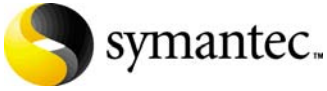
Veritas Storage Foundation™ and High Availability Solutions for Windows Release Notes

5.0 Rollup Patch 2



Veritas Storage Foundation and High Availability Solutions for Windows
Release Notes

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

Product version: 5.0 Rollup Patch 2

Document version: 5.0 RP2.2

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information

- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support web page at the following URL:
www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:
www.symantec.com/business/support/
Customer Service is available to assist with non-technical questions, such as the following types of issues:

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

Support agreement resources

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

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Veritas Storage Foundation and High Availability Solutions Release Notes

Introduction

This document provides important information about the Veritas Storage Foundation and High Availability (HA) Solutions 5.0 Rollup Patch 2 for Windows. Review this entire document before installing this patch.

Rollup Patch 2 (RP2) supersedes Rollup Patch 1a (RP1a) and includes all the fixes and enhancements provided in RP1a.

This document includes all the applicable information in the RP1a ReadMe. It lists separately the new fixes and enhancements provided with RP2.

This rollup patch applies to the products shown in the following table.

Table 1-1 Product software supported for Rollup Patch 2

Product	Versions
Veritas Storage Foundation for Windows	5.0 5.0 Rollup Patch 1a
Veritas Storage Foundation HA for Windows	5.0 5.0 Rollup Patch 1a
Veritas Cluster Server for Network Appliance SnapMirror	5.0 5.0 Rollup Patch 1a 5.0 Release Update 1

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

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

Changes introduced in the RP2 release

This section describes the changes introduced in the RP2 release. RP2 also includes the changes that were introduced earlier in the RP1a release. These changes are covered separately.

See “Changes introduced in the RP1a release” on page 17.

Updated MountV agent

This release includes an updated MountV agent. The update is related to the CheckFSAccess function of the MountV agent.

CheckFSAccess is a MountV agent function that allows you to enable or disable MountV agent's file system access monitoring on volumes mounted using SFW. CheckFSAccess is enabled by default.

The CheckFSAccess function has been enhanced to allow granular control on the behavior of MountV resources.

To enable or disable the CheckFSAccess function for a specific MountV resource, run the following command

```
hares -action <MountV_resource_name> CheckFSAccess -actionargs
<arg1> [<arg2>] -sys <system_name>
```

The parameters included in the command are as follows:

- <MountV_resource_name> is the name of the MountV resource.
- <arg1> can take a value of 1 or 0.
  Setting this to 1 enables file system check; setting this to 0 disables it. The default value is 1 (enabled).
- [<arg2>] can take a value of 1 or 0, and is optional.
  Setting this to 1 indicates that the <arg1> setting is persistent in the cluster. The <arg1> setting remains in effect even if you restart the Veritas High Availablity Engine (HAD).
  Setting this to 0 indicates that the <arg1> setting is non-persistent and is reset to the default value of 1, whenever the Veritas High Availability Engine (HAD) is restarted.
- <system_name> is the name of the cluster node on which the MountV resource is configured to fail over.

The changes take effect on the next agent monitor function. Repeat the command for each system that the specified MountV resource is configured to fail over. You can run the command from the same node; replace <system_name> with the cluster node name. The change takes effect when the MountV resource is brought online on those nodes.

To enable or disable the CheckFSAccess function for all MountV resources on a cluster node simultaneously

Perform these steps if you wish to disable file system access monitoring globally, across a cluster. It will apply to all the MountV resources in the cluster.

Note: In a case where file system access monitoring is disabled for all MountV resources using this procedure, but is enabled for a MountV resource individually, then the setting for MountV resource takes precedence. The agent performs file system access monitoring for the volume configured in the MountV resource.

Perform the following steps on each cluster node, one node at a time.

1. Make a backup copy of the registry.
2. To open the Registry Editor, click **Start > Run**, type **regedit**, and then click **OK**.
3. In the registry tree (on the left), navigate to `HKEY_LOCAL_MACHINE > SOFTWARE > Veritas > VCS > BundledAgents`.
4. Click **Edit > New > Key** and create a key by the name **MountV**, if it does not exist already.
5. Select MountV and then click **Edit > New > Key** and create a key by the name __GLOBAL__. (underscore-underscore-GLOBAL-underscore-underscore)
6. Select __GLOBAL__ and add a DWORD type of value.
7. Specify Value name as CheckFSAccess and Value data as follows:
   - Set the value to 0 to disable CheckFSAccess.
   - Set the value to 1 to enable disable CheckFSAccess.

   The specified setting applies to all the MountV resources on the cluster node.
8. Save the changes and exit the Registry Editor.

VCW support to configure LLT over UDP

In this release the VCS Cluster Configuration Wizard (VCW) includes support for configuring Low Latency Transport (LLT) over the User Datagram Protocol (UDP) layer.

While configuring the cluster using this wizard, you can now configure LLT over UDP.

See "Configuring LLT over UDP" on page 44.

