 5.1.

General support

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

- 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://entsupport.symantec.com/docs/290657>.

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

Configuration Checker enhancements

The following are Configuration Checker enhancements:

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

Veritas Storage Foundation

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

New features and changes in this release

with Microsoft Disk Management and can manage the dynamic disk group created by it.

- 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, could have improved performance by using the SmartMove feature.

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 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

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.

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.

EMC SRDF/Star enterprise agent

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

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

In order 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, 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 at:

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

Supported applications include the following:

Microsoft Exchange Server

- Microsoft Exchange Server 2003: Standard Edition or Enterprise Edition (SP 2 required)

Note: Microsoft support for Exchange Server 2003 is limited to 32-bit versions of the Windows 2003 operating system.

- Microsoft Exchange Server 2007 (SP1 supported): Standard Edition and Enterprise Edition (Mailbox server role required for SFW HA)

Microsoft SQL Server

- Microsoft SQL Server 2000, 32-bit: Standard Edition or Enterprise Edition (SP4 required)
- Microsoft SQL Server 2000, 64-bit: Standard Edition or Enterprise Edition (SP4 required)
- Microsoft SQL Server 2005, 32-bit: Standard Edition or Enterprise Edition (SP1 or higher required, SP2 required for Windows Server 2008)
- Microsoft SQL Server 2005, 64-bit: Standard Edition or Enterprise Edition, supports x64 platforms (SP1 or higher required)

Oracle

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

Table 1-1 Supported 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)

Requirements

Review these product installation requirements before installing Storage Foundation 5.1 for Windows or Storage Foundation HA 5.1 for Windows.

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

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

Operating system requirements

SFW and SFW HA have client and server components that run on specific Windows operating systems.

The requirements for operating system support shown below supersede any different requirements that may be listed in the product documentation.

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

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

SFW and SFW HA software for servers

Your server must run one of the following operating systems:

- 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)
- Windows Server 2003 Web Edition: fully supports SFW and supports only file share for SFW HA (SP2 required)
- Windows Server 2003 x64 Editions (for AMD64 or Intel EM64T): Standard x64 Edition, Enterprise x64 Edition, or Datacenter x64 Edition
- Windows Server 2003 x64 Editions (for AMD64 or Intel EM64T): Standard x64 R2 Edition, Enterprise x64 R2 Edition, or Datacenter x64 R2 Edition
- 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

SFW and SFW HA software for clients

Your client must run one of the following operating systems:

- 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
- Windows Server 2003 x64 Editions (for AMD64 or Intel EM64T): Standard x64 Edition, Enterprise x64 Edition, or Datacenter x64 Edition
- Windows Server 2003 x64 Editions (for AMD64 or Intel EM64T): Standard x64 R2 Edition, Enterprise x64 R2 Edition, or Datacenter x64 R2 Edition
- 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 XP Professional (SP 2 or higher required)
- Windows Vista (32-bit) (SP1 supported): Business, Enterprise, and Ultimate editions
- Windows Vista (64-bit) (SP1 supported): Business, Enterprise, and Ultimate editions

Hardware requirements

Disk space

The following table estimates disk space requirements for product installation of Veritas Storage Foundation and HA Solutions 5.1.

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

For normal operation, all installations require an additional 50 MB of disk space.

Table 1-2 summarizes approximate disk space requirements for SFW and SFW HA on 32-bit and 64-bit systems.

Table 1-2 Disk space requirements

Installation options	Install directory or drive 32-bit/64-bit
SFW + all options + client components	1200 MB/1500 MB
SFW + all options	940 MB/1240
Client components	360 MB/380 MB
SFW HA + all options + client components	1770 MB/2160 MB
SFW HA + all options	1390 MB/2020 MB
Client components	530 MB/560 MB

Memory

- Minimum required: 1 GB of RAM

System processor

Processor requirements are as follows:

32-bit

- 800-megahertz (MHz) Pentium III-compatible or faster processor
- 1GHz or faster processor recommended

x64

- 1GHz AMD Opteron, AMD Athlon 64, Intel Xeon with Intel EM64T support, Intel Pentium IV with EM64T support processor or faster

Storage device compatibility

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

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

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

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

General requirements

Supported browsers

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

- Microsoft Internet Explorer 6.0.x, 7.0, or newer
- Firefox 1.5, 2.0, or newer

Veritas Cluster Server Management Console requires the Macromedia Flash Plugin v8.0 or 9.0.

Anti-spyware, firewall and port availability requirements

Before installing SFW or SFW HA, disable spyware monitoring and removal software. Ensure that your firewall settings allow access to ports used by SFW HA wizards and services. For a detailed list of services and ports used by SFW HA, refer to the appendix in the *Veritas Storage Foundation and High Availability Solutions for Windows Installation and Upgrade Guide*. For any updates on port requirements, see the Support TechNote:

<http://entsupport.symantec.com/docs/286714>

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.

Driver signing options

Depending on the installation options you select, some Symantec drivers may not be signed.

The product installer provides an installation option for Symantec Trusted Software Publisher Certificate.

When installing on systems running Windows Server 2003, if you do not select this option, you must set the Windows driver signing options to allow installation. On local systems, set the driver signing option to either Ignore or

Warn. On remote systems, set the option to Ignore so that the installation can proceed without user interaction.

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 HA Solutions for Windows Installation and Upgrade Guide*.

Network access

You must have network access to each remote system. SFW HA and SFW with the VVR option do not support Dynamic Host Configuration Protocol (DHCP); you must use a static IP address for replication and clustering.

