Veritas Storage Foundation™ and High Availability Solutions Release Notes

Windows 2000, Windows Server 2003

5.0

Veritas Storage Foundation and High Availability Solutions Release Notes

Storage Foundation 5.0 for Windows HA

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

1/5/07

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://entsupport.symantec.com 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

Veritas Storage Foundation and High Availability Solutions Release Notes

Introduction

This document provides important information regarding the two products included in Veritas Storage Foundation and High Availability Solutions 5.0 for Windows:

- Veritas Storage Foundation™ 5.0 for Windows (SFW)
- Veritas Storage Foundation™ HA 5.0 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/285845

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

New features

The changes described below are introduced in Veritas Storage Foundation and Storage Foundation HA version 5.0.

General support

Veritas Cluster Management Console

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

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

Storage Foundation for Windows Basic (SFW Basic)

Storage Foundation 5.0 for Windows is also available as Storage Foundation for Windows Basic (SFW Basic). SFW Basic is a free technology specifically designed for edge-tier workloads. It is a zero cost SFW license and includes the Dynamic Multi-pathing option. However, an SFW Basic license is required for each physical server and the following limitations apply:

- A maximum of two physical processors
  Each processor may be comprised of multiple processing cores which may each independently act as individual processors. A Processor with "n" cores will be counted as 1 processor.
- A maximum of four dynamic volumes and file systems
  This is specific to volumes for application-related user data. Volumes required for booting (per physical server) are not included in the four volume maximum.
- Licenses may not be aggregated
  Only one license per physical server is permitted.

SFW Basic can be upgraded to SFW 5.0 or SFW HA 5.0.

See http://www.symantec.com/enterprise/sfbasic/index.jsp for more information.

New application support

- Support for Microsoft SharePoint Portal Server 2003
- Support for Microsoft Exchange Server 2007 (supported limited to SFW only)

Storage Foundation and High Availability 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, Microsoft SQL Server 2005, and for additional applications.

You can use the Configuration Center and its wizards to set up your environment for any combination of the following configurations:

- High availability at a single site for a new installation
- Wide area disaster recovery involving two sites
- Quick Recovery for on-host recovery from logical errors in application data (available for Microsoft Exchange and for Microsoft SQL Server 2005)
- Fire drill to test the fault readiness of your disaster recovery environment

Integration with LiveUpdate

Integration with Symantec LiveUpdate allows you to automatically or selectively download and install updates to SFW 5.0 or SFW HA 5.0.

Installation and licensing

Product installer enhancements

- Support for 'No License Key' evaluations
  An evaluation license key is embedded in the product. This license key is valid for a limited evaluation period only.
- Pre-installation Configuration Checker
- Built-in hyperlink to verify software and hardware compatibility during installation
- Selective installation of Veritas Dynamic Multi-pathing (DMP) DSMs
  During product installation you may choose to install one or more DMP DSMs to adds fault tolerance to disk storage by making use of multiple paths between a computer and individual disks in an attached disk storage system.

Licensing changes

See the *Storage Foundation and High Availability Solutions Installation and Upgrade Guide* for more information on these features.

- Integration with Symantec License Inventory Manager (SLIM)
  The Symantec License Inventory Manager is an enterprise asset management tracking tool. It inventories Symantec Information Availability products in your network and consolidates critical information on the deployment of these products. The Symantec License Inventory agent is automatically installed.
- Storage Foundation Basic for Windows
  Storage Foundation Basic for Windows (SFW Basic) is a free technology specifically designed for edge-tier workloads. It is a zero cost SFW license and includes the Dynamic Multi-pathing option. An SFW Basic license is required for each physical server and certain limitations apply.
- New Virtual Server Licensing Policy
  Each copy of the Veritas Storage Foundation and High Availability Solutions including all options and agents, whether used on a physical server or within a virtual machine must be separately licensed. Each Licensed Software license specifies the number of instances of the Licensed Software you may run on a particular server at one time.

Veritas Storage Foundation

Storage Management

- IP SAN Management (iSNS/iSCSI)
- Command line log for CLI operations
- Volume Shrink
- Volume Shred
- GUID Recycling

Microsoft Operations Manager (MOM) 2005 SFW Management Pack Enhancements

- Task View for VEA/VCS GUI's/Wizards
- VVR Topology diagrams
- New MOM reports
- DMP path performance statistics and Graphing

Performance

- Automated Track Aligned Volumes
- Disk group performance improvements
  - Scalability improvements for the Volume Manager Disk Group resource in an MSCS environment
  - Faster disk group import/deport for disk groups with more than 500 LUNs

Availability

- SFW Campus Cluster coordination to ensure volume growth at the correct DR site
- Wizard to backup and restore disk/disk group configuration (Private Regions) for recovery purposes
- Allow users to detach LUNs for array maintenance

Predictability

- Grow Volumes in Specific Array or Controller Locations to Ensure Proper Performance and Operation

- Monitor FlashSnap FastResync Object Locations to Ensure Fast and Reliable Snapshot Recovery

Dynamic Multi-pathing (Veritas DMP)

- Veritas DMP DSM (MPIO) Support for multiple array families
  See the Hardware Compatibility list at http://entsupport.symantec.com for specific array support and supported hardware configurations.
  Array support added for this 5.0 release includes:
  - EMC Symmetrix 8000 Series
  - EMC Symmetrix DMX Series
  - EMC CLARiiON CX Series (CX200, CX300, CX400, CX500, CX600, CX700)
  - EMC CLARiiON CX-3 Ultrascale Series Arrays (CX3-20, CX3-40, CX3-80)
  - Hitachi TagmaStore Universal Storage Platform (USP100, USP600, USP1100)
  - Hitachi TagmaStore Network Storage Controller (NSC55)
  - Hitachi TagmaStore Adaptable Modular Storage (AMS200, AMS500, AMS1000)
  - Hitachi TagmaStore Workgroup Modular Storage (WMS100)
  - Hitachi 9500V Thunder Series
  - Hitachi 9900 Lightning Series (9900 and 9900V)
  - Hitachi SANRISE9900V (SANRISE9970V, SANRISE9980V)
  - Hitachi SANRISE2000 (SANRISE2200, SANRISE2800)
  - HP StorageWorks XP128 Disk Array
  - HP StorageWorks XP256 Disk Array
  - HP StorageWorks XP1024 Disk Array
  - HP StorageWorks XP10000/XP12000 Disk Array
  - HP StorageWorks Enterprise Virtual Arrays (EVA4000, EVA6000, EVA8000)
  - HP StorageWorks Enterprise Virtual Arrays (EVA3000, EVA5000) Active/Active
  - HP StorageWorks Modular Storage Arrays (MSA1000, MSA1500) Active/Active
  - IBM System Storage N3000/N5000 Series (N3700, N5200, N5500)
  - IBM TotalStorage™ DS4000 Series (DS4200, DS4300, DS4700, DS4800)
  - IBM TotalStorage™ DS6000 Series
  - IBM TotalStorage™ DS8000 Series

- IBM TotalStorage™ ESS800/ESS750
- Network Appliance F800 Series
- Network Appliance FAS200 Series (FAS250, FAS270)
- Network Appliance FAS900 Series (FAS920, FAS940, FAS960, FAS980)
- Network Appliance FAS3000 Series (FAS3020, FAS3050)
- Network Appliance FAS6000 Series (FAS6030, FAS6070)
- Network Appliance NearStore Series
- Network Appliance V-Series
  (GF270c, GF960c, GF980c, V3020c, V3050c, V6030, V6070)
- Nihon Unisys SANArena 2200 Series (SANArena 2200 and 2800)
- Sun StorEdge SE9900 Series (StoreEdge SE9910 and SE9960)
- Sun StorEdge SE9900V Series (StoreEdge SE9970V and SE9980V)
- Sun StorEdge SE9990 Series
- Sun StorageTek 6000 Series (6130, 6140, 6540)
- Sun StorageTek FlexLine 300 Series Storage Systems (FLX380)

- New DMP Load Balancing Algorithms
  Balanced Path, Weighted Path, Least Blocks, Round Robin with Subset
- Dynamic Multi-pathing Management Enhancements
  - Dynamic Multi-pathing Graphic Usage Analysis
  - Tunable parameters for all supported arrays
  - Selective installation of DMP DSM's
- Third-party MPIO DSM co-existence

Veritas FlashSnap enhancements

- Volume Shadow Copy Service (VSS) Support
  VSS Snapshot Scheduler Wizard
  Microsoft SQL 2005 VSS Writer Support
  VSS Snapshots default to 'Read Only' Snapshots
- Snapshot Performance Improvements
  Striped Snap Plex; Striping the snap plex versus creating a simple/concatenated plex will increase performance, thereby improving resync times.
  Multi-threaded tasks results in faster snapshot mirror resynchronization. Multiple tasks are created during a resync operations with each task responsible for one of the volume's regions.

Disk Selection for the Snapshot Log Volume (DCO); Moving the DCO from the current default location of same disk as the volume to another disk greatly improves performance.

Veritas Cluster Server

Support for SharePoint Portal Server 2003 in a disaster recovery configuration

Microsoft SharePoint Portal Server 2003 is supported in a disaster recovery configuration. See the *Veritas Cluster Server Application Note: Disaster Recovery for Microsoft SharePoint Portal Server 2003* for detailed information.

Microsoft Operations Manager (MOM)

Storage Foundation HA 5.0 introduces support for Microsoft MOM 2000 and MOM 2005 with Management Packs for Veritas Cluster Server.

New hardware replication agent support

Storage Foundation HA 5.0 introduces a hardware replication agent for the IBM MetroMirror array.

New RemoteGroup agent to monitor service groups in remote clusters

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

Advanced networking support

- Added support for Networks that use Child Domains
- Enable use of CNAMES; Create a virtual name with an IP address as a CNAME alias
- Remote Group Agent support enables users to manage or monitor remote service groups from a local cluster

RemoteGroup resource type attribute definitions (763408)

The RemoteGroup resource type definition has the following additional attributes: `DomainType` and `BrokerIP`.