Wizard support to upgrade Exchange 2007 to Exchange 2007 SP1

This release includes the Exchange 2007 Upgrade Wizard for VCS. You can use this wizard to upgrade Exchange 2007 to Exchange 2007 SP1, in a VCS cluster environment.

If you already have Exchange 2007 set up in a VCS cluster and wish to upgrade Exchange 2007 to Exchange 2007 SP1 using the wizard, you must first install RP2, then install the updated VCS agent for Exchange 2007, and then proceed with the Exchange upgrade.

See "Installing the rollup patch using the GUI" on page 32.

See "Installing support for Microsoft Exchange Server 2007" on page 40.

See "Upgrading Exchange 2007 to Exchange 2007 SP1" on page 45.

Updated VCS Management Packs for MOM 2005

The VCS management packs have been updated to include fixes for the following issues:

- This issue occurs in a disaster recovery configuration with Microsoft Operations Manager (MOM) 2005 deployed to monitor nodes at both the primary and the secondary sites. After importing the VCS MOM packs, the MOM server is flooded with resource and service group offline alerts. These alerts came from nodes at the secondary site (DR site) where the service groups and the resources were offline. In the MOM console, these alerts show up as critical alerts, thereby requiring administrative attention.
  With this release, the resource and service group offline alerts now appear as informational messages and do not require any administrative action.
- In a VCS cluster with a MOM 2005 monitoring environment, the VCS state monitoring script logs alerts for all resources in a service group whenever there is a change in the state of any resource/service group. This results in a large number of alerts on the MOM server.
  With this release, the alerts are generated only for the resource/service group whose state has changed.
- On a MOM 2005 SP1 server, when a service group is taken offline from online state or online from offline state, if VCS MOM script is called during the transition period, the state monitoring script generates alerts.
  With this release, the state monitoring script does not initiate alerts during fail over of a service group when the service group is in partial starting or partial stopping state.

See "Importing the VCS Management Pack" on page 43.

VEA support for a configurable port range for PBX

The default port for PBX is 49162. In certain environment configurations, a conflict for this port may occur. To resolve the port conflict, you can change the port range for PBX.

To configure the port range for PBX, a Windows registry key must be added for vxsvc and agents.

- For vxsvc, add the registry key under
  \HKEY_LOCAL_MACHINE\Software\Veritas\VxSvc\CurrentVersion\Network\Params\Security
  with the following:
  - type = REG_SZ
  - name = CLIENT_PORT_RANGE
  - value in the form X-Y, where X and Y are numeric values and Y > X.
- For agents, add the registry key under
  \HKEY_LOCAL_MACHINE\Software\Veritas\VRTSobc\pal33\Agents\<agentname>\Network\Params\Security
  where <agentname> is the name of the agent, such as StorageAgent, gridnode, actionagent, etc.

Note: If the registry key is not present, then port range 49162-65535 is assumed.

Changes introduced in the RP1a release

This section describes changes introduced in the RP1a release.

These changes also apply in the RP2 release.

Any changes introduced in the RP2 release are covered separately.

See "Changes introduced in the RP2 release" on page 13.

New version of VCS Management Console

An updated version of Veritas Cluster Server Management Console is available for use with Storage Foundation and High Availability Solutions 5.0 RP1a. VCS Management Console 5.1 is compatible with SFW HA 5.0 RP1a.

Enhanced support for Microsoft Exchange Server 2007

The following are enhancements to support Microsoft Exchange Server 2007:

- SFW supports VSS-based backup and restore operations with Exchange 2007.
  See "SFW support for VSS operations with Microsoft Exchange Server 2007" on page 18.
- SFW HA supports Exchange 2007 (including Service Pack 1).
  SFW HA support for Exchange 2007 is available for the Mailbox Server role only.
  Refer to the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange 2007* to configure a new HA and DR environment for Exchange 2007.

  Note: The Solutions Configuration Center does not provide a workflow to configure Exchange Server 2007.

  If you already have Exchange 2007 set up in a VCS cluster and wish to upgrade Exchange 2007 to Exchange 2007 SP1 you must first install SFW HA 5.0 RP1a, then install the updated VCS agent for Exchange 2007, and then proceed with the Exchange upgrade.
  See "Installing the rollup patch using the GUI" on page 32.
  See "Installing support for Microsoft Exchange Server 2007" on page 40.
  See "Upgrading Exchange 2007 to Exchange 2007 SP1" on page 45.

SFW support for VSS operations with Microsoft Exchange Server 2007

For Exchange 2007, SFW continues to support a set of VSS operations based on Flashsnap as it did with earlier releases of Microsoft Exchange. Applying this patch addresses issues in the following:

- VEA GUI
- MSCS environment
- VCS environment
- Using a Snapshot of a Replica for Database Recovery

In addition, this release provides support for the Microsoft VSS Writers when the Local Continuous Replication (LCR) and Cluster Continuous Replication (CCR) features of Exchange 2007 are enabled.