Single instance of SFW

Only one instance of SFW 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 HA 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.

No longer supported

The following behavior has changed in this release.

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 (DR) wizard 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 an 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. See “[License management](#)” on page 30.
- If you are in need of the debug symbols for this release, contact Symantec Technical Support.
- For information about installing or upgrading to Veritas Storage Foundation and HA Solutions 5.1 and options, refer to the *Veritas Storage Foundation and HA Solutions for Windows 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 HA Solutions for Windows 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, with any installation options for version 5.1, such as VCS Agents or VVR
 - The Release Notes file is located on the SFW HA product media. Updated Release Notes can be found at <http://entsupport.symantec.com/docs/303042>.
 - 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.
- A post-installation step is required for 64-bit platforms running IIS 6.0. See “[Installation or upgrade](#)” on page 29.

Software limitations

The following limitations apply to Veritas Storage Foundation and High Availability Solutions 5.1 for Windows.

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

<http://entsupport.symantec.com/docs/303042>

Installation or upgrade

Installation or upgrade on a 64-bit platform requires post-installation step for environments running IIS 6.0

SFW 5.1 installs 32-bit .Net Framework 1.1 in silent mode on all platforms. Installation or upgrade on a 64-bit platform requires a post-installation step to enable both the 32-bit and 64-bit ASP.NET environments to run in IIS 6.0.

If installing in interactive mode on a 64-bit platform, .Net Framework 1.1 will pop up a message about a known incompatibility with Internet Information Services (IIS) on this platform.

If IIS is required for your application environment, ensure that when installing or upgrading to 5.1 on a 64-bit platform, you follow the Microsoft instructions to run the commands required after installation is complete. Refer to the following Microsoft KB article on support.microsoft.com for more information:

KB894435, "How to switch between the 32-bit versions of ASP.NET 1.1 and the 64-bit version of ASP.NET 2.0 on a 64-bit version of Windows"

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

SFW and SFW HA installation CLI does not support adding license keys after installation

SFW and SFW HA installation can be performed using either a product installer or a command line utility. Both 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 utility does not support updating license keys after installation.

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

- 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>`

Veritas Storage Foundation

This section covers limitations specific to Storage Foundation functionality.

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 `CMPNENTS\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

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 a 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 2003 server issue. Refer to Microsoft case 100-42023 for additional information.

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 because third-party MPIO DSMs may not implement a common method in the Microsoft MPIO framework for getting or setting load balancing policies. In addition, there is no clear definition in the Microsoft MPIO framework to define parameters for setting load balance policies through a common method. This is a known Microsoft problem.

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

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 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 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 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. Therefore, 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>sc). Continue through the wizard until the Synchronizing Schedules panel shows that synchronization between cluster nodes is complete. Click Finish to exit the wizard.

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 will not be able 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 the Cluster Manager (Java GUI) and default cluster admin credentials (1188218)

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

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

VCWSilent does not support LLT over UDP configuration

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

VCW does not support configuring broadcasting for UDP

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

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

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

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)

Java Console for VCS 5.0 or higher is required

Cluster Manager (Java Console) from previous VCS versions cannot be used to manage VCS 5.0 or later 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

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 are 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 -cmdtocf` and `hacf -cftocmd` truncates the path of the `types.cf` file and updates the `main.cf` file with the truncated path.

Lock by third-party monitoring tools on shared volumes

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

Workaround: Symantec recommends adding a custom resource as the topmost parent for an affected service group. Use the custom resource to manage onlineing, 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 above 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.

Cannot rename nodes with Veritas Security Services

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

Undocumented commands and command options

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

Undefined behavior when using VCS wizards for modifying incorrectly configured service groups (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 prior to the MirrorView Agent being killed, or crashing.

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

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

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

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

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.

Disaster Recovery Configuration Wizard

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 DR wizard already exists on the secondary site, the DR Wizard does not validate the configuration or add missing resources.

Software limitations

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

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 in .Net 2.0 SP1, which is deployed with SFW HA 5.1. The fix allows you to disable the signature verification through use of a configuration file setting. Information on the fix is provided in the following Microsoft article:

<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."

Known issues

The following known issues exist in Veritas Storage Foundation 5.1 for Windows and Veritas Storage Foundation HA 5.1 for Windows.

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

<http://entsupport.symantec.com/docs/303042>

Installation, upgrades, and licensing

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

Disk time out value not reset during SFW uninstall (1297012)

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 time out value in the Windows registry is not reset to its original value.

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.

SFW HA installation may fail on x64 systems (635814)

SFW HA installation may intermittently fail on one or more systems. This happens on x64 systems only.