Attribute	Description
DomainType	For a secure remote cluster only, enter the domain type information for the specified user. Type and Dimension: string-scalar This attribute is for UNIX only. Do not configure this attribute for Windows.
BrokerIP	For a secure remote cluster only, if the user needs the RemoteGroup agent to communicate to a specific authentication broker, then set this attribute. Enter the information for the specific authentication broker in the format "IP:Port". Type: string-scalar Example: "128.11.295.51:1400" Type and Dimension: string-scalar This attribute is for UNIX only. Do not configure this attribute for Windows.

- Lanman agent updated to run under the context of a virtual name for simplified deployment in environments with anti-virus applications

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.

Enhanced support for creating secure clusters

While configuring secure clusters, the VCS Configuration Wizard (VCW) now enables searching existing Symantec Product Authentication Service Root Brokers (RB) in a Windows domain. It allows to search a root broker across the entire domain, or an Organization Unit in the domain. You can also use the available filter criteria options to search systems matching a certain condition.

Support for global clusters in a secure environment

For global clusters, VCS now provides the option of making inter-cluster communications secure. The following communications can be made secure:

- Communications between wide-area connectors
- Communications between wide-area connectors and the Steward process.

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

Veritas Cluster Server for NetApp SnapMirror

Adds support for Microsoft SQL Server 2000 & 2005

VCS privileges for operating system user groups

You can now assign VCS privileges to native users at an operating system (OS) user group level in secure clusters.

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

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

Five levels of service group dependencies

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

Enhancements to the hastop command

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

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

Simulator supports deleting simulated clusters

VCS Simulator now supports deleting simulated clusters.

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

Backup of VCS configuration files

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

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

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

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

Separate logger thread for HAD

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

New term: Daemon Down Node Alive (DDNA)

Daemon Down Node Alive (DDNA) is a condition in which the VCS high availability daemon (HAD) on a node fails, but the node is running. See the *Veritas Cluster Server Administrator's Guide* for more information.

Change in behavior: Use comma or semicolon as delimiter

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

Change in behavior: New format for engine version

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

Change in behavior for the resfault trigger

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

Change in behavior: New option for the hastart command

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

New attributes

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

Cluster attributes

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

System attributes

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

Service group attributes

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

Removed attributes

- MajorVersion—The EngineVersion attribute provides information about the VCS version.
- MinorVersion—The EngineVersion attribute provides information about the VCS version.

Veritas Volume Replicator

Veritas Volume Replicator (VVR) is an option available with Veritas Storage Foundation 5.0 for Windows or Veritas Storage Foundation HA 5.0 for Windows.

Bunker replication

Bunker replication enables VVR to achieve complete Recovery Point Objective (RPO) and limited Recovery Time Objective (RTO) without any major impact on the application's performance. With the Bunker Replication solution, a bunker site, located geographically close to the primary site, is added to the disaster recovery environment. A copy of the Primary Replicator Log is maintained, but not associated data volumes. This feature combines the advantages of synchronous and asynchronous modes of replication.

Synchronized VSS snapshots

VVR extends the SFW VSS snapshot capability for Exchange storage groups and integrates IBC messaging to create synchronized snapshots of the storage group at the primary and secondary sites. In case of a disaster at the primary site, the synchronized snapshot on the secondary site can be used to quickly recover the data up to a certain consistent point-in-time.

Volume Replicator Advisor (VRAdvisor) enhancements

- Support for multiple Replicated Volume Groups (RVGs)
- Improved graphing feature
- Improved analysis capability
- Online help

Application support

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

http://entsupport.symantec.com/

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

Note: The requirements for application support shown below supersede those requirements listed in the product documentation.

See the software compatibility list for a complete list of supported applications. Supported applications include:

Microsoft Exchange Server

- Microsoft Exchange 2000 Server: Standard Edition or Enterprise Edition (SP3 with August 2004 rollup patch required)
- 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: Standard Edition and Enterprise Edition (Evaluation support only for Storage Foundation for Windows, not supported in production environments; not supported for Storage Foundation HA for Windows)

Microsoft SQL Server

- Microsoft SQL Server 2000, 32-bit: Standard Edition or Enterprise Edition (SP4 required)
- Microsoft SQL Server 2000, 64-bit, Enterprise Edition. Supports Itanium
- Microsoft SQL Server 2005, 32-bit: Standard Edition or Enterprise Edition (SP1 required)
- Microsoft SQL Server 2005, 64-bit Standard Edition or Enterprise Edition, supports x64 platforms and Itanium-based systems (SP1 required)

Oracle

- Oracle9i Release 1 (9.0.1)
- Oracle 9i Release 2 (9.0.2)
- Oracle10g Release 1 (10.1)
- Oracle10g Release2 (10.2)

Requirements and support

Review these product installation requirements before installing Storage Foundation 5.0 for Windows or Storage Foundation HA 5.0 for Windows.

Operating systems

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

SFW and SFW HA software for servers

Your server must run one of the following operating systems:

- Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2000 Datacenter Server (all require Service Pack 4 with Update Rollup1).
- Windows Server 2003 (32-bit): Standard Edition, Enterprise Edition, or Datacenter Edition (SP 1 required for all editions)
- Windows Server 2003 R2 (32-bit): Standard Edition, Enterprise Edition, or Datacenter Edition
- Windows Server 2003 Web Edition: fully supports SFW and supports only file share for SFW HA (SP1 required)
- Windows Server 2003 for 64-bit Itanium (IA64): Enterprise Edition or Datacenter Edition (SP 1 required for all editions)
- 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

SFW and SFW HA software for clients

Your client must run one of the following operating systems:

- Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2000 Datacenter Server (all require Service Pack 4 with Update Rollup1)
- Windows Server 2003 (32-bit): Standard Edition, Enterprise Edition, or Datacenter Edition (SP 1 required for all editions)
- Windows Server 2003 R2 (32-bit): Standard Edition, Enterprise Edition, or Datacenter Edition
- Windows Server 2003 for 64-bit Itanium (IA64): Enterprise Edition or Datacenter Edition (SP 1 required for all editions)

- 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 XP Professional (SP 2 required): supported only for SFW, not SFW HA
- Windows 2000 Professional (SP 4 required): supported only for SFW, not SFW HA

Hardware requirements

Disk space

The following table estimates disk space requirements for product installation of Veritas Storage Foundation and HA Solutions 5.0.

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

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

Table 1-1 Disk space requirements

Installation options	Installation on system drive	Installation on non-system drive
SFW + all options + client components	1240 MB	Non-system space: 1240 MB System space: 265 MB
SFW + all options	980 MB	Non-system Space: 980 MB System space: 225 MB
Client components	420 MB	Non-system space: 420 MB System space: 80 MB
SFW HA + all options + client components	1675 MB	Non-system space: 1675 MB System space: 345 MB
SFW HA + all options	1230 MB	Non-system space: 1230 MB System space:285 MB
Client components	630 MB	Non-system space: 630 MB System space: 115 MB

Table 1-1 Disk space requirements (Continued)

Installation options	Installation on system drive	Installation on non-system drive
Language Pack	325 MB	Non-system space: 325 MB System space: 90 MB

Memory

- Minimum required: 512 MB
- Recommended: 1GB

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

IA64

- 1GHz Itanium or faster processor
- 1GHz Dual-Core Intel Itanium 2 or faster processor

Display resolution

- Minimum required: 800 x 600 pixels
- Recommended: 1024 x 768 pixels or higher

Supported browsers

Veritas Cluster Management Console is supported on the following browsers:

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

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

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://entsupport.symantec.com/

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

Additional requirements

Windows firewall

Before installing SFW or SFW HA, disable the Windows Firewall and anti-spyware.

Disable spyware monitoring and removal software before installing SFW or SFW HA. You must also disable the firewall to enable discovery of the local client. (270627, 274112)

Installing on 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.

Installing on remote systems in an MSCS environment

In Windows 2000 environments, Symantec recommends that you do not use Terminal Services to remotely install SFW on systems in an MSCS cluster. You may use Terminal Services using the console switch to remotely install SFW on systems in an MSCS cluster on Windows 2003 systems.

Port availability

A list of ports that are used by Storage Foundation for Windows (SFW) and Storage Foundation HA for Windows (SFW HA) is available here: http://entsupport.symantec.com/docs/286714.

Driver signing options

Depending on the installation options you select, some Symantec drivers may not be signed. When installing on systems running Windows Server 2003, you must set the Windows driver signing options to allow installation.

Table 1-2 describes the product installer behavior on local and remote systems when installing options with unsigned drivers.

Table 1-2 Installation behavior with unsigned drivers

Driver Signing Setting	Installation behavior on the local system	Installation behavior on remote systems
Ignore	Always allowed	Always allowed
Warn	Warning message, user interaction required	Installation proceeds. The user must log on locally to the remote system to respond to the dialog box to complete the installation.
Block	Never allowed	Never allowed

On local systems set the driver signing option to either Ignore or Warn. On remote systems set the option to Ignore in order to allow the installation to proceed without user interaction.

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*.

Internationalization support

The Storage Foundation for Windows and Storage Foundation HA for Windows products are internationalized to function with the following non-English language versions of the Windows Server operating system:

- European Language Group (ISO/IEC 8859-1 and ISO/IEC 8859-2 Language Group)
  This Language Group includes the following Western and Central European Languages: French, Italian, German, Spanish, Swedish, Dutch, Czech, Polish, Turkish, and Hungarian.
- East Asian Language Group (ISO/IEC 2022 Language Group)
  This Language Group includes the following East Asian Languages: Simplified Chinese, Traditional Chinese, Japanese, and Korean.

No longer supported or changed features

The following terms and behaviors have been changed in this release.