VEA GUI

If replication is enabled for Exchange 2007, the VEA GUI does not display the hierarchy of active store writers and replica store writers correctly. After applying this patch and enabling replication for Exchange 2007, the display of the Microsoft Exchange Replication Service instance of the Microsoft Exchange Writer is enabled and displayed correctly. It appears as the Microsoft Exchange Writer Replica in the VEA GUI and is displayed in the tree view of the VEA subordinate to the VSS Writers node.

Right-clicking the Microsoft Exchange Writer Replica node displays a context menu that shows VSS Snapshot, VSS Snapback, and VSS Refresh selections. Restoring the replica with the VSS Restore operation and the Schedule VSS Snapshot operation for the replica are not supported.

No other changes are made to the VEA GUI or to the SFW wizards after applying this patch.

- The Prepare command is required before using VSS Snapshot. For more information about snapshots, see the *Veritas Storage Foundation Administrator's Guide*.
- The Quick Recovery wizard in the Solutions Configuration Center does NOT support Exchange 2007. For more information about Quick Recovery using Microsoft Exchange 2003, see the *Veritas Storage Foundation and High Availability Solutions Quick Recovery and MSCS Solutions Guide for Microsoft Exchange*.

MSCS environment

In an MSCS environment, you have to manually set the dependency of the Microsoft Exchange database instance to the Volume Manager Disk group resource so that it fails over in the correct sequence.

VCS environment

SFW supports the VSS operations based on Flashsnap in a VCS environment. However, the name of the Exchange Virtual Server was not recognized. After applying this patch, the Exchange Virtual Server name appears as the VCS Resource name for Exchange 2007.

vxsnap CLI command

After applying this patch and enabling replication for Exchange 2007, a new vxsnap CLI command option is made available to take a snapshot of a Microsoft Exchange Writer Replica (Microsoft Exchange Replication Service instance of the Microsoft Exchange writer) or of a Microsoft Exchange Writer (Microsoft Exchange Service instance of the Microsoft Exchange writer).

In the command, you can specify the replica store writer to take the snapshot of the replica or the active store writer to take the snapshot of the active store. If the replica store writer or the active store writer is not specified, then "Microsoft Exchange Writer" is used as a default.

For example:

```
vxsnap -x snapdata.xml create writer="Microsoft Exchange Writer
Replica" component=SG1 backupType=COPY -E -O
```

specifies that the VSS Writer, Microsoft Exchange Writer Replica, is used to take a snapshot of the replica.

Note: The Prepare operation must be completed on the volumes that contain the replica before taking a snapshot of a replica. This can be done using the VEA GUI or the `vxsnap prepare` CLI command. When using the CLI, the `vxsnap prepare` command must specify the Microsoft Exchange Writer Replica.
For example:

```
vxsnap prepare component=SG1/writer="Microsoft Exchange
Writer Replica" source=L:/harddisk=harddisk2
```

For more information about `vxsnap` command, see the *Veritas Storage Foundation Administrator's Guide.*

Using a Snapshot of a Replica for Database Recovery

A snapshot of a replica can be used to restore an Exchange database to the point of failure (POF) or be used to restore a complete Exchange storage group to a point in time (PIT).

Taking a snapshot of a replica can be done with the VEA GUI by using the VSS snapshot wizard or with the vxsnap CLI command (described above). Taking a snapshot of a replica automatically takes a snapshot of all the volumes that the replica uses.

To restore the database from a snapshot of a replica, you must first manually perform a "Restore-StorageGroupCopy" on the storage group, and then perform the restore on the active writer. (The restore operation on the replica store writer is not supported.)

Originally for SFW 5.0, a manual dismount of the database was required before the restore operation. After applying this patch, the dismount of the database is automatically done as a part of the restore operation. (For the `vxsnap restore` CLI command, specify the `-a` option to dismount the database.)

Note: In a VCS environment, applying this patch automatically dismounts the database and sets the database for overwrite by restore as a part of the restore operation. However in an MSCS environment, a manual dismount of the database and manually setting the database for overwrite by restore are both required.

Note: When SFW 5.0 fails to automatically dismount the database during a restore operation, the restore operation fails. The restore operation can be performed again after manually dismounting the databases and manually setting the databases for overwrite by restore. If LCR or CCR was previously enabled, then it must be suspended before performing the restore operation again.

To perform the restore on the active writer, use the Exchange Management shell to execute the following cmdlets:

- Dismount Database cmdlet
  ```
  dismount-Database -Identity <DatabaseIdParameter>
  [-DomainController <Fqdn>]
  ```
- RestoreStorageGroupCopy cmdlet
  ```
  Restore-StorageGroupCopy
  -Identity:<Server>\<StorageGroupName>
  -ReplaceLocations
  ```
  Additional considerations when running the RestoreStorageGroupCopy cmdlet:
  - The LCR copy is automatically disabled when running the Restore-StorageGroupCopy cmdlet
  - If a schedule for snapshots exists for the active store, running the RestoreStorageGroupCopy cmdlet makes the schedule invalid. The schedule becomes invalid because it no longer has updated volume/plex information to take the snapshot. In this situation, the

user must delete the invalid schedule before performing the restore operation.