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  
MSI (s) (A8:5C) [17:13:13:455]: Product: SFW -- Internal Error  
2356. Data1.cab
```

Workaround: From the Windows Add/Remove programs, launch the SFW HA installer again and choose the Repair option. If the installation does not complete in Repair mode, uninstall SFW HA and reinstall it.

After upgrade to SFW HA 5.1 on 64-bit system, the Symantec Product Authentication Service menu does not work (1251282)

After upgrading to SFW HA 5.1 on a 64-bit system, if you select Symantec Product Authentication Service from the Start menu, nothing happens. The administration console is not displayed.

Workaround: Make sure that Java 1.4.2 or above is installed on your system and is pointed to in the PATH variable. For more information, refer to the Java web site.

Uninstalling after upgrade to SFW HA 5.1 does not delete all files from the system (1263431)

If you upgrade to SFW HA 5.1, and then uninstall, documentation PDFs remain on the system in the `Veritas\Docs` directory.

Workaround: Delete the directory manually.

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.

Software installs 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 <http://www.microsoft.com>.

Internationalization issues

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.

The installation directory for the VRTSWebApp service must include only U.S. ASCII characters (864183)

Non-ASCII characters in the installation path of the VRTSWebApp service causes it to fail.

Workaround: Use U.S. ASCII characters only when specifying the installation path for the VRTSWebApp service.

Language preference in Veritas Enterprise Administrator (VEA) must be set to English (United States) or Japanese (Japan) (849497)

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

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.

Veritas Storage Foundation

This section provides information on known Storage Foundation issues.

Storage management issues

Converting style of disk in Microsoft Disk Management Disk Group fails (1202636)

On Windows 2008, converting the style of disk that belongs to a Microsoft Disk Management Disk Group fails. In addition, the message that appears states the error incorrectly.

Workaround: Convert the style of disk using Microsoft Disk Management. In SFW, perform a rescan operation to correctly display the style of disk in the VEA GUI.

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

On Windows 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. The `vx dg init` CLI command creates a dynamic disk group type depending on the version of Windows running on the system.

Snapshot and Restore issues

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 will fail.

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

- Eventviewer 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.

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, 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.

The vxsnap start and vxsnap create commands fail in an environment with two virtual Exchange servers (508893)

The `vxsnap start` and `vxsnap create` CLI commands fail in an environment with two virtual Exchange servers when both have a storage group with the same name.

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.

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 snap shot 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

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 is providing patches for Windows 2003 that address this change. 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 impacted 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 impacts the Snapshot Scheduler.

- On the first day of DST, any snapshots scheduled during 2:00am - 2:59am are taken during 3:00am - 3:59am DST.
- On the last day of DST, any snapshots scheduled during 1:00am - 1:59am are taken 1:00am - 1:59am Standard Time.
- If during 1:00am - 1:59am 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 1:30am on the last day of DST, then any snapshots scheduled during 1:00am - 1:29am 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 will 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 will start working with the next scheduled snapshot operation. If the mirror preparation operation was skipped, it will be 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 vxvm service is restarted on the original node. However, any existing schedules will 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.

Synchronization of missing schedule entries sometimes fails in multi-node clustered environment (1361969)

While creating missing schedule entries on passive cluster nodes, the Quick Recovery Configuration wizard sometimes fails to create the following Windows Registry entries:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\VxSvc\CurrentVersion  
\Schedules\<Schedule-GUID>
```

Name-Value pairs:

- OperationTime (type:DWORD)
- LastOperation (type:DWORD)

This can occur when PostScript and PreScript entries are different across nodes and require a synchronization.

Since the schedule creation time related entries are missing, the wizard displays the following error message:

```
"Wizard can not perform schedule synchronization because  
inconsistency is detected in schedule configuration.
```

```
Either the schedules were created using previous version  
of Quick Recovery Configuration Wizard or some entries in  
schedule configuration are missing."
```

Workaround: To recover from this situation, you can do either of the following

- Create the specified registry entries manually on all nodes. Ensure that the value is the same on all nodes.
- Recreate all the schedules by deleting all of them and adding them again. In order to preserve the schedule details, you could save them as a template before deleting and later import the template while adding the schedules.

In a multi-node cluster environment, QR wizard sometimes fails to create schedules on passive nodes (1363774)

When the Quick Recovery wizard is launched for the first time after the Scheduler service is restarted, it sometimes fails to create some schedule registry keys on the passive nodes of the cluster. This only occurs the first time the wizard is launched after the Scheduler service is restarted.

On the QR wizard Implementation panel, the following error message is shown:

```
"Failed to either Create, Modify or Delete the schedules  
on the following nodes: <PassiveNode Name/IP>"
```

The following registry key on the passive nodes contains fewer schedule keys than the active node:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\VxSvc\CurrentVersion\Schedules\)
```

In the "SchedService0.log" log file the following trace appears:

```
"ChildSocketThread, MultiByteToWideChar failed with error: 122"
```

Workaround

Run the QR wizard again.

The wizard will synchronize the schedules across nodes, thus creating the missing schedule keys on the passive nodes.

Note: If the wizard displays an error message that it cannot perform schedule synchronization, see incident 1361969 above in the release notes for the workaround.

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 allows you to 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

VEA GUI fails to login to iSCSI target (1287942)

On a Windows 2008 system, the operation to log into 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 login 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 login of an iSCSI target, you can use the Microsoft iSCSI Initiator Applet to successfully perform the operation.

VEA GUI does not display a new iSCSI disk as a part of the Enclosure object (1362435)

In Windows 2008, when a new iSCSI disk is presented, the VEA GUI does not display the disk as a part of the Enclosure object.

VEA GUI incorrectly displays a new iSCSI disk as online (1362395)

In Windows 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.

VEA GUI does not display a new iSCSI disk as a part of the iSCSI initiator object (1362434)

When a new iSCSI disk is presented, the VEA GUI does not display the disk as a part of the iSCSI initiator object.

Workaround: Restart the Storage Agent service to display the new iSCSI disk as a part of the iSCSI initiator object.

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 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 actually 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.

Connecting VEA to localhost fails with message of object not found (644467)

When connecting VEA to localhost fails, the Veritas Storage Agent service is not able to complete the connection.

Workaround: The workaround to this issue is to restart the Veritas Storage Agent service before connecting VEA to localhost. If connecting to localhost still fails after starting the service, reboot the system and restart SFW.

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 enables the display of double-byte characters.

Windows 2003 or Windows XP:

- 1 Right click on the desktop.
- 2 Select Properties > Appearances 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.

Windows 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 a reverse lookup zone exists in the DNS.

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 vxdumpadm (1287130)

DMP DSM operations are not currently supported by the vxdumpadm setattr dsm command. The vxdumpadm setattr dsm command is not available in this release.

Workaround: Use the vxdumpadm setattr array command to manage DMP DSMs.

Microsoft Systems Center Operations Manager 2007 (Ops Mgr 2007) issues**Performance Graph for MPIO does not display data (914312)**

When monitoring the performance activity of a volume with the Performance Graph of Ops Mgr 2007, no data is displayed. As such, the MPIO rule that gathers MPIO data, "Get MPIO Path Performance Data", should not be enabled.

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 Ops Mgr 2007 when the last RVG is deleted or when an RVG is moved. This is due to Ops Mgr 2007 being unable to recognize the empty collection of item sent by discovery workflows.

Other issues

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 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 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 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 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.

Errors logged in application log when dynamic disk group is destroyed (930283)

When a dynamic disk group is destroyed, Microsoft VDS logs error messages in the application log. These error messages are generated erroneously and indicate no error with the destroy disk group operation.

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.

SFW dynamic volumes are not displayed in the Microsoft Disk Management GUI or by the diskpart utility (1178919)

On Windows Server 2008, SFW dynamic volumes are not displayed in the Microsoft Disk Management GUI or by the diskpart utility. VDS limits the number of providers that it works with and this results in VDS not working with the SFW VDS provider plugin to display the SFW dynamic volumes.

Diskpart does not display dynamic volumes as Readonly (930308)

Using Diskpart to display information about a Readonly dynamic volume does not display the volume as Readonly.

Workaround: Use Diskpart to perform a rescan operation or restart the VDS service to synchronize the dynamic volume with VDS properties and enable Diskpart to display the dynamic volume information correctly.

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 in to SFW as a member of the Windows Administrator group requires additional credentials (1233589)

On Windows Server 2008, by design, logging in 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.

When capacity monitoring threshold is exceeded no automatic email alert is sent (1184088)

The SFW capacity monitoring feature does not automatically send an email alert when the capacity threshold is reached.

Workaround: To send an automatic email alert when the capacity threshold is reached, use the Action Agent Rule Manager to set up a new rule to send the email alert. Specify the alert topics, "Volume capacity reached error condition" and "Volume capacity reached warning condition" in the rule.

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 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 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 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 will be 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 console may appear as an entry labeled as "NoName". These labels are not harmful and refer to a task that is running.

Upgrading a basic disk to a dynamic disk causes an error message (799237)

An E_NOINTERFACE error message is recorded in the system event log when a basic disk is upgraded to a dynamic disk. This condition does not affect SFW or the operation of the server. This issue has been reported to Microsoft.

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 are unable to 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.

Known issues

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.

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

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

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

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

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

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

Method 1:

- 1 Reboot the cluster nodes that do not have GAB membership.
- 2 Verify the GAB operation in the cluster. Type the following on the command prompt:

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

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

Method 2:

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

```
C:\>net stop llt
```
- 2 Delete the cluster using VCW.
- 3 Ensure that the network adapters are able to ping each other and then re-create the cluster using VCW.

MountV resource takes time to offline on Windows 2008 systems (1189260, 1235123)

The MountV resource may take considerable amount of time to go offline on Windows 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 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 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.

Workaround

- 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 impact 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, and the other group, G1, is offline when VCS is started on the node.
- The offline group is probed before the online group is probed.

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

Workaround

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

Trigger not invoked in REMOTE_BUILD state

In some situations, VCS does not invoke the 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

Engine may hang in LEAVING state

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

Workaround

Issue the command `hastop -local -force`.

Timing issues with AutoStart policy

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

Issues related to Cluster Manager (Java Console)

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

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

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

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

wizard will fail to validate the user credentials even if the logged in user is a cluster administrator. The following error is displayed:

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

Workaround

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

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. Typically, this may happen with Japanese locales.

Workaround

Copy the bmc and bmcmap files to the location specified in [Table 1-3](#):

Table 1-3 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.
(For Japanese) D:\Program Files\Veritas\messages\ja Where, D: is the drive on which VCS is installed.	%VCS_HOME%\messages\ja Where, %VCS_HOME% is the default installation directory for VCS, typically C:\Program Files\Veritas\Cluster Server.

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 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

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

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

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

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

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

Workaround:

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

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

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

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

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

The state should display as RUNNING.

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

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

Workaround

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

Global service groups

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

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

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

Workaround

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

Group does not go online on AutoStart node

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

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

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 the host bus adapter has the proper drivers installed. Modify the Topology, ResetFF, and ResetTPRLO drive settings in the Emulex adapter BIOS settings, as instructed below.

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

Note: When using EMC storage, you must make additional changes to Emulex host bus adapter settings. See TechNote 245039 on this topic at <http://entsupport.symantec.com>.

QLogic Fibre Channel adapters

When configured over QLogic Fibre Channel host bus adapters, the DiskReservation agent requires the Target Reset option of the adapter to be

enabled. By default, this adapter option is disabled, causing the agent to hang during failover.

Workaround

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

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

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:

- 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\MSE
xchangeIS\VirusScan
- 5 In the right pane, double-click **Enabled**.

- 6 Click **Decimal**, enter **0**, and then click **OK**.
- 7 On the File menu, click **Exit** to quit Registry Editor.

Error while performing Exchange post-installation steps (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.

Workaround

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

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