Storage Foundation for Windows

- The Prepare command replaces the Snap Start command in the GUI. Both `prepare` and `start` keywords are available in the CLI, however prepare is the recommended keyword.
- The term Dynamic Multi-pathing DSM (DMP DSM) replaces the term MPIO DSM.
- Hot Relocation is now disabled by default.
- GUID Recycling is disabled by default.
- Results from the Search feature can be saved and search queries created can be added to the VEA GUI tree view.
- Rule Manager no longer supports the following:
  - Importing and exporting rules.
  - Global SNMP setting for the recipients of notifications.
  - User-defined path for script execution log.
  - Rules based on an alert classification.
  - Configurable email subject and body for notifications.
  - Sorting the list of alerts that are available when creating a new rule.

Veritas Cluster Server

- The *VERITAS Cluster Server Application Note: High Availability for VMware ESX Virtual Machines* describing the use of a SFW HA virtual machine in a VCS for Linux environment has been removed from the documentation set. For VMware environments, Symantec recommends using the VCS for VMware ESX product.
- The `-stale` and `-force` options for the `hastart` command have been discontinued. Now, VCS backs up all configuration files (<config>.cf) including main.cf and types.cf to <config>.cf.autobackup. The configuration is backed up only if the BackupInterval is set and the configuration is writable.
  See the *Veritas Cluster Server Administrator's Guide* for more information.
- The Cluster Manager (Web Console) has been replaced by the Cluster Management Console. The Cluster Management Console can be run in single cluster mode to manage a single cluster or a central server can be configured to manage multiple clusters.
- The following attributes for the VMDg agent have been deprecated:
  - `VxobFailAction`
  - `VxobRestartAttempts`

  These have been replaced by VxVMFailAction, and VxVMRestartAttempts attributes respectively.
  See the Veritas *Cluster Server Bundled Agents Reference Guide* for more information.

Veritas Enterprise Administrator

The VEA architecture has been updated and revised. The following changes affect Storage Foundation for Windows and the Veritas Volume Replicator option:

- In previous releases, restarting the Veritas Enterprise Administrator (vxob) service was frequently used as a step to troubleshoot VEA issues. Beginning with the 5.0 release, restart the Veritas Storage Agent (vxvm) service to update the objects and operations found under the StorageAgent node.
- The refresh and rescan operations are available only after a storage agent or component within the storage agent has been selected.
- All StorageAgent related commands, such as reset SCSI bus or vxcache memory configuration, are available after the StorageAgent node has been selected.

- When VEA is launched, the local host is no longer the default connection. You must specify a host to connect to.
- VEA now follows a host-based approach. Only one host at a time can be viewed. You can use the New Windows button to launch multiple windows. To view a different host in your current window either switch connections using the URL bar (Select Host) or click View > Connection > *<machine name>*.
- The Favorite Hosts and Network nodes have been eliminated from the tree view.
- The VSFW Assistant has been replaced by the Assistant perspective. The Assistant presents the most commonly used tasks on the selected host or domain.
- The properties menu item available when a component (disk group, disk, volume, etc.) is selected in the tree view has been moved from the Actions menu to the File menu. To access properties for a selected component, click File > Properties.

Veritas Volume Replicator

- The VVR Security Service Configuration (VxSAS) Wizard is no longer launched automatically after installing SFW or SFW HA with the VVR option. You may choose the appropriate time in your configuration process to launch the wizard manually (Start > All Programs > Symantec > Veritas Storage Foundation > Configuration Wizards > VVR Security Service Configuration Wizard).
- After changing the VRAS logging level or timeout values, VVR no longer requires the restart of the vxvm or vxob service. To change these tunables:

  1. Open the registry editor using the command, `regedit`.
  2. Navigate to one of the following locations:
     For 32-bit systems
     HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\VRTSobc\pal33\Agents\StorageAgent\constants
     for 64-bit systems
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VERITAS\VRTSob\pal33\Agents\StorageAgent\constants
  3. To change the logging level, modify the registry DWORD value for the LOG_LEVEL entry, from the default value of 0 to 10 to increase the logging level or from 10 to 0 to decrease the logging level.

4 To change the VRAS timeout, modify the registry DWORD value for the AE_TIMEOUT entry, from the default value of 30 seconds to a higher value or restore from a higher value to 30 seconds.

5 In order for the registry key change to take effect, at the command prompt type:
vxassist refresh

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.
- The Symantec License Inventory Agent Release Notes contain required configuration information for the SLIM Agent. These Release Notes can be found at http://entsupport.symantec.com/docs/285602.
- 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 5.0 and options, refer to the *Veritas Storage Foundation and HA Solutions for Windows Installation and Upgrade Guide*.

Warning: Make sure that you update Windows 2000 to SP4 with Update Rollup1 before you upgrade to SFW 5.0 or SFW HA 5.0. Otherwise, system corruption can occur.

- Install the Veritas Storage Foundation and HA Solutions software in the following sequence:
  - Veritas Storage Foundation and HA Solutions 5.0, with any installation options for version 5.0, such as VCS Agents or VVR
  - Language Pack for 5.0

- The Release Notes file is located on the Veritas product disc and updated Release Notes can be found at http://entsupport.symantec.com/docs/285845. 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.

Note: Updated Release Notes can be found at http://entsupport.symantec.com/docs/285845

Software limitations

See http://entsupport.symantec.com/docs/285845 for a complete list of software limitations as well as other late-breaking news.

The following limitations apply to Veritas Storage Foundation and High Availability Solutions 5.0 for Windows.

Installation and licensing

This section provides information on limitations specific to installation and licensing.

Installation of 4.3 MP1 does not proceed with dynamic multi-pathing drivers (DDI-3 or higher)

If the Dynamic Multi-pathing drivers (DDI Package) currently installed are a more recent version than the version contained in this maintenance pack, the SFW 4.3 MP1 upgrade installation does not proceed with the install.

Workaround: Uninstall the DDI Package before proceeding and reinstall it after the installation of this maintenance pack.

Demonstration license is for new installations only [367061]

Demonstration (NFR) license keys should only be used for new installations. If you use a demonstration license to upgrade a system that has an existing permanent license, then the SFW options enabled by the license key do not function correctly.

Invalid characters in computer names (410462)

Computer names are limited to letters, numbers, and some special characters. Invalid characters in computer names include the following: blank space, ~ ! @ # $ > * ( ) = + [ ] { } \ | ; : ' " , < > / ?

Growth in swap file may leave insufficient space for installation (221771)

The Veritas installer does not account for growth in the swap file when determining sufficient disk space. If the swap file grows while copying the files to the local system, not enough space may remain to complete the installation.

Symantec License Inventory Agent not installed on Windows 2000 (799257)

On systems running Windows 2000, the Symantec License Inventory agent is not automatically installed with a new installation or upgrade of SFW or SFW HA. If you want to use the License Inventory agent, you must install it separately. See the Symantec License Inventory Agent Release Notes at http://entsupport.symantec.com/docs/285602.

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:

- VDS 1.1 Hardware Providers (available from your array vendor)
- Windows Server 2003 R2 (32-bit): Standard Edition, Enterprise Edition, or Datacenter Edition
  - Including 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)
- Microsoft iSCSI Software Initiator, version 2.02 or higher

Note: : iSCSI support is available for Windows Server 2003 R2 (32-Bit) operating system only at this time. Support for the x64 and IA64 versions of Windows Server 2003 R2 are planned, but are not supported at this time.

Limitations on 64-bit systems

No iSCSI node after launching VEA GUI on 64-bit machines (641273, 819142)

iSCSI support is only available for Windows Server 2003 R2 (32-Bit) operating system at this time. Support for the x64 and IA64 versions of Windows Server 2003 R2 are not supported at this time.

After upgrading 64-bit systems to SFW HA 5.0, the Vxbridge service fails to register (850332)

The Vxbridge service is not upgraded properly. This prevents the VMDg and MountV resources in the upgraded service group from being probed.

Workaround: Execute the %VMPATH%VM5INF\UpgSvcs.bat batch file after the upgrade is complete.

VCS Configuration Wizard cannot be launched after upgrading an x64 cluster to SFW HA 5.0

The VCS Configuration Wizard cannot be launched on an x64 cluster after upgrading the cluster to SFW HA 5.0. After upgrading, the path to VCW.exe is no longer included in the environment path variable.

Workaround: Edit the environment path variable to include the location of VCW.exe. The default location of VCW.exe is: `C:\Program Files (x86)\VERITAS\Cluster Server\Bin\VCW`

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.

SFW cannot support VDS on 64-bit Windows 2003 Server (309292)

SFW does not currently support Virtual Disk Service (VDS) on 64-bit servers because the 64-bit Windows 2003 interface does not support SFW.

This is a 64-bit Windows 2003 issue and has been reported to Microsoft. Refer to Microsoft case 100-43599 for additional information.

Booting an IA64 Windows 2003 Server from a mirror of a GPT system partition may fail (349934)

Booting a 64-bit Itanium (IA64) Windows 2003 server from a mirror of a GPT system partition may fail. This problem occurs when the disk where the original system partition resides is missing or removed from the system. The system cannot be booted from the mirror when the original system partition is missing.

This is a known Microsoft issue. See Microsoft Knowledge Base article KB814070 for details.

SFW does not support DMP ASLs on Windows Server 2003 64-bit systems

SFW support for Windows Server 2003 64-bit systems is available only for arrays that have an MPIO Device Specific Module (DSM) available.

Cluster disk groups not recognized in Microsoft SQL 2000 (308430, 418435)

On Windows Server 2003 64-bit Itanium systems running both SFW and SQL 2000, cluster disk groups created in SFW 4.3 are not recognized in SQL 2000. This Microsoft SQL 2000 issue has been reported to Microsoft.

Note: If SQL Server 2000 is not installed and the SFW cluster disk group is already created, you must first install SQL Server 2000 on basic disks and then perform the following workaround.