For more information about the Exchange Management shell and cmdlets, refer to the Microsoft Exchange 2007 product documentation.

After completing the "Restore-StorageGroupCopy" on the storage group, you would use the VSS restore wizard or the vxsnap restore command to complete the recovery operation.

Note: Although applying this patch allows you to restore the database from a snapshot, restoring just the database log files is not supported by this patch.

An example of a PIT recovery procedure from a snapshot of a replica of an Exchange storage group, SG1, that contains two databases, DB1 and DB2, on an Exchange server, TestExch, would be as follows:

1. Run Dismount Database cmdlet on DB1 and DB2 databases.
   ```
   Dismount-database -Identity TestExch\SG1\DB1
   Dismount-database -Identity TestExch\SG1\DB2
   ```
2. Run RestoreStorageGroupCopy cmdlet on SG1 storage group.
   ```
   Restore-StorageGroupCopy -Identity TestExch\SG1
   -ReplaceLocations
   ```
3. Run Mount Database cmdlet on DB1 and DB2 databases.
   ```
   Mount-database -Identity TestExch\SG1\DB1
   Mount-database -Identity TestExch\SG1\DB2
   ```
4. Perform refresh.
   ```
   vxsnap refresh
   ```
5. Perform VSS restore operation using snapshot of replica.
   ```
   vxsnap -x snapdata.xml restore RestoreType=PIT
   writer="Microsoft Exchange Writer"
   ```

   Note: For this example, assume that the snapshot of the replica was performed with
   ```
   vxsnap -x snapdata.xml create writer="Microsoft
   Exchange Writer Replica" component=SG1 backupType=COPY
   -E -O
   ```

For an MSCS environment, there are additional considerations when restoring the database.

- After performing the refresh operation, the user must manually dismount the databases before performing the restore operation.

- If CCR is enabled, then the user must disable the circular logging feature before restoring the database.

Client support on Windows Vista

SFW 5.0 and SFW HA 5.0 client components are supported on the Windows Vista operating system.

See "Post installation tasks" on page 42.

Compatibility between SFW 5.0, SFW 5.0 RP1a, and Storage Foundation Manager 1.1.0.0

A patch (upgrade_SFW50.bat) ships with Storage Foundation Manager (SF Manager) 1.1.0.0. This patch provides a fix for a limitation that prevents you from converting your standalone SFW 5.0 hosts to managed hosts that are discovered and monitored by a SF Manager Management Server. After you apply the patch to a SFW 5.0 host, you can add the host to a SF Manager management domain. The host is thereafter identified as a managed host.

Apply the upgrade_SFW50.bat patch only to SFW 5.0 hosts. If you upgrade your SFW 5.0 host to SFW 5.0 RP1a, you should not apply the upgrade_SFW50.bat patch. If you have already applied the patch to your SFW 5.0 host, you can upgrade the host to SFW 5.0 RP1a. Upgrading to SFW 5.0 RP1a does not affect the earlier application of the patch. You can convert a standalone SFW 5.0 RP1a host to a managed host without any additional steps.

See the *Storage Foundation Manager Administrator's Guide* for more information about converting standalone SFW hosts to managed hosts.

VCS Management Pack changes for MOM 2005

The VCS Management Pack will not display any Information messages. Only Error, Warning, and Success states will be reported on the MOM server. The MOM server displays the service group state for the node, if service group is online, partially online or faulted on the node. If the service group is offline, it will be shown only at the node which has highest priority in the SystemList attribute of that service group.

For example, consider a service group configured on nodes N1 and N2, where N1 is at Priority 0 (top priority) for that service group. If the service group is online or offline on N1, the appropriate state will be displayed for N1. There will not be any messages or service group state information for N2. However, in case the service group is faulted on N1 and is partially online on N2, it will report a Critical alert on N1 and a Warning on N2.