```
C:\>net start had
```
- 2 Verify that HAD is running. Type the following at the command prompt:

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

The state should display as RUNNING.
- 3 Click **Retry** on the Exchange Setup Wizard panel and proceed with the Exchange post-installation steps.

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.

Workaround

Perform the following steps:

- 1 Take all the ExchService resources in the Exchange 2003 service group offline.
- 2 From the Services MMC snap-in, restart the WMI service.
- 3 Run VCW to perform the required tasks.
- 4 Bring the ExchService resources online.

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

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

```
Server name mismatch Server: EVS1
```

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

You can ignore this error and proceed with the analysis.

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

```
HKLM\SOFTWARE\VERITAS\VCS\EXCHCONFIG.
```

Even if any of the failover nodes die, the corresponding entry still exists in the system list of the EVS. During installation, the Exchange Setup wizard refers to this incorrect registry entry and fails.

Workaround

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

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

- 1 To open the Registry Editor, click **Start > Run**, type `regedit`, and then click **OK**.
- 2 In the registry tree (on the left), navigate to `HKLM\SOFTWARE\VERITAS\VCS\EXCHCONFIG`
- 3 From the Exchange Virtual Server keys, delete the keys representing the nodes that are being rebuilt.
- 4 Repeat steps 1 to 3 for the Exchange virtual server on all the nodes in the cluster.
- 5 Exit the Registry Editor.

Resource for Exchange Information Store may take time to online

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

As a default behavior, the enterprise agent for Exchange waits in the Online entry point and returns only when the IS resource starts or when the start operation fails. When IS service is delayed, the enterprise agent for Exchange logs the following message:

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

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

Workaround

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

- 1 Open the Registry Editor.
- 2 From the navigation pane, go to
`\\hkey_local_machine\software\veritas\vcs\exchconfig\parameters\msexchangeis`
- 3 On the **Edit** menu, select **New**, and then click **DWORD Value**.
- 4 Name the value *ForceExit*.
- 5 Right-click the value and select **Modify**.
- 6 In the Edit DWORD Value dialog box, specify the value data as '1'. Click **OK**.

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

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

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. See Technote 274174 at <http://entsupport.symantec.com> for more information.

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. See TechNote 277440 at <http://entsupport.symantec.com> for more information.

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 will 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.

Note: 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:

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 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:

- 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 will recognize that the VVR replication settings are complete and enable you to proceed to GCO configuration.

DR wizard will fail to create RVG if name of volume that is being replicated is assigned as a label to another volume (1316917)

In a VVR environment, if the name of the volume that is being replicated has been assigned as a label to another volume, RVG creation fails. The wizard

action panel displays a message that RVG creation has failed. The typical scenario where this might happen is if the Quick Recovery wizard has been run before running the DR wizard. In running the Quick Recovery wizard, the volume name may have been assigned as a label to the snapshot volume.

Workaround

- 1 Open Veritas Enterprise Administrator (VEA) on the target system.
If the primary RVG creation failed, open VEA on the primary system. If the secondary RVG creation failed, open VEA on the secondary system.
- 2 Change the volume label so that it does not match the name of the volume being replicated.
- 3 Run the wizard again.

IP address conflict may cause DR Wizard to fail during discovery of primary system in an Exchange Server cluster (833906)

An "Unable to find Exchange server information..." error message is displayed by the DR Wizard while performing discovery on the primary system of an Exchange server cluster.

Workaround

Verify that no DNS entries conflict with the Exchange Virtual server. Remove all Exchange server IP entries from the DNS table that are not in use.

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 DR 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 DR 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 DR 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 DR 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 DR 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 do this, 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 DR 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 will fail 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 DR 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 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, 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. This volume lock issue can result in the DR wizard failing to create secondary RVGs. This 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 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

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 will require 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 will only allow 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).

Workaround

- 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 will come 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.

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:

```
hagr -offline service_group -sys system_name -clus  
cluster_name
```

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

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

VCS wizards may fail to probe resources (1318552)

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

The following error is displayed:

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

Workaround

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

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 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.

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

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

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

Workaround

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

If VCS upgrade fails on one or more nodes, HAD fails to start and cluster becomes unusable (1251272)

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

The VCS installer does not allow you to remove VCS from those nodes with an error that those nodes are part of a cluster. The VCS Cluster Configuration

Wizard (VCW) does not allow you to remove those nodes from the cluster with an error that the nodes have a different version of VCS installed.

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

Workaround

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

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

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