Workaround: This workaround is for SQL Server 2000 in an environment with Microsoft Cluster Server (MSCS). With Microsoft SQL Server 2000 offline, use the following procedure to enable SQL Server 2000 to recognize a dynamic disk resource:

1. Update SQL Server 2000 with the most recent service pack.
2. Open the Cluster Administrator console and find the resource group that contains the resources for SQL Server.
3. Take the SQL Server resource group offline:
   a. Right-click the SQL Server resource group.
   b. Select **Take Offline**.
4. Remove the Physical Disk resource from the Dependencies tab of any resources in the SQL Server resource group where it is listed. For each resource:
   a. Right-click each resource and select **Properties**.
   b. In the Properties window, click the **Dependencies** tab and select **Modify**.
   c. Remove the Physical Disk resource, if it exists, from the right column.
   d. Record the resources that depend on the Physical Disk resource, so they can be added to the dependency list of the SFW Disk Group resource.
5. Remove the Physical Disk resource from the cluster:
   a. Right-click the **Physical Disk** resource.
   b. Select **Delete** from the menu that appears.
6. Upgrade the SQL Server disk to a cluster dynamic disk.
   a. Open the VEA console.
   b. Click the **Disk View** tab.
   c. Right-click the disk that SQL Server is installed on.
   d. Select **New Dynamic Disk Group** from the context menu to launch the wizard.
   e. Provide a new dynamic disk group name and check **Create Cluster Group**.

7 Open the Cluster Administrator console and create a new SFW Disk Group resource in the SQL Server resource group using the newly created cluster dynamic disk group.

8 Make each of the cluster resources on the list from Step 4 dependent on the SFW Disk Group resource created in Step 7.

   a Right-click each resource.

   b Select **Properties**.

   c In the Properties window, click the **Dependencies** tab and then click **Modify**.

   d Select the resource created in Step 7 from the list on the left side and add it to the list of dependencies on the right side.

9 Bring the SQL Server cluster resource group back online.

10 Verify that SQL Server is functioning properly.

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.

DMP ASLs do not support Active/Active configuration in a clustered environment (263516)

In a clustered environment, Active/Active configuration of multiple paths using Dynamic Multipathing array support libraries (DMP ASLs) is not supported.

Workaround: Set disks in a clustering environment or disks with private dynamic disk group protection enabled to Active/Passive load balancing.

Note: An Active/Active configuration in a clustered environment is supported by Dynamic Multipathing MPIO DSMs. For more information, see the Dynamic Multipathing chapter of the *SFW Administrator's Guide*.

DMP does not support basic disks as a cluster resource under MSCS (101036)

Failover may not function properly when using the Dynamic Multipathing DMP feature with an MSCS basic disk cluster resource. Refer to TechNote 251662 on the Veritas Support site for details.

Workaround: The initial setup of MSCS requires that you use a basic disk as the quorum disk. To use DMP with SFW and an MSCS cluster, you must convert the MSCS basic disk cluster resources to dynamic disk cluster resources before activating DMP. After SFW is installed, create a new cluster disk group and a mirrored volume. Create a new quorum resource of the VMDg type and then convert the Quorum resource from the basic resource to the new dynamic resource. See the MSCS chapter of the *SFW Administrator's Guide*.

Error when creating a partition in a system with DMP installed (123280)

You may receive a "Volume never arrived" error when creating a partition in a system with the Dynamic Multipathing DMP feature installed. DMP was designed to support storage on dynamic disks. In some situations, DMP does not support the creation of new partitions on basic disks.

Workaround: Convert the basic disk to a dynamic disk.

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.

Basic disk cannot be used as MSCS quorum disk for Active/Active load balancing (415290)

MPIO DSMs do not support the use of a basic disk as an MSCS quorum disk in Active/Active load balancing configurations.

Failover may not function properly when using MPIO DSMs with an MSCS quorum basic disk. You must convert the MSCS quorum disk from a basic disk to a dynamic disk. Although the initial setup of MSCS requires that you use a basic disk as the quorum disk, once SFW is installed, you should upgrade this basic disk to a dynamic disk.

VEA GUI does not display storage array information (492740)

When rebooting a system and enabling its paths to the storage in an MSCS cluster on Windows 2000, the VEA GUI does not display the storage array information.

The storage array information does not appear because of a problem with VDsm interfacing with WMI.

Workaround: The workaround is to perform a rescan operation to display the information in the VEA GUI. However, you may also have to restart the WMI and vxob services if the rescan operation does not cause the information to appear.

Limitations of SFW with Exchange and SQL

Support for VSS snapshots (836802)

The Storage Foundation and High Availability Solutions for Windows 5.0 release uses Veritas FlashSnap with the Microsoft Volume Shadow Copy Service (VSS) technology to support snapshots of Exchange 2003 storage groups and SQL Server 2005 databases. The following tables describe Symantec support for the different snapshot methods offered in the 5.0 release.

Table 1-3 describes support in Microsoft Exchange 2003 environments.

Table 1-3 VSS snapshot support with Microsoft Exchange 2003

Snapshot method	standalone (non-clustered) environment	MSCS with SFW environment	SFW HA (clustered) environment
VSS Snapshot Wizard or VSS Snapshot Scheduler Wizard	✔	✔	✔
vxsnap command line interface	✔	✔	✔
Quick Recovery Configuration Wizard	✔	X	✔

Table 1-4 describes support in SQL Server 2005 environments.

Table 1-4 VSS snapshot support with Microsoft SQL Server 2005

Snapshot method	standalone (non-clustered) environment	MSCS with SFW environment	SFW HA (clustered) environment*
VSS Snapshot Wizard or VSS Snapshot Scheduler Wizard	✔	✔	X
vxsnap command line interface	✔	✔	X
Quick Recovery Configuration Wizard	✔	X	X

*In an SFW HA environment, Symantec supports SQL Server 2005 with the vxsnapsql command line interface.

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.

Veritas Cluster Server

This section covers limitations specific to Veritas Cluster Server.

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 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.

A user in a user group does not receive Cluster Administrator rights (864671)

When adding a user group to a cluster, users in that group do not receive Cluster Administrator rights. This is a limitation only in the Java GUI. However the users in the group do get full administrative permissions for using CLI commands.

Workaround: Use the Java GUI to add individual users to the cluster to receive the Cluster Administrator rights.

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.

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 onlining, monitoring, and offlining of the third-party monitoring tool.

VCS lock on shared volumes during Exchange recovery

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

Workaround: Symantec recommends freezing the service group containing the MountV resources before recovering Exchange volumes. To recover an Exchange volume that is monitored by VCS:

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

If custom resources are configured in VCS to monitor a snapshotted volume, follow the procedure 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.

VCW configures the cluster with both upper and lower case of the same system name (506454)

By design, the VCS Engine (HAD) is case sensitive. If you change the system name through the System Properties dialog box or any other method and follow a capitalization format different from that of the original name then the VCS engine considers this as a new system and creates an additional entry in the `main.cf` file.

Workaround: If you use the system name in any of the VCS commands, make sure that the system name is in uppercase (all caps).

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.

Reconfiguring a root broker in a secure cluster may cause VCS commands to fail (764745)

If you reconfigure the root broker while editing a secure cluster, VCS commands may fail on the node on which you edit the cluster. The following error message is displayed:

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

However, the VCS commands work from the other nodes in the cluster.

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.

Veritas Volume Replicator

This section covers limitations specific to Volume Replicator.

Resize Volume and Autogrow Not Supported in Synchronous Mode (103613)

The Resize Volume and Autogrow operations are not supported when replication is 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.

Known issues

See http://entsupport.symantec.com/docs/285845 for a complete list of known issues as well as other late-breaking news.

The following known issues exist in Veritas Storage Foundation 5.0 and Veritas Storage Foundation HA 5.0.

Installation and licensing

This section provides information on known installation and licensing issues.

Software installs registry keys with read-write permission for Power Users group

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.

Upgrade to SFW 5.0 or SFW HA 5.0 requires Windows 2000 SP4 with Update Rollup 1

Make sure that you update Windows 2000 to SP4 with Update Rollup1 before you upgrade to SFW 5.0 or SFW HA 5.0. Otherwise, system corruption can occur.

Adding a license to enable a feature requires SFW Service restart (102481, 206555)

If you enter a license key to add a feature or option (such as VVR, MSCS, or FlashSnap) to the already installed SFW program, you must stop and restart the SFW storage agent service (vxvm) for the feature to take effect.

To stop and start the service, enter the following at the command line:

```
net stop vxvm
net start vxvm
```

You must restart the VEA console after the commands run.

A default evaluation license key is used for installation (770728)

The *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide* contains the statement, "No license key is required for the version of the SFW and SFW HA release 5.0." If you do not have a license key a default evaluation license key is supplied for you to use during a limited evaluation period. To use this evaluation key click Next on the License key screen. You must purchase the product to obtain a permanent license key.

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.

Installer may display an error message when trying to locate nodes (107360)

When the domain controller and the system where the installer is running are located in different subnets, the installer is unable to locate the target nodes for installation.

Workaround: Continue the installation by manually entering the host names or the IP addresses of the missing nodes.

Installation to remote servers may fail if the user account has a roaming profile

A roaming profile does not always create the necessary folder structure required by Microsoft on remote servers. The Microsoft Installer looks for the folder structure for the user account (used to install SFW) in the "Documents and Settings" folder on each remote server. If the user's folder is not present, the installation will fail. This problem can be resolved by logging in as a user without a roaming profile (with Domain Administrator's privileges). Refer to Microsoft for information on roaming profiles.

Configuration Checker wizard cannot perform checks outside of the current domain (833120)

You can select nodes outside the current domain and the Configuration Checker wizard can perform a check on those nodes, but *only* if the target domain has the same set of administrator credentials as the ones that are used to log into the current domain.

For example, if you log into domainA as administrator with password "password", and run the Configuration Checker wizard on node B, which is in domainB, you can only perform checks on node B if domainB has the administrator credentials with the password of "password".

NetBackup 6.0 MP4 installation media required (858241)

NetBackup 6.0 Maintenance Pack 4 is required for SFW HA 5.0 environments. The EMM database will not be configured correctly if you install NetBackup 6.0 and then upgrade to Maintenance Pack 4.