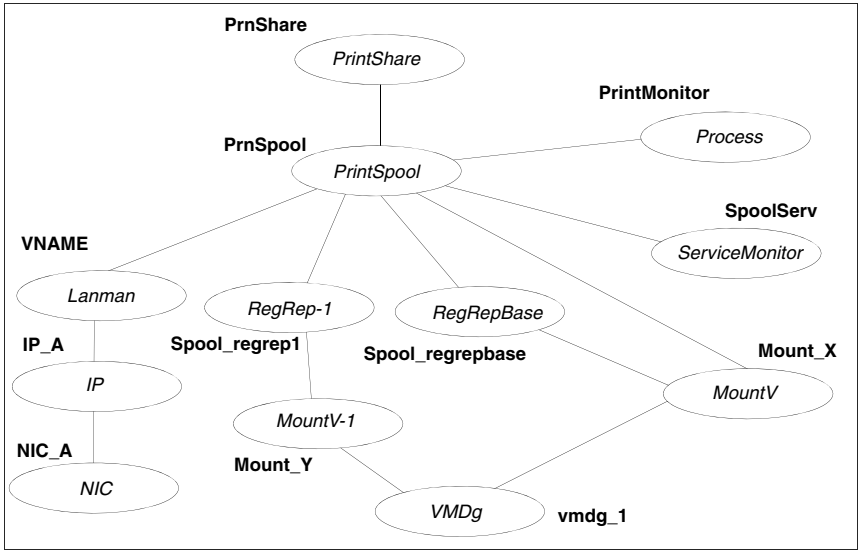
PrintShare agent changes

The PrintShare agent is modified to address performance issues in cases where a large number of PrintShare resources are configured in a service group. A new process, PrintMonitor.exe, handles the printer addition notifications and configures regrep resources for them.

After installing the 5.0 Rollup Patch 1a, when you create a Print Share service group, the Print Share wizard splits the Registry Replication resource into multiple resources such that each resource contains a maximum of 25 registry keys.

Figure 1-1 shows the new Print Share service group dependency diagram.

Figure 1-1 Print Share service group dependency graph



Note: In case of VCS for NetApp, the NetApp Filer and NetApp SnapDrive agents are used instead of the VMDg and MountV agents respectively.

If you have Print Share service groups in the cluster, you must run the Print Share Configuration wizard after installing SFW HA 5.0 Rollup Patch 1a. The wizard modifies existing Print Share service groups per the new changes to the PrintShare agent.

See "Modifying Print Share service groups after installing the rollup patch" on page 43.

System requirements

This section describes the system requirements for this release.

Supported hardware

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

http://entsupport.symantec.com

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

Supported software

Rollup Patch 2 applies to the following products:

Table 1-2 Product software supported for Rollup Patch 2

Product	Versions
Veritas Storage Foundation for Windows	5.0 5.0 Rollup Patch 1a
Veritas Storage Foundation HA for Windows	5.0 5.0 Rollup Patch 1a
Veritas Cluster Server for Network Appliance SnapMirror	5.0 5.0 Rollup Patch 1a 5.0 Release Update 1

This Rollup Patch includes support for the following software that was also supported in Rollup Patch 1a:

- Microsoft Exchange Server 2007 Standard Edition or Enterprise Edition (Mailbox Server role only) (SP1 supported)
  with
  Windows Server 2003 x64 Standard Edition, Enterprise Edition, Datacenter Edition (SP1 required for all editions, SP2 supported)
  or
  Windows Server 2003 R2 x64 Standard Edition, Enterprise Edition, Datacenter Edition
- Windows Vista

Refer to the *Veritas Storage Foundation and High Availability Solutions 5.0 Installation and Upgrade Guide* for more information on the list of supported software.

Also, see the Symantec Software Technical Support web site, http://entsupport.symantec.com/ for the latest information about Veritas Storage Foundation and HA for Windows and associated service packs and rollup patches.

Installation notes

This section provides information related to installing the patch.

Download locations

Download packages for this release from the following locations:

Table 1-3 Download Paths

To install	Download packages from
SFW HA 5.0 RP2 (32-bit) or Veritas Cluster Server for NetApp SnapMirror (32 bit)	http://entsupport.symantec.com/docs/319690
SFW HA 5.0 RP2 (64-bit) or Veritas Cluster Server for NetApp SnapMirror (64 bit)	http://entsupport.symantec.com/docs/319691
Support for Exchange 2007	http://entsupport.symantec.com/docs/319985

Notes for Japanese locales

This release does not include support for Japanese language. Before upgrading to 5.0RP2, uninstall the language pack, if installed earlier.

Preparing to install the rollup patch

This section describes the pre-installation tasks you need to perform to prepare your site for an upgrade to 5.0 RP2.

Before installing the rollup patch:

- Back up all your data in a safe location.
- Back up the system state.
- Test the system after each upgrade, especially after applying other product upgrades. An incremental upgrade eases the troubleshooting process.
- You must have network access to each remote computer.
- SFW HA and SFW with the VVR option do not support DHCP.

Note: In Windows 2000 environments, Symantec recommends that you do not use Terminal Services to remotely install SFW on systems in an MSCS cluster.

In addition to the these common tasks you also need to perform a set of tasks, depending on the environment of your primary site.

Depending on your environment, select one of the following procedures to prepare your primary site for an upgrade to 5.0 RP2.

- Preparing a VVR environment
- Preparing a Dynamic Multi-pathing (DMP) environment
- Preparing an MSCS environment
- Preparing an SFW HA environment
- Removing the Japanese language pack

Preparing a VVR environment

If you have VVR to replicate data from a primary site to a secondary site, select one of the following procedures to stop replication.

For additional information, refer to the *Veritas Volume Replicator 5.0 Administrator's Guide*.

- For VVR sites with a VCS cluster, proceed to "Preparing a clustered VVR environment" on page 28.

- For VVR sites without a cluster, proceed to "Preparing a non-clustered VVR environment" on page 28.