```
C:\>net stop had  
C:\>net stop llt
```
- 2 On a node on which VCS was upgraded successfully, open the file *llthosts.txt* and delete the entries of all the cluster nodes on which the upgrade failed. For example, consider a cluster with three nodes, N1, N2, and N3. The *llthosts.txt* file contains the following entries:

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

If the upgrade failed on N3, delete the last entry from the file. So the modified *llthosts.txt* file should look like this:

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

The *llthosts.txt* file is typically located at `C:\Program Files\VERITAS\comms\llt`. Here `C:\` is the drive on which VCS is installed.

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

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

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

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

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

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

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

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

The gabtab.txt file is typically located at C:\Program Files\VERITAS\comms\gab. Here C:\ is the drive on which VCS is installed.

- 4 From the Windows Services snap-in, change the startup type of the Veritas High Availability Engine (HAD) service to Manual.
- 5 Repeat step 2, step 3, and step 4 on all the nodes on which VCS was upgraded successfully.
- 6 On one of the nodes on which VCS was upgraded successfully, open the VCS configuration file *main.cf* in a text editor and remove the entries of all the cluster nodes on which the VCS upgrade failed.
The main.cf file is located at %VCS_Home%\conf\config. The variable %VCS_HOME% is the default installation directory for VCS, typically C:\Program Files\VERITAS\Cluster Server.
- 7 Start HAD on the node on which you modified the VCS configuration file in step 6 earlier. Type the following on the command prompt:

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

You can remove VCS from the affected nodes using the clean up scripts provided with the software. These scripts are .bat files located in the \Tools\vpi directory on the software DVD. Refer to the readme.txt file located in the directory for details on how to use the cleanup scripts. After removing VCS, install VCS using the product installer and then add the nodes to the cluster. Contact Symantec Technical Support for more information.

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 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 -force` to stop the cluster or node where any such group is online. This workaround is not required if the cluster or node is stopped without the force option.

VCS Simulator installation may require a reboot (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 re-installing 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 will run 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 on known Veritas Volume Replicator issues.

General Issues

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 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 acknowledgement 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) is 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 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:

- 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.

Note: 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 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, prior to 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, 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 acknowledgement to the request, the pause operation would fail.

Workaround: To avoid this, perform the following:

- ◆ 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 allows you to specify a checkpoint and maintains the connection between Primary and Secondary.

Or

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 after every VCS MS Exchange 2K3 Service Group Migration 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. Even after enabling the vxcache for the volume, "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.

Software fixes and enhancements

Fixed issues and software enhancements are referenced by Symantec incident number and described briefly below.

Veritas Storage Foundation

The following issues were fixed in this release:

Table 1-4 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 vxsnap restore command fails when using the -a 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 vxsnap prepare command cannot accept more than one harddisk 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, vxsnap prepare, 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.

Table 1-4 Fixed issues for Storage Foundation for Windows (Continued)

Incident Number	Description
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.
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.

Veritas Cluster Server

The following issues were fixed in this release.

Table 1-5 Fixed issues for Veritas Cluster Server

Incident Number	Description
	Concurrency violation with online firm dependencies
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
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.

Veritas Volume Replicator

The following issues were fixed in this release.

Table 1-6 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

Table 1-6 Fixed issues for Veritas Volume Replicator

Incident Number	Description
1074533	System crash due to vxio.sys
1086439	The <code>vxedit</code> command does not work if diskgroup 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
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 for Windows and Veritas Storage Foundation HA 5.1 for Windows.

Veritas Storage Foundation and High Availability Solution Quick Recovery and Microsoft Clustering Solutions Guide for Microsoft Exchange

In the chapters on configuring Microsoft clustering with Exchange and VVR, the steps on selecting product options during SFW installation include the following limitation, which is incorrect:

Do not select the Dynamic Multi-pathing option.

The DMP Device Specific Modules (DSMs) option can be selected when installing SFW with the Microsoft Cluster Option for MSCS/Failover Clustering and VVR.

The corrected information about selecting product options for SFW with MSCS/Failover Clustering and VVR is as follows:

- Select the **Volume Replicator (VVR)** option.
- Select the **Cluster Option for Microsoft Cluster Service (MSCS)/Failover Cluster** option.