Workaround: After installing SFW HA 5.0, use the bundled installation media for NetBackup 6.0 MP4. This installs NetBackup 6.0 and Maintenance Pack 4 in a single step and the EMM database will be correctly configured. If you are upgrading from a previous version of SFW HA with NetBackup 6.0, first upgrade NetBackup 6.0 to NetBackup 6.0 MP4, then upgrade SFW HA.

Reboot after installing NetBackup and SFW on the same system (102053) (866167)

Volume creation may fail when NetBackup 6.0 GA, 6.0 MPx, or 6.5 and Storage Foundation for Windows 4.3, 4.3 MP1, or 5.0 are installed on the same system. This situation occurs when the system is not rebooted after installing the NetBackup server or client.

Workaround: Reboot the system after installing either the NetBackup server or client.

Files install to directories other than directory specified

On a 32-bit operating system, SFW and SFW HA install to:

```
C:\Program Files\Veritas
```

On a 64-bit operating system, files install to:

```
C:\Program Files\Veritas
C:\Program Files (x86)\Veritas
```

If you specify a different target directory, most files install to that location. However, some files also install to:

```
C:\Program Files (x86)\Veritas
C:\Program Files\Common Files\Veritas
C:\Program Files (x86)\Common Files\Veritas.
```

Files remain on system after SFW is uninstalled (259398)

User data files and files related to the uninstall process are left behind after Veritas Storage Foundation is uninstalled.

Workaround: Delete the files contained in the following directories:

boot drive\Documents and Settings*logon ID*\Application Data\Veritas

boot drive\Documents and Settings*logon ID*\Local Settings\Temp

boot drive\Documents and Settings\All Users\Application Data\Veritas
boot drive\WINDOWS\Temp\VManager

Delete the following directories:

boot drive\Documents and Settings*logon ID*\Application Data\Veritas
boot drive\Documents and Settings\All Users\Application Data\Veritas
boot drive\WINDOWS\Temp\VManager
boot drive\Config.Msi

Push installations are done in a serial fashion (221780)

During a push installation, binaries are copied to one node at a time and are not installed in parallel. Installation progress reaches approximately 10% on one system before the installation begins on the next system.

Uninstalling SFW HA removes VRTSweb and disables SLIM manager (700978)

The VRTSweb service is used by SFW HA and SLIM manager. Uninstalling SFW HA from a system removes the VRTSweb service. If the SLIM manager is also installed on the system, the removal of the VRTSweb service disables the SLIM manager.

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

Error Message while uninstalling SFW or SFW HA (763769)

While uninstalling SFW or SFW HA you may encounter an error indicating "strong name validation failure for plugin host."

This error does not affect product functionality.

Workaround: Click OK to close the error message dialog box. Allow the uninstall to proceed unless the process stops and the progress bar turns red. If this occurs, cancel the uninstall process and then relaunch the uninstall wizard from Add or Remove Programs.

Troubleshooting errors (639785)

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.

Snapshot and Restore issues

Memory leaks occur during VSS snapshot operations (884205)

A memory leak occurs during the course of repeated VSS-based Quick Recovery snapshot operations. This issue is observed on all snapshots that use Veritas FlashSnap with the Microsoft Volume Shadow Copy Service (VSS) technology, including scheduled snapshots created by the VSS Snapshot Scheduler Wizard or Quick Recovery Configuration Wizard as well as snapshots created using the VSS Snapshot Wizard or vxsnap command line. Several causes of this memory leak have been identified and are under investigation by Symantec Corporation and Microsoft Corporation (KB913648). The Late-Breaking News TechNote at http://entsupport.symantec.com/docs/285845 is updated regularly as information and hotfixes become available.

In order to fully understand the impact the memory leak will have in your specific environment, Symantec recommends that you deploy your Quick Recovery scenario in a test environment prior to installing SFW or SFW HA 5.0 in your production environment.

Workarounds: Symantec strongly recommends that you install the Volume Shadow Copy Service update from Microsoft available at http://support.microsoft.com/kb/913648/ in order to reduce the amount of memory leak.

Additionally, you can release the memory by stopping and restarting the Veritas Storage Agent service (vxvm) from the Service Control Manager or with the **`net stop vxvm`** and **`net start vxvm`** commands from the command line. You may find it useful to plan to stop and restart the Veritas Storage Agent service during your regularly scheduled maintenance window.

In an MSCS environment, when the Veritas Storage Agent service is stopped the group containing the Veritas Volume Manager DG resource fails over to another cluster node. Symantec recommends that you restart the Veritas Storage Agent service on the inactive cluster nodes, move the group to one of those nodes, and then restart the Veritas Storage Agent service on the node that previously hosted the group.

In an SFW HA environment, when the Veritas Storage Agent service is stopped, the VMDg and MountV resources transition to an UNKOWN state. Once the service is restarted, the resources return to an ONLINE state. No failover occurs.

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

VSS Restore Wizard may not list the Quick Recovery snapshot XML file required to restore a snapshot set (818798)

If you are restoring a snapshot set with the VSS Restore Wizard, the wizard lists only the XML files located as follows:

- If a redirect.txt file is present in `C:\Program Files\Veritas\Veritas Volume Manager 5.0\VSSXML`, the wizard lists the files in the directory specified in the redirect.txt file.
- Otherwise, it lists the files in the default VSSXML directory: `C:\Documents and Settings\All Users\Application Data\Veritas\VSSXML\`*`ApplicationName`*

However, in the Quick Recovery Wizard you can specify a different directory to store XML files. If you did so, but did not also create a redirect.txt file pointing to that directory, the VSS Restore wizard does not list the XML files in that directory.

Workaround: In the redirect.txt file, include the full file path to the location of the XML files, for example: G:\SnapshotSets. Then run the VSS Restore wizard. The XML files from that directory will now be displayed.

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. 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.

Restoring Exchange subcomponent that spans more than one volume is not supported (342776)

Restoring a subcomponent of an Exchange database that spans more than one volume is not supported in SFW.

Workaround: The workaround is to contain each subcomponent in only one volume.

The `vxsnap prepare` command cannot accept more than one harddisk per volume (649092)

The `vxsnap prepare` CLI command is limited to the specification of one harddisk per volume by design. Enhancing the `vxsnap prepare` CLI command to allow the specification of more than one harddisk per volume is being considered for a future release of SFW.

The `vxsnap restore` command fails when using the -a option to dismount volumes (511754)

When you run the `vxsnap restore` command from the CLI with the `-a` option (to dismount volumes), only the mail boxes are dismounted and the restore fails with an open handle message for the mounted volume.

Workaround: Run the `vxsnap restore` command from the CLI with the `-f` option as well as the `-a` option.

For Exchange Server 2007 environments, manually dismount Exchange database stores before doing the VSS Restore (796211)

In Exchange Server 2007 environments, the VSS Restore Wizard does not automatically dismount Exchange database stores.

Workaround: Manually dismount all Exchange database stores and close all open handles. Either launch the VSS Restore Wizard or use the `vxsnap restore` command with the `-f` option to restore Exchange Server 2007 VSS snapshot sets.

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

Scheduled snapshots fail if there are multiple subcomponents on single volume (704644)

Snapshots scheduled with the VSS Scheduler or with the Quick Recovery Configuration Wizard may fail if the different objects of an Exchange storage

group (for example, mailbox, public folder, log folder) share the same volume, or if a SQL database and log volume share the same volume.

Workaround: Ensure that the Exchange storage group objects or SQL database components do not share the same volume.

Scheduled snapshots fail if volumes have the same name (630138)

Scheduled snapshots may fail if any of the volumes associated with the database components have the same internal volume name as another volume on the system.

Workaround: Ensure that the volume names for database components are unique on the system.

Some registry entries created by the Quick Recovery Wizard remain after the schedule is deleted using the VEA console (841623)

If you delete a snapshot schedule using the Veritas Enterprise Administrator console instead of using the Quick Recovery Wizard, the registry entry for the snapshot schedule is correctly deleted. However, the mirror preparation registry entry created by the Quick Recovery Wizard is not deleted.

Workaround: Check the TechNote for the availability of a utility that cleans up these obsolete Quick Recovery Wizard registry entries:
http://entsupport.symantec.com/docs/285845

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: Check the TechNote for the availability of a utility that synchronizes snapshot registry entries on all nodes:
http://entsupport.symantec.com/docs/285845

When a node is added to a cluster, existing snapshot schedules are not replicated to the new node (800766)

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: Check the TechNote for the availability of a utility to update the registry entries:

http://entsupport.symantec.com/docs/285845

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 Configuration Wizard issues

The Quick Recovery Wizard does not update the screen that shows available disks for snapshot volumes while the wizard is running (621856)

If the wizard shows there are not enough disks to snap prepare a volume, and you then make more disks available (add a new disk to the disk group or free up some disks), those changes are not visible in the running instance of the Quick Recovery Wizard.

Workaround: Close the current instance of the wizard and restart the wizard.

The Quick Recovery Wizard fails to disable the settings for disk assignment once mirror preparation is complete (848908)

If you want to use the Quick Recovery Wizard to change the assigned disks for snapshot volumes, you can do so only before the snapshot mirror preparation is scheduled to start. Once mirror preparation is complete, although the disk assignment fields remain enabled, if you edit the disk assignments, the wizard displays an error when you reach the implementation panel.

Workaround: Symantec recommends leaving the original disk assignments for snapshot volumes. If you need to change the disk locations of the snapshot volumes, use the Quick Recovery Wizard to add a new snapshot set for the required component.

The Quick Recovery Wizard does not prevent scheduling snapshots for Exchange 2000 but the scheduled snapshots will fail (787564)

The Quick Recovery Wizard allows scheduling snapshots for Exchange 2000 but Exchange 2000 does not support VSS snapshots and the snapshots will fail.

Workaround: Verify that the Exchange version for which you want to schedule snapshots meets the requirements for supported software.

The Quick Recovery Wizard may return an SFW discovery error if run after failover to another cluster node (843076)

The Quick Recovery Wizard may return an SFW discovery error if run after Exchange fails over to another cluster node.