Note: For VVR environments with multiple secondary sites, any operations that need to be performed at a secondary site must be repeated on all secondary sites.

Preparing a clustered VVR environment

To prepare the site from the VCS java Console in a VVR environment

1. On the primary site, offline the service group for the application that uses VVR to replicate data between the sites.
   - From the VCS Java Console, right-click the service group and select the **Offline** menu option.
   - From the command prompt, type:
     `hagrp -offline group_name -sys system_name`
     where *group_name* is the name of the service group and *system_name* is the node on which the group is online.
2. On the primary site, offline the RVG service group.
3. On the secondary site, offline the RVG service group.
4. Prepare the cluster.
   Depending on the type of cluster, select one of the following procedures:
   - For a VCS cluster, proceed to "Preparing an SFW HA environment" on page 30.
   - For an MSCS cluster, proceed to "Preparing an MSCS environment" on page 29.

Preparing a non-clustered VVR environment

To prepare the sites from the VEA GUI in a non-clustered environment

1. On the primary site, stop the application that uses VVR to replicate data between the sites.
2. Select the primary RVG, right-click, and select the **Disable Data Access** option from the menu.
3. Select the secondary RVG, right-click, and select the **Disable Data Access** option from the menu.

To prepare the sites from the command line in a non-clustered environment

1. On the primary site, stop the application that uses VVR to replicate data between the sites.
2. On the primary site, disable data access to the volumes using the **vxrvg** command.
   ```
   vxrvg -g diskgroup_name stop rvg_name
   ```
3. On the secondary site, disable data access to the volumes using the **vxrvg** command.
   ```
   vxrvg -g diskgroup_name stop rvg_name
   ```

Preparing a Dynamic Multi-pathing (DMP) environment

If you have a previous installation of DMP on your system, disconnecting DMP paths should not be necessary for this Rollup Patch 2 update.

For instructions about disconnecting DMP paths, refer to the *Veritas Storage Solutions 5.0 for Windows Installation and Upgrade Guide*.

Note: Do not use the SFW 5.0 entry in Add or Remove Programs of the Windows Control Panel to change or remove DMP DSM options after the installation of any SFW 5.0 DDI package. Use the SFW DMP 5.0 DDI entry in the Add or Remove Programs of the Windows Control Panel to remove or to make any changes to the SFW DMP Solution.

Preparing an MSCS environment

Before installing the rollup patch in an MSCS environment, make sure that MSCS is running on the cluster.

Use a rolling upgrade as installation of the rollup patch requires a reboot, and reboot causes the active node of the cluster to failover.

Install the rollup patch on the inactive node or nodes of the cluster first, then use the **Move Group** command in MSCS to move the active node. Install the rollup patch on the cluster's remaining node. Refer to the *Veritas Storage Solutions 5.0 for Windows Installation and Upgrade Guide,* and the MSCS chapter in the *Veritas Storage Foundation 5.0 for Windows Administrator's Guide* for more information about the **Move Group** command.

To install this rollup patch on an MSCS cluster with SFW

1. Install the rollup patch on the inactive node or nodes of the cluster first, or move all cluster resources to another cluster node using the **Move Group** command in the MSCS Cluster Administrator.

2 Install the rollup patch on the inactive node or nodes.
See “Setting Windows driver signing options” on page 32 or “Installing the rollup patch silently” on page 37.

3 Move the cluster resources to one of the nodes with the rollup patch installed.

4 Repeat step 2 on the remaining node of the cluster.

Preparing an SFW HA environment

Prior to upgrading your SFW HA environment to 5.0 RP2, you must save and close the existing cluster configuration, using the VCS Java Console.

Additionally, if you are upgrading from SFW HA 5.0 with one or more nodes having VCS Management Console 5.1 installed, you must first remove the VCS Management Console from the nodes on which it is installed.

See “Removing VCS Management Console” on page 30.

See “Saving and closing the cluster configuration” on page 31.

Removing VCS Management Console

If one or more nodes in the cluster have Veritas Cluster Server Management Console 5.1 installed, you must remove the management console before installing the rollup patch. You can reinstall the management console after upgrading to 5.0 RP2.

See “Re-installing VCS Management Console 5.1” on page 42.

Note: This procedure is not required if you are upgrading from RP1a to RP2.

To remove VCS Management Console 5.1

1 Stop the VCS Management Console. If the management console is clustered, take the CMC_MS service group offline.

2 Back up the console’s data directory and datadir.conf files. Typically, the files are located at the following paths:

- C:\Program Files\Symantec\VRTScmcm or
- C:\Program Files x86)\Symantec\VRTScmcm

3 Remove VCS Management Console 5.1 from all nodes in the cluster using Windows Add/Remove Programs.

Saving and closing the cluster configuration

Before installing the rollup patch, use the VCS Java Console to “save and close” the configuration. This operation involves saving the latest configuration to disk and changing the configuration state to read-only mode. You must also bring the service groups offline and stop VCS before installing the rollup patch.