- Select any additional options applicable to your environment.
- Verify that the **Veritas Storage Foundation 5.1 for Windows (Client Components)** check box is selected to install the client components.

Veritas Storage Foundation and High Availability Solutions Quick Recovery and Microsoft Clustering Solutions Guide for Microsoft SQL

In the chapters on configuring Microsoft clustering with SQL and VVR, the steps on selecting product options during SFW installation are changed to remove the following sentence, which is incorrect:

Do not select the Dynamic Multi-pathing option.

The DMP Device Specific Modules (DSMs) option can be selected when installing SFW with the Microsoft Cluster Option for MSCS/Failover Clustering and VVR.

The corrected information about selecting product options for SFW with MSCS/Failover Clustering and VVR is as follows:

- Select the **Volume Replicator (VVR)** option.

- Select the **Cluster Option for Microsoft Cluster Service (MSCS)/Failover Cluster** option.
- Select any additional options applicable to your environment.
- Verify that the **Veritas Storage Foundation 5.1 for Windows (Client Components)** check box is selected to install the client components.

Veritas Storage Foundation and High Availability Solutions, Solutions Guide

In the chapters on configuring an application with Microsoft clustering and VVR, the steps on selecting product options during SFW installation are changed to remove the following sentence, which is incorrect:

Do not select the Dynamic Multi-pathing option.

The DMP Device Specific Modules (DSMs) option can be selected when installing SFW with the Microsoft Cluster Option for MSCS/Failover Clustering and VVR.

The corrected information about selecting product options for SFW with MSCS/Failover Clustering and VVR is as follows:

- Select the **Volume Replicator (VVR)** option.
- Select the **Cluster Option for Microsoft Cluster Service (MSCS)/Failover Cluster** option.
- Select any additional options applicable to your environment.
- Verify that the **Veritas Storage Foundation 5.1 for Windows (Client Components)** check box is selected to install the client components.

Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange

Exchange pre-installation on first node (secondary site) (page 603)

After step 4 of the procedure insert two missing steps:

5. Specify the name or IP address of the cluster node at the primary site and click **Next**.

6. Select the name of the Exchange Virtual Server for which you want to set up a secondary site and click **Next**.

On step 7 of the procedure (which will become step 9), verify the Exchange virtual server name and domain address. Those fields are not editable. The

wizard screen shown in this step of the procedure has minor differences from the actual screen in this release of the software.

Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange 2007

Exchange pre-installation on first node (secondary site) (page 599)

After step 4 of the procedure insert two missing steps:

5. Specify the name or IP address of the cluster node at the primary site and click **Next**.
6. Select the name of the Exchange Virtual Server for which you want to set up a secondary site and click **Next**.

On step 7 of the procedure (which will become step 9), verify the Exchange virtual server name and domain address. Those fields are not editable. The wizard screen shown in this step of the procedure has minor differences from the actual screen in this release of the software.

Veritas Storage Foundation Administrator's Guide

Location of New Volume tool on the VEA GUI toolbar (page 59)

The statement that the New Volume tool on the VEA GUI toolbar being the third tool from the left side of the toolbar is incorrect. The correct location of the New Volume tool on the VEA GUI toolbar is the fourth tool from the left side of the toolbar.

Setting up a dynamic boot and system volume on Windows Server 2008 (page 68)

The note that on Windows Server 2008, SFW does not manage the dynamic boot and system volume is misleading and requires clarification.

A more accurate statement is as follows:

On Windows Server 2008, although you can create and manage the dynamic boot and system volume using the SFW VEA console, the native Windows driver handles the input/output operations for that volume. Therefore, ensure that you comply with Windows Server 2008 information on best practices and restrictions on the use of a dynamic boot and system volume.

Appearance of Snapshot Volume tab (page 95)

The statement that the Snapshot Volume tab appears only when you have created snapshot volumes is incorrect. The Snapshot Volume tab always appears and does not depend on having created snapshot volumes.

Appearance of Alerts tab (page 95)

The statement that the Alerts tab appears only when an event has occurred that generates an alert is incorrect. The Alerts tab always appears and does not depend on having an event that generates an alert.

Right-click computer icon to view all drive paths (page 157)

The statement to right-click the computer icon to view all drive paths is incorrect. To view all drive paths, you right-click the StorageAgent icon.

Right-click computer icon to destroy dynamic disk group (page 182)

The statement to right-click the computer icon to destroy a dynamic disk group is incorrect. To destroy a dynamic disk group, you right-click the StorageAgent icon.

Renaming a cluster disk group (page 185)

The section to rename a dynamic disk group does not address how to rename a cluster disk group. The following note describes how to rename a cluster disk group.

Note: A cluster disk group can be renamed by entering a new cluster disk group name during the import cluster disk group operation.

Veritas Storage Foundation Volume Replicator Administrator's Guide

Read-only access given to volumes under RVG when RVG is stopped (page 306)

This information is documented in *Veritas Storage Foundation Volume Replicator Administrator's Guide*. Some additional information is given here. Earlier both Read and Write access was blocked when the RVG was stopped to disable data access. These changes have been made in Windows 2008 Server as the user is asked to format the volume after operations like failover or disk group deport or import.

Enhancements made for vxio logging

This information is missing in the *Veritas Storage Foundation Volume Replicator Administrator's Guide*.

RvRp log files are now named in the following format:

```
<type>_<objectName>__<dgName>_<dgid>.number
```

```
ex. rp_r1k_vvrocta2_1922__dg1_686c5219-038b-4e94-8ed0-d9fd12682f55.
```

This format makes it easier to locate the correct log for a particular object.

A new log called `vvr_nm__default_log.number` is created which is not associated with any RVG or RLINK. It holds the logging information pertaining to heartbeat information etc. The time information with RvRp log entries have been changed from "clock ticks since last system boot" to "time since epoch". This information is less granular but easily gives the exact system date and time for any particular message.

"Packets sent and received in a UDP port since RLINK last connected" are now logged to `nmlog` in every half an hour. This information gives an idea of the packet loss characteristic network, which is important for UDP flow control.

Every connect and disconnect is now logged to `nmlog` or `rplog` with information about TCP/UDP and number of connections.

Enhancements done in VRAS logging

This information is missing in the *Veritas Storage Foundation Volume Replicator Administrator's Guide*.

In case of version mismatch between two nodes, `vradmin log` will have the information regarding hostname, major, and minor versions along with "message version mismatch" of remote vras.

Additionally, when a user restarts vxvm service `vradmin logs` will contain major and minor versions of vras.

Miscellaneous logging enhancements

This information is missing in the *Veritas Storage Foundation Volume Replicator Administrator's Guide*.

- Logging added for vxffdc service register and unregister. Log file is created at %VMPATH%logs\vxffdcservice.log
- Logging added for vvrddcombridge service register and unregister. Log file is created at %VMPATH%logs\vxobjectserver.log

Veritas Cluster Server Administrator's Guide

Setting the checksum option (page 691)

On page 691, replace the 3rd bullet with the following:

- 2 - checksum calculated for header and message.
When set to 2, LLT also checksums the whole data buffer submitted by the client to be verified by the peer before delivering it to peer-client. In case the checksum verification fails on the receiver, LLT drops that packet, causing the sender to retransmit it. A message containing the number of bad checksum packets sent is logged in the event log.

Configuring BlackBerry Enterprise Server in a VCS environment (page 406)

The first bullet under the heading Prerequisites is incorrect. It states:

- You are required to configure an Exchange service group. Make sure you verify the prerequisites for installing and setting up Exchange in a VCS environment.

To cluster BlackBerry Enterprise Server with VCS, you are not required to cluster Microsoft Exchange with VCS. You can use other clustering solutions to cluster Microsoft Exchange as long as they are installed on different servers from those running BlackBerry Enterprise Server and VCS.

Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide

The following information is missing in the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide*.

Upgrading an Exchange Server cluster (Chapter 5)

Perform these steps before you proceed with the tasks mentioned in the topic **Optional tasks after upgrading SFW HA 5.1** on page 154.

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:

- 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.

Documentation

Storage Foundation for Windows documentation is included on the product software discs for Veritas Storage Foundation and High Availability Solutions 5.1 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: Updates to release notes can be found at:
<http://entsupport.symantec.com/docs/303042>

Table 1-7 Veritas Storage Foundation and High Availability Solutions for Windows Documentation Set

Title	File Name
Veritas Storage Foundation and High Availability Solutions	
<i>Veritas Storage Foundation and High Availability Solutions 5.1 Getting Started Guide</i>	SFW_GettingStarted.pdf
<i>Veritas Storage Foundation and High Availability Solutions 5.1 Installation and Upgrade Guide</i>	SFW_InstallUpgrade.pdf
<i>Veritas Storage Foundation and High Availability Solutions 5.1 Release Notes</i>	SFW_ReleaseNotes.pdf
<i>Veritas Storage Foundation and High Availability Solutions 5.1 Solutions Guide</i>	SFW_Solutions.pdf
<i>Veritas Storage Foundation and High Availability Solutions 5.1 HA and Disaster Recovery Solutions Guide for Microsoft Exchange</i>	SFW_HA_DR_Exch2003_Solutions.pdf
<i>Veritas Storage Foundation and High Availability Solutions 5.1 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 5.1 Quick Recovery and Microsoft Clustering Solutions Guide for Microsoft Exchange</i>	SFW_QR_MSCS_Exch_Solutions.pdf
<i>Veritas Storage Foundation and High Availability Solutions 5.1 HA and Disaster Recovery Solutions Guide for Microsoft SQL</i>	SFW_HA_DR_SQL_Solutions.pdf
<i>Veritas Storage Foundation and High Availability Solutions 5.1 Quick Recovery and Microsoft Clustering Solutions Guide for Microsoft SQL</i>	SFW_QR_MSCS_SQL_Solutions.pdf

Table 1-7 Veritas Storage Foundation and High Availability Solutions for Windows Documentation

Title	File Name
Veritas Storage Foundation	
<i>Veritas Storage Foundation 5.1 Administrator's Guide</i>	SFW_Admin.pdf
Veritas Cluster Server	
<i>Veritas Cluster Server 5.1 Administrator's Guide</i>	VCS_Admin.pdf
<i>Veritas Cluster Server 5.1 Agent Developer's Guide</i>	VCS_AgentDev.pdf
<i>Veritas Cluster Server 5.1 Bundled Agents Reference Guide</i>	VCS_BundledAgents.pdf
<i>Veritas Cluster Server 5.1 Application Note: Disaster Recovery for Microsoft SharePoint Server</i>	VCS_AppNote_Sharepoint.pdf
<i>Veritas Cluster Server 5.1 Application Agent for Microsoft Exchange, Configuration Guide</i>	VCS_Exch_Agent.pdf
<i>Veritas Cluster Server 5.1 Database Agent for Oracle, Configuration Guide</i>	VCS_Oracle_Agent.pdf
<i>Veritas Cluster Server 5.1 Database Agent for Microsoft SQL, Configuration Guide</i>	VCS_SQL_Agent.pdf
<i>Veritas Cluster Server 5.1 Hardware Replication Agent for EMC SRDF, Configuration Guide</i>	VCS_SRDF_Agent.pdf
<i>Veritas Cluster Server 5.1 Hardware Replication Agent for EMC SRDF/Star, Configuration Guide</i>	VCS_SRDFStar_Agent.pdf
<i>Veritas Cluster Server 5.1 Hardware Replication Agent for Hitachi MirrorView, Configuration Guide</i>	VCS_MirrorView_Agent.pdf
<i>Veritas Cluster Server 5.1 Hardware Replication Agent for Hitachi TrueCopy, Configuration Guide</i>	VCS_TrueCopy_Agent.pdf
<i>Veritas Cluster Server 5.1 Hardware Replication Agent for IBM Metro Mirror, Configuration Guide</i>	VCS_MetroMirror_Agent.pdf
Veritas Cluster Server Management Console	
<i>Veritas Cluster Server Management Console 5.1 Implementation Guide</i>	VCMC_Implementation.pdf
<i>Veritas Cluster Server Management Console 5.1 Release Notes</i>	VCMC_Notes.pdf

Table 1-7 Veritas Storage Foundation and High Availability Solutions for Windows Documentation

Title	File Name
Veritas Volume Replicator	
<i>Veritas Storage Foundation 5.1 Volume Replicator, Administrator's Guide</i>	VVR_Admin.pdf
<i>Veritas Storage Foundation 5.1 Volume Replicator Advisor, User's Guide</i>	VVR_Advisor.pdf
Symantec Product Authentication Service	
<i>Veritas Storage Foundation and High Availability Solutions 5.1, Quick Start Guide for Symantec Product Authentication Service</i>	SPAS_QuickStart.pdf
<i>Symantec Product Authentication Service 4.3 Administrator's Guide</i>	SPAS_AT_Admin.pdf
<i>Symantec Product Authentication Service 4.3 Release Notes</i>	SPAS_AT_ReleaseNotes.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>