Workaround: In the Veritas Enterprise Administrator console, connect to the system you had selected in the wizard and do a rescan (right-click the storage agent and click **Rescan**). Then restart the wizard.

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 (866516)

The same system may be running both a standalone SQL Server instance and a SQL instance that is part of an MSCS cluster. The Quick Recovery Wizard does not support the clustered instance but it does support the standalone instance, except in the following case: If the instance that is part of an MSCS cluster has been configured as a default rather than a named SQL instance, the wizard is unable to discover either SQL instance. In that case the wizard displays an error message that no application instance exists on the system.

Workaround: Use the VSS Snapshot Scheduler Wizard.

VEA Console issues

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.

iSCSI issues

Unable to define an alias for an iSCSI target under the initiator in tree view (640547)

In the left pane tree view of the GUI, an alias for a target under the iSCSI node cannot be defined. When this action is attempted, the error message “Failed to define alias for target” appears.

Internationalization issues

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

The version number of DMP ASLs is not updated in the Device Manager after an upgrade. (499290)

After upgrading to SFW 5.0, the DMP ASL version number of the original release is displayed in the Windows Computer Management's Device Manager despite a successful upgrade. Product performance is not affected.

MPIO parameters are not persistent after rebooting (845637)

When you change an MPIO parameter value, the value returns to the default value after you reboot the system.

The DSM Balanced Path load balancing policy becomes unusable after a system reboot. (862074)

After a reboot, the configuration for the Balanced Path policy is lost and the policy becomes unusable.

Workaround: Re-enter the settings for the Balanced Path policy after system reboots. For additional information about this issue, contact Technical Support (http://entsupport.symantec.com).

Other issues

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.

Extra spaces are inserted in Rule Manager alert topics (915091, 915208)

When editing a rule based on alert topics by the Rule Manager in SFW 5.0, extra spaces are inserted in the alert topics string. The rule fails to execute when these extra spaces are in the alert topics string.

For example after editing a rule, the resulting alert topic string may be " event.alert.vrts.stop, event.alert.vrts.start ". In this example, leading and trailing spaces were inserted in the string, and a space following the comma was inserted in the middle of the string.

Workaround: Each alert topic that was edited must be adjusted with the Rule Manager to delete all spaces in the string. For instance, in the alert topic string from the example above delete the extra spaces so that the string becomes "event.alert.vrts.stop,event.alert.vrts.start".

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.

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.

Cannot stop VCS when PromptClusStop is set (893131)

If you set the EngineShutdown attribute to PromptClusStop, the hastop command may not work.

Partial groups go online after restart (821454)

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

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

If your service groups have a large number resources or resource dependencies, and if the PrintTree attribute is set to 1, saving the configuration may cause cause the configuration file to become excessively large in size and may impact performance.

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 require
51031	Unable to automatically fail over global group %s remotely because local cluster does not have Authority for the group.
50913	Unable to automatically fail over global group %s remotely because clusters are disconnected and ClusterFailOverPolicy is set to %s. Administrative action is required.
50914	Global group %s is unable to failover within cluster %s and ClusterFailOverPolicy is set to %s. Administrative action is required.
50916	Unable to automatically failover global group %s remotely due to inability to communicate with remote clusters. Please check WAN connection and state of wide area connector.
50761	Unable to automatically fail over global group %s remotely because ClusterList values for the group differ between the clusters. Administrative action is required.
50836	Remote cluster %s has faulted. Administrative action is required.
51032	Parallel global group %s faulted on system %s and is unable to failover within cluster %s. However, group is still online/partial on one or more systems in the cluster
51033	Global group %s is unable to failover within cluster %s and AutoFailOver is %s. Administrative action is required.

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)

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 1-5:

Table 1-5 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)

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).
```

Workaround: Use the `hastop -all` command to stop HAD and related processes. Then run the `hastart` command to restart HAD.

VEA console may not populate after upgrading a secure 4.x SFW HA cluster (701336)

After upgrading a secure 4.x SFW HA cluster to SFW HA 5.0, the VEA console may not populate the view below the localhost icon because the security credentials may not have been updated.

Workaround: After upgrading to SFW HA 5.0, complete the following steps on each node in the secure cluster:

1. Create a temporary folder anywhere on the cluster node.
2. Navigate to the directory, `C:\ProgramFiles\Veritas\Security\Authentication\systemprofile\certstore`
   (For 64-bit machines, the directory is `C:\Program Files(x86)\Veritas\Security\Authentication\systemprofile\certstore`).
   Here, C: is the drive on which VCS is installed.
3. Move all the contents, except the **keystore** and **trusted** directories, to the temporary folder you created earlier in step 1. (Do not move the keystore and trusted directories.)

   Note: Note that you must move (Cut) and not copy the contents of the directory.

4. Restart `vxob` on the node. Type the following on the command line:

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

5. Copy all the contents from the temporary folder that you created earlier in step 1, back to the directory `C:\Program Files\Veritas\Security\Authentication\systemprofile\certstore`. (For 64-bit machines, the directory is `C:\Program Files(x86)\Veritas\Security\Authentication\systemprofile`

\certstore). Click **No** when prompted whether you want to replace any existing files. DO NOT replace any existing files in the target directory.

6 Delete the temporary folder that you created earlier in step 1. This step is optional. You may want to retain this directory, for debugging purposes.

Repeat these steps on each node in the secure cluster.

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`.

Cluster Manager (Java Console) privileges on German systems (348920)

On German systems with Windows Server 2003 Enterprise Edition, user privileges change to Guest when users log into the Java Console. This issue is observed on German systems after Symantec Product Authentication Service is used to create a secure cluster.

Workaround: Manually assign privileges on German systems:

1 On all nodes, set HAD service startup type to MANUAL.

2 Reboot all nodes.

3 Add users to the Users attribute in main.cf file

4 On all nodes, set HAD service startup type to AUTO.

5 Run `hastart` on all nodes.

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 5.0 with specific Fibre Channel host bus adapters.

Emulex Fibre Channel adapters

For servers configured with Emulex Fibre Channel host bus adapters, you must modify settings of the adapter. The default settings of the adapter do not ensure proper function of SCSI reserve and release.

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

1. Locate and run the Emulex utility for changing Miniport driver settings.
2. Select **Configuration Settings**.
3. Select **Adapter Settings**.
4. Set the **Topology** parameters to **1, Permanent,** and **Global**.
5. Set the **ResetFF** parameters to **1, Permanent,** and **Global**.
6. Set the **ResetTPRLO** parameters to **1, Permanent,** and **Global**.
7. Save the configuration.
8. Repeat step1 through step 7 for all Emulex adapters in each system.
9. Reboot the systems.

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

QLogic Fibre Channel adapters

When configured over QLogic Fibre Channel host bus adapters, the DiskReservation agent requires the Target Reset option of the adapter to be enabled. By default, this adapter option is disabled, causing the agent to hang during failover.

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

1. During system startup, press **ALT+Q** to access the QLogic adapter settings menu.
2. Select **Configuration Settings**.
3. Select **Advanced Adapter Settings**.

4 Set the **Enable Target Reset** option to **Yes**.

5 Save the configuration.

6 Repeat step 1 through step 5 for all QLogic adapters in each system.

7 Reboot the systems.

VCS 5.0 with Microsoft Exchange Server

The following issues apply to VCS 5.0 with Microsoft Exchange Server.

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

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

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

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

---

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

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

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

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

5 Exit the Registry Editor.

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.

VCW is unable to add a new node to a secure cluster (623540)

Under certain conditions, such as, when the node name is modified, VCW wizard is unable to add a new node to an existing secure cluster. This is specifically observed in an Exchange environment. When the Exchange pre-installation completes the Exchange virtual server values are temporarily assigned to the node. All network connections to the node are made using the temporary name. After the pre-installations completes, the system is rebooted and the Symantec Product Authentication Service (`vrtsat`) reassigns the root credentials based on the new root domain (new virtual server name) in the Root Broker Hash file.

However, post Exchange installation the system name is reassigned back to its actual physical name, and the root credentials used are reverted back to the original root domain (physical node name) which is not however updated in the Root Broker Hash file. Due to the ambiguous credentials the new node is unable to be added.

Workaround: When setting up and configuring Exchange, prior to renaming the Exchange Virtual Server (EVS) stop the Symantec Product Authentication Service (`vrtsat`) and change the startup mode to `manual` and then restart it. After the system name reverts back to the original name, set the `vrtsat` service back startup mode to `automatic`.

Cluster operations fail if an Exchange service group is online in a secure cluster

If an Exchange service group is online on a node in a secure cluster, cluster operations using `ha` commands or Cluster Manager (Java Console) fail to execute on that node.

Workaround: Perform cluster operations on nodes where the Exchange service group is not online. For cluster operations specific to a node where the service group is online, use the `hasys` command and arguments.

Changes made to the Exchange domain controller configuration settings do not appear when the Exchange virtual server is failed over to another node (263417)

If you are upgrading a setup that is configured with SFW HA 4.3 for Exchange (or earlier versions), to use SFW HA 4.3 MP1 or later versions, then the RegRep resource is not automatically updated with an attribute for the registry key: HKLM\\SYSTEM\\CurrentControlSet\\Services\\MSExchDSAccess

In this situation, if the Exchange Virtual Server (EVS) fails over to another node in the cluster, then any Domain Controller configuration changes that were made when the Exchange service group was online on the first node are not visible on the failed-over node.

Workaround: Use the Java Console, Web Console, or the hares command to update the RegRep resource with an attribute for the MSExchDSAccess key that is present at:
HKLM\\SYSTEM\\CurrentControlSet\\Services\\MSExchDSAccess

Note: If the setup is configured for disaster recovery then you must ensure that the RegRep resource on the primary as well as the secondary cluster is updated to include the attribute for the MSExchDSAccess registry key.

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 5.0 with Oracle

The following issues apply to VCS 5.0 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 5.0 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.

VCS with NetBackup

NetBackup Wizard may fail to bring service group online

Occasionally, the NetBackup Configuration wizard reports an error on the final screen, and the NetBackup service group does not come online.

Workaround: In the final screen of the NetBackup wizard, clear the check box for bringing the service group online, then Finish. Use Cluster Manager or the command line interface to bring the service group online.

Cannot failover after installing NetBackup on an SFW HA cluster (866167)

After installing NetBackup 6.0 GA, 6.0 MPx, or 6.5 on an SFW HA 4.3, 4.3 MP1, or 5.0 cluster and creating a NetBackup service group, the service group comes online successfully. However, switching the service group to another node in the cluster will not succeed.

Workaround: Before attempting to switch or failover the NetBackup service group, reboot the nodes in the cluster that are not hosting it. After the rebooted nodes are brought online, switch the NetBackup service group to another node in the cluster and then reboot the first node.

Other issues

PrintSpool resource may fail to come online (311724)

On Itanium-based systems or 64-bit systems running Windows Server 2003 x64 Edition, the PrintSpool resource occasionally fails to come online during the Add Printer procedure of the PrintShare configuration wizard.
Workaround: From Cluster Explorer, disable the PrintSpool resource. Re-enable the PrintShare resource and then bring it online. Return to the PrintShare wizard to add the printer and continue the configuration process.

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 onlines 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.

IIS Configuration Wizard crashes if IIS is not installed (863043)

The IIS Configuration Wizard crashes if you run the wizard on a node on which IIS is not installed.

Fatal error (BSOD) in GAB (645728)

In a cluster setup on a VMware ESX Server configuration, one of the nodes encounters a fatal error (BSOD). This issue is observed when the cluster receives corrupt LLT packets.

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.

Workaround: Currently, no workaround is available for this issue.

NetBackup Wizard may fail to bring service group online

Occasionally, the NetBackup Configuration wizard reports an error on the final screen, and the NetBackup service group does not come online.

Workaround: In the final screen of the NetBackup wizard, clear the check box for bringing the service group online, then Finish. Use Cluster Manager or the command line interface to bring the service group online.

In VCW, the Notifier and the Web Console cannot be set to use same NIC resource (894979)

If you have already configured the cluster service group and are preparing to configure the notification options, you will not be able to select the same NIC resource as the cluster service group in the VCW Notifier Card Selection window.

Workaround: In the Notifier Card Selection window, select the Create new NIC resource for "Notifier Manager" option and select the appropriate adapter in the select adapter box. This workaround will create a duplicate NIC resource in the main.cf file. You can then use the Java GUI to delete this duplicate NIC resource

and set the notification resource dependency on cluster service group NIC resource.

Lanman resources fail to come online if multiple Lanman resources depend on the same IP resource (493266)

On x64 platforms, if you configure multiple Lanman resources such that all the Lanman resources depend on the same IP resource, the Lanman resources will fail to come online. Typically, only one Lanman resource may come online.

Veritas Volume Replicator

This section provides information on known Volume Replicator issues.

The execution frequency documented for the VVR Objects Discovery Data and the VVR Object State Monitoring Data scripts run is incorrect.

In the Monitoring and Reporting chapter of the Veritas Storage Foundation™ and High Availability Solutions Management Pack Guide for Microsoft Operations Manager 2005, the run frequency documented for the VVR Objects Discovery Data and the VVR Object State Monitoring Data scripts run is incorrect.

In the VVR State view section:

- The VVR Objects Discovery Data script collects data every 15 minutes not every 5 minutes as stated.
- The VVR Object State Monitoring Data script collects data every 9 minutes not every 3 minutes as stated.

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 further details, see 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\constantsversion\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.

RDS Displayed as Noname

- Performing the following operations on a setup with VVR may result in an RDS being displayed as `Noname`. (273418)
  - Disconnecting VEA from the local host and then connecting it again.
  - In a VCS cluster, taking the replication group offline and bringing it online on the same node.
  - On an MSCS cluster, performing a move group operation to move the replication group from one node to another, and then moving the group back to the original node.

  Workaround: Close VEA using **File** > **Exit** and then restart it.

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
```