To save and close the configuration

From the VCS Java Console, click **File > Save** and **File > Close Configuration** on the Cluster Explorer toolbar.

To bring the service groups offline

1. From the VCS Java Console, right-click the service group and then click **Offline**.

   or

   From the command prompt, type:

   ```
   hagrp -offline group_name -sys system_name
   ```

   where *group_name* is the name of the service group and *system_name* is the node on which the group is online.

   Repeat this for all service groups that are online.

To stop VCS services

1. Stop HAD on all the cluster nodes. Type:

   ```
   hastop -all -force
   ```

2. Stop the Veritas VCSComm Startup service on all the cluster nodes. Type:

   ```
   net stop vcscomm
   ```

3. Stop GAB and LLT on all the cluster nodes. Type:

   ```
   net stop gab
   net stop llt
   ```

Removing the Japanese language pack

This release does not include support for Japanese language. In case you have the Japanese language pack installed, ensure that you remove the pack before you upgrade to 5.0RP2.

Note: While installing RP2 if the Veritas Product Installer (VPI) detects the language pack, it will prompt a message to remove the pack.

To remove the language pack

1. Access Windows Add Remove Programs.
2. Select the language pack.
3. Click **Remove**.

Installing the rollup patch using the GUI

Prior to installing the Rollup Patch, complete any pre-installation tasks required for your environment.

See "Preparing to install the rollup patch" on page 27.

The following are the stages for installing the rollup patch using the GUI:

- Setting Windows driver signing options
- Installing the rollup patch
- Resetting the Windows driver signing options

Setting Windows driver signing options

Depending on the installation options you select, some Symantec drivers may not be signed. When installing on remote or local systems running Windows Server 2003, you must thus set the Windows driver signing options to either **Ignore** or **Warn**. If the driver signing option is set to **Ignore** then the software will be automatically installed. If the driver signing option is set to **Warn** then a dialog box may prompt you to accept unsigned drivers.

The driver signing options can be changed manually on each local system or the Microsoft's Group Policy Object can be used in a Windows 2000 or Windows Server 2003 domain.

Note: For VCS 5.0 Rollup Patch 2 for Network Appliance SnapMirror, the Symantec drivers are signed by default.

To change the driver signing options on each local system

1. Open the Control Panel and click **System**.
2. Click the **Hardware** tab and click **Driver Signing**.
3. In the Driver Signing Options dialog box, note the current setting, and select **Ignore** or **Warn** to allow installation to proceed.
4. Click **OK**.
5. Repeat for each computer.

If you do not change these options, the installation may fail on that computer during validation. After you complete the installation, reset the driver signing options to their previous states.

To change the driver signing options using the Group Policy Object

1. From the Domain Controller, click **Start > Programs > Administrator Tools**.
2. In the Active Directory Users and Computers snap-in, right-click the domain root, click **Properties**, and then click the **Group Policy** tab.
3. Click the default domain policy, and then click **Edit**.
4. Expand **Computer Configuration**, expand **Windows Settings**, and then expand **Security Settings**.
5. Expand **Local Policies**, expand **Security Options**, and then modify **Device: Unsigned driver installation** behavior to the setting **Silently succeed**.
6. To force an immediate refresh, type `gpupdate` at the command line.

If you do not change the driver signing options, the installation may fail on that computer during validation. After you complete the installation, reset the driver signing options to their previous states.

Installing the rollup patch

Download the installation files from the support page for Storage Foundation for Windows on the Symantec Web site. The rollup patch is installed to the same directory as the 5.0 base installation.

Note: In case you have only the client components installed on your system, follow the steps below to upgrade these components to 5.0 RP2.

To install the rollup patch

1. Download the required packages.
   See “Download locations” on page 26.

2 Double-click the rollup patch executable file and extract the packages to a temporary location on your system.

3 Navigate to the location of the extracted files and double-click **Setup.exe**.

4 On the Select product to install panel, select the appropriate product to update:

- Storage Foundation 5.0 Rollup Patch 2 for Windows
- Storage Foundation HA 5.0 Rollup Patch 2 for Windows
- VCS for Network Appliance SnapMirror Release Update Rollup Patch 2 for Windows

5 Review the Welcome message and click **Next**.

- Specify the domain and computers for the installation:
- Select the domain and the computer. This list can take some time to populate depending on the domain and network size, speed, and activity.
- To add a computer for installation, click **Add**. You can also type the computer's name in the **Computer** field.
- To remove a computer, click the computer in the **Selected Computers for Installation** field, and click **Remove**.

Repeat the above steps for each computer. Click a computer's name to see its details.

To install the software on a remote or local computer, make sure that you have set the driver signing options to **Ignore** or **Warn**.

6 The installer checks the prerequisites for the selected computers and displays the results. Review the information and click **Next**.

If a computer fails validation, address the issue, and repeat the validation. Note that the selection in step 2 on page 34 must match the currently installed product.