Disaster Recovery Configuration Wizard

Storage cloning does not complete if the disks that are on the non-shared bus are selected (704021)

The Disaster Recovery Configuration Wizard is unable to distinguish between the shared and non shared disks at the secondary site. As a result, on the Disk Selection for Storage Cloning panel the wizard allows selection of such disks that are not on the shared bus. The wizard goes through the storage cloning wizard completely and displays (**x**) symbols on the implementation panel indicating unsuccessful completion of the cloning task. The cluster disk group is not created in this case.

Workaround: Symantec recommends that you select only the shared disks; otherwise the storage cloning may not succeed. If there are disks on the non-shared bus that the wizard has selected, then make sure you unselect these disks and select only the disks that exist on the shared bus.

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.

Secondary RVG fails if you specify the same name for the primary and secondary RLINK (855170)

When you are running the Disaster Recovery Wizard to configure replication, you can optionally specify a primary RLINK name and a secondary RLINK name, using the Advanced Settings option from the Replication Settings panel. If you specify the same name for both the primary and secondary RLINK, the secondary RVG creation will fail.

Workaround: Rerun the Disaster Recovery Wizard and ensure that you specify a different name for the primary and secondary RLINK.

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 already created the storage layout at the secondary site and installed the application, only use the DR wizard 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 you had 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.

Storage cloning may time out on a large mirrored volume and fail to create any subsequent volumes (893550)

When you are running the Disaster Recovery Wizard to clone the storage, the cloning may time out during cloning of a large mirrored volume and the wizard fails to clone any subsequent volumes. However, no error is displayed and the wizard allows you to continue with service group cloning. The final task of the wizard is configuring VVR replication and/or the global cluster option. Only at this stage is an error message displayed about the missing volumes.

Workaround: If you discover that not all volumes were cloned successfully, run the Disaster Recovery Wizard again. It will discover the missing volumes and clone them.

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.

Fire Drill Wizard

The Fire Drill Wizard does not delete the DCO log volume when deleting a fire drill configuration (837702)

When you select the option in the Fire Drill Wizard to delete the fire drill configuration, the wizard performs a snap abort of the snapshot mirrors created on the secondary site, deleting the mirror volumes. However the DCO volume associated with the snapshot mirror is not deleted. If you prepare the same volume for a fire drill at a later date, the DCO volume is re-used.

Workaround: If desired, you can delete the DCO volume using the `vxassist remove log` command.

The Fire Drill Wizard may give an SFW discovery error if the replication service group has been switched between systems on the secondary site (843076)

In the Fire Drill Wizard, the Restore to Prepared State operation and the Delete Fire Drill Configuration operation may fail if the replication service group has been switched back and forth between cluster systems on the secondary site. The wizard displays the error that it failed to discover SFW components.

Workaround: In the Veritas Enterprise Administrator console, connect to the system you had selected in the wizard and do a rescan (right-click the storage agent and click **Rescan**). Then restart the wizard.

The 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 is has at least 15 GB free.

Workaround: Assign volumes to separate disks or ensure that if more than one volume is assigned to the disk that the disk is large enough to accommodate all the volumes assigned.

Software fixes and enhancements

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

Veritas Storage Foundation

Table 1-6 Fixed issues for Storage Foundation for Windows

Incident Number	Description
83939	Java Incompatibility with Video Card May Cause System Hang
87768	High I/O Rate May Fill Volume Before Volume Growth Is Triggered
101524	SFW Does Not Support the Latest Released Driver for Emulex HBAs
102456	SFW Does Not function properly after uninstalling Dell OpenManage Array Manager
103239	Expand Volume May Cause Error When Used with Replication
103381	Microsoft Server Appliance Kit Does Not Recognize SFW Dynamic Volumes
160437	Resources to offline before recovery of an Exchange Storage Group in an MSCS environment
257804	Incomplete Point-of-Failure Recovery of a SQL Database
264112	Snapshots for off-host backup with Backup Exec 10.0 may cause backup job to fail
304139	VEA May Sort Disks Incorrectly after Destroying Dynamic Disk Group
311816	Display of VEA on Asian Operating Systems May Require Font Adjustment
373467	"SCSI-3 Reserved" attribute does not get updated after a primary path failure and recovery
425390	I/O Failures Occur When Using the Active/Active SCSI-3 Mode of MPIO DSMs on an EMC Symmetrix Array
431949	VEA GUI Hangs System During Rescan Operation
492852	The resynchronization of volumes cannot be disabled in Rescan command
499290	Incorrect Version Displayed by Device Manager After Upgrading to SFW 4.3 with Dynamic Multipathing
589653	Creating mirror with CLI command after configuring task performance, results in CLI command returning before all tasks finish
603045	VDS and iSCSI providers hang at startup

Table 1-6 Fixed issues for Storage Foundation for Windows (Continued)

Incident Number	Description
617880	Creating striped volume across different ports may not yield expected stripe layout
626424	Java GUI displays folder icons under iSNS
625558	Java GUI does not display some fields correctly in the drive table
629899	iSCSI enclosures do not appear in the Array Capacity Usage Report
632247	One VSS snapshot fails when two Exchange components scheduled at same time
632793	CLI commands may fail with error message stating PBX Acceptor cannot be opened
635025	Unable to set IPsec tunnel addresses
636425	Storage utilization does not appear in the Web GUI
636812	VxBridge executable causes increased memory use over time
637581	Changing system time does not enable VSS snapshot to be scheduled
640501	The iSCSI target does not appear in GUI after rebooting
640541	Target number increases by one after an alias is defined
643041	No data under iSCSI or fibre channel attached storage array in GUI
643994	Managing summary for HBAs is empty in the Web GUI
644662	Scheduled QR snapshots fail if an incorrect pre-script name is submitted using the Quick Recovery Wizard
645820	VDS command line interface, DISKPART, cannot convert basic disk to dynamic disk
646921	System hung after installing SFW
647322	Default layout setting when creating mirror does not match layout of source volume
701155	Information about volumes contained in OEM partitions may not display correctly in VEA GUI
701336	VEA fails after restarting vxob service
704644	VSS scheduler fails when two subcomponents of Exchange storage group reside on same volume
766106	After failover in MSCS environment, Snap Prepare Volume does not resynchronize
767238	For SQL 2005, the implementation of the Recovery and No Recovery options is reversed in vxsnap from the vxsnapsql implementation for SQL 2000

Veritas Cluster Server

Concurrency violation with online firm dependencies

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

Other fixed issues

The following issues were fixed in this release.

Table 1-7 Fixed issues for Veritas Cluster Server

Incident Number	Description
582351	Error Bringing Mount Points Online After Power-Off
425035	Use a Valid Script File for Detail Monitoring
603211	DNS Scavenging Affects Virtual Servers Configured in VCS
582837	On a Japanese locales, Selection panel of the VCW wizard displays distorted system selection panes
515644	hacf does not handle MAXARG values of vector/associative attributes in the main.cf.
584243	hares options do not filter correctly.
426932	Indeterministic service thread cancellation.
271167	Provide finer control over the hastop -all command.
603107	SQL OLAP service fails to come online.
348647	Installation order of SQL Server 2005 affects MSSearch.
367950	Automatic Change Tracking of SQL 2005 catalogs prevents failover of service group.
310020	SQL Server 2005 resource may go into unknown state
703925	Resync action for MirrorView agent does not resynchronize mirrors in a fractured or consistent state.
765323	AddArrayUser action for the MirrorView agent fails on x64 systems.
312350	Error installing printer drivers.
765954	HAD may give warning message and fail to restart.

Veritas Volume Replicator

The following issues were fixed in this release.

Table 1-8 Fixed issues for Veritas Volume Replicator

Incident Number	Description
128824	VxSAS Wizard is Not Launched Automatically After Installation
312243	Autogrow May Fail if Autogrow-Enabled Volumes are Included in RDS
310980	Volume Replicator Agent Configuration Wizard Does Not Exit
493942	Secondary Volumes Need to be Resynchronized after a System Reboot
634780	Unable to failover the RVG Resource to another node in the cluster

Documentation changes

See http://entsupport.symantec.com/docs/285845 for a complete list of changes to the product documentation as well as other late-breaking news.

The information in this section updates information provided in the product documentation.

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

Recovering using snapshots and log replay page 122

In the procedure for recovering with log replay, step 8 on page 123 is changed to clarify how to specify the log backups:

8. On the Select Restore Type panel, do the following and click Next:

- Click Recovery + Log replay.
- In the Log file names field, type the full path of the first log backup to be applied and press Enter.

- Repeat for each additional log backup, in the order that they are to be applied.

Veritas Storage Foundation Administrator's Guide

Configuration backup page 115

In the description for the Automatic Checkbox of Configuration Backup that describes the number of minutes between backups on page 115, replace:

"This setting is ignored when Automatic is selected." with

"This setting is ignored when Automatic is not selected.".

CLI command vxcbr backup page 373

The description for the vxcbr backup CLI command on page 373 is changed to include information about the default path to store the configuration.

Replace:

"Specifies the path to the directory where the configuration information will be archived."

with

"Specifies the path to the directory where the configuration information will be archived. The default path is %ALLUSERSPROFILE%\Application Data\VERITAS\VXCBR\ManualCBR".

Restoring the SQL database with recovery and logs page 581

The procedure to restore a SQL database with recovery and logs on page 581 is changed to the following:

To use log replay for an automatic roll-forward recovery to a point of failure using the VEA

1. Ensure that you have backed up the transaction logs within SQL Server using the "overwrite existing media" option to create uniquely-named backup files.
2. Close the SQL GUI and all Explorer windows, applications, consoles (except the VEA), or third-party system management tools that may be accessing the volumes. It is also recommended to bring the database offline.
3. From the VEA console, navigate to the system where the database volumes are located.
4. Expand the system node, the Storage Agent node, and the **VSS Writers** node.

5 Right-click **SQLServerWriter** and click **VSS SQL Restore**.

6 Review the Welcome page and click **Next.**

7 Select the snapshot set XML metadata file to be used for this operation and click **Next**.
The XML metadata file contains all required information needed to restore the snapshot set, including the names of the database and transaction logs volumes. Click the appropriate header to sort the list of available files by **File Name** or **Creation Time**.

8 On the Select Restore Type panel, do the following and click Next:
- Click **Recovery + Log replay.**
- In the Log file names field, type the full path of the first log backup to be applied and press Enter.
- Repeat for each additional log backup, in the order that they are to be applied.

9 You may receive a message “Some volumes in this component have open handles. Do you want to override these handles and do this restore? Click **Yes** to proceed.” Click **No**, close any open handles and retry the command.

10 Verify the restore specifications and click **Finish**.
After the most recent backup log is replayed, the SQL Server database is closed and left in an operational state. If you took it offline earlier, bring it back online.

11 The restore operation leaves the snapshot volumes snapped back to the production volumes. To ensure that another split-mirror snapshot set is immediately available, use the VSS Snapshot Wizard to create a new snapshot of all the volumes in the database.

Documentation

Storage Foundation for Windows documentation is included on the product software discs for the Veritas Storage Foundation and High Availability Solutions 5.0 for Windows release in Adobe Portable Document Format (PDF) in the `\Docs` directory. To view a document, explore the software disc and double-click the file name.

Note: Updated Release Notes can be found at http://entsupport.symantec.com/docs/285845

Table 1-9 Veritas Storage Foundation and High Availability Solutions for Windows Documentation Set

Title	File Name
Veritas Storage Foundation and High Availability Solutions	
Veritas Storage Foundation and High Availability Solutions 5.0 Getting Started Guide	SFW_GettingStarted.pdf
Veritas Storage Foundation and High Availability Solutions 5.0 Installation and Upgrade Guide	SFW_InstallUpgrade.pdf
Veritas Storage Foundation and High Availability Solutions 5.0 Release Notes	SFW_ReleaseNotes.pdf
Veritas Storage Foundation and High Availability Solutions 5.0 Solutions Guide	SFW_Solutions.pdf
Veritas Storage Foundation and High Availability Solutions 5.0 HA and Disaster Recovery Solutions Guide for Microsoft Exchange	SFW_HA_DR_Exch_Solutions.pdf
Veritas Storage Foundation and High Availability Solutions 5.0 Quick Recovery and MSCS Solutions Guide for Microsoft Exchange	SFW_QR_MSCS_Exch_Solutions.pdf
Veritas Storage Foundation and High Availability Solutions 5.0 HA and Disaster Recovery Solutions Guide for Microsoft SQL	SFW_HA_DR_SQL_Solutions.pdf
Veritas Storage Foundation and High Availability Solutions 5.0 Quick Recovery and MSCS Solutions Guide for Microsoft SQL	SFW_QR_MSCS_SQL_Solutions.pdf
Veritas Storage Foundation	
Veritas Storage Foundation 5.0 Administrator's Guide	SFW_Admin.pdf

Table 1-9 Veritas Storage Foundation and High Availability Solutions for Windows Documentation

Title	File Name
Veritas Cluster Server	
Veritas Cluster Server 5.0 Administrator's Guide	VCS_Admin.pdf
Veritas Cluster Server 5.0 Agent Developer's Guide	VCS_AgentDev.pdf
Veritas Cluster Server 5.0 Bundled Agents Reference Guide	VCS_BundledAgents.pdf
Veritas Cluster Server 5.0 Application Note: Disaster Recovery for Microsoft SharePoint Portal Server 2003	VCS_AppNote_Sharepoint.pdf
Veritas Cluster Server 5.0 Application Agent for Microsoft Exchange, Configuration Guide	VCS_Exch_Agent.pdf
Veritas Cluster Server 5.0 Database Agent for Oracle, Configuration Guide	VCS_Oracle_Agent.pdf
Veritas Cluster Server 5.0 Database Agent for Microsoft SQL, Configuration Guide	VCS_SQL_Agent.pdf
Veritas Cluster Server 5.0 Hardware Replication Agent for EMC SRDF, Configuration Guide	VCS_SRDF_Agent.pdf
Veritas Cluster Server 5.0 Hardware Replication Agent for Hitachi MirrorView, Configuration Guide	VCS_MirrorView_Agent.pdf
Veritas Cluster Server 5.0 Hardware Replication Agent for Hitachi TrueCopy, Configuration Guide	VCS_TrueCopy_Agent.pdf
Veritas Cluster Server 5.0 Hardware Replication Agent for IBM Metro Mirror, Configuration Guide	VCS_MetroMirror_Agent.pdf
Veritas Cluster Server 5.0 Hardware Replication Agent for IBM PPRC, Configuration Guide	VCS_PPRC_Agent.pdf
Veritas Cluster Management Console	
Veritas Cluster Management Console 5.0 Implementation Guide	VCMC_Implementation.pdf
Veritas Cluster Management Console 5.0 Release Notes	VCMC_Notes.pdf
Veritas Volume Replicator	
Veritas Storage Foundation 5.0 Volume Replicator, Administrator's Guide	VVR_Admin.pdf

Table 1-9 Veritas Storage Foundation and High Availability Solutions for Windows Documentation

Title	File Name
Veritas Storage Foundation 5.0 Volume Replicator Advisor, User's Guide	VVR_Advisor.pdf
Symantec Product Authentication Service	
Veritas Storage Foundation and High Availability Solutions 5.0 Quick Start Guide for Symantec Product Authentication Service	SPAS_QuickStart.pdf
Symantec Product Authentication Service 4.3 Administrator's Guide	SPAS_AT_Admin.pdf
Symantec Product Authentication Service 4.3 Release Notes	SPAS_AT_ReleaseNotes.pdf

PDF copies of the product guides are also available on the Symantec Support website at http://entsupport.symantec.com/

Documentation feedback

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions to sfwha_solns_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://entsupport.symantec.com.