Click the computer in the list of computers to display information about the failure. Click **Validate Again** to begin the validation process again.

7 Review the information and click **Install**. Click **Back** to make changes.

8 The **Installation Status** screen displays status messages and the progress of the installation.

- If an installation fails, the status screen shows a failed installation. Click **Next** to review the report and address the reason for failure. Then remove the rollup patch.
  See "Removing the rollup patch" on page 53.
- Repeat Rollup Patch 2 installation on that computer.
  See "Setting Windows driver signing options" on page 32 or "Installing the rollup patch silently" on page 37.

If the installation is successful on all nodes, the installation report screen appears.

Make sure you have set the driver signing options properly.
See "Setting Windows driver signing options" on page 32.

9 Review the report and click **Next**.

10 Reboot the remote nodes. You cannot select the local computer or computers where the installation has failed.

For VCS 5.0 Rollup Patch 2 for Network Appliance SnapMirror, a reboot is not needed. However, VCS services and HAD must be restarted manually if the nodes are not rebooted.

- Click the check box next to the remote nodes that you want to reboot. The check box is selected, by default, for remote nodes where the installation was successful.
- Click **Reboot**.
- Click **Next** to reboot the selected nodes.

11 Once the nodes have finished rebooting, click **Finish**.

12 Click **Yes** to reboot the local node.

Resetting the Windows driver signing options

After completing the installation sequence, reset the driver signing options on each computer.

To reset the driver signing options

1 Open the Control Panel, and click **System**.

2 Click the **Hardware** tab and click **Driver Signing**.

3 In the Driver Signing Options dialog box, reset the option to **Warn** or **Block**.

4 Click **OK**.

5 Repeat these steps to reset the driver signing options on each computer.

To reset the driver signing options using the Group Policy Object

1. From the Domain Controller, click **Start > Programs > Administrator Tools**.
2. In the **Active Directory Users and Computers** snap-in, right-click the domain root, click **Properties**, and then click the **Group Policy** tab.
3. Click the default domain policy, and then click **Edit**.
4. Expand **Computer Configuration**, expand **Windows Settings**, and then expand **Security Settings**.
5. Expand **Local Policies**, expand **Security Options**, and reset the policy to the original setting.
6. To force an immediate refresh, type `gpupdate` at the command line.

After installing the rollup patch, complete any post-installation tasks required for your environment.

See "Post installation tasks" on page 42.

Installing the rollup patch silently

Prior to installing the rollup patch, complete any pre-installation tasks required for your environment.

See "Preparing to install the rollup patch" on page 27.

You can perform a silent installation using the command line. Use the command `Setup.exe` to perform a silent installation. The rollup patch is installed to the same directory as the 5.0 base installation.

Note: With a silent installation, you can install on only one computer at a time.

Examples showing the installation of the rollup patch are included at the end of this section.

See "Silent installation example: Local Server" on page 38.

See "Silent installation example: Remote Server" on page 39.

To start the installation from the command window

1. Download the required packages.
   See "Download locations" on page 26.
2. Extract the packages to a temporary location on your system.
3. Open a command window by clicking **Start > Run.**
4. Type **cmd** in the Open field and click **OK**.
5. In the command window, navigate to the location of the media or network share containing the Setup.exe file.
6. Use the following command to install Rollup Patch 2:

   ```
   Setup.exe /s [INSTALL_MODE=InstallMode] [SOLUTION=Solution]
       [NODE=SysA] [REBOOT=RebootMode]
   ```

   For more information on the parameters of Setup.exe,
   See "Parameters for Setup.exe" on page 38.
7. Reboot the system at the end of installation to ensure that the rollup patch is installed correctly.
   For VCS 5.0 Rollup Patch 2 for Network Appliance SnapMirror, a reboot is not needed. However, VCS services and HAD must be restarted manually if the nodes are not rebooted.

Parameters for Setup.exe

Information about the possible parameter values are as follows:

/s	Set for silent mode. If not entered, the product installer GUI starts.
INSTALL_MODE	Set to indicate to install or remove. ***1*** = To install ***5*** = To remove The default setting is ***1*** to install. Set this parameter to ***5*** to remove. Example: **INSTALL_MODE=*1***
SOLUTION	Set to the product for installation. ***1*** = Storage Foundation 5.0 Rollup Patch 2 for Windows ***2*** = Storage Foundation HA 5.0 Rollup Patch 2 for Windows ***6*** = VCS 5.0 Rollup Patch 2 for Network Appliance SnapMirror for Windows The default setting is ***1***. Example: **SOLUTION=*1***
NODE	Set the node name. Specify only one node at a time. The default setting is the local node. Example: **Node=*SysA***
REBOOT	Set the automatic reboot of the system at the completion of the installation. ***0*** = No reboot ***1*** = Reboot The default setting is 0 for no system reboot. Example: **REBOOT=*0***

Silent installation example: Local Server

This command installs the rollup patch on the local node and tells the system to reboot at the end of the installation. The rollup patch is installed to the same directory as the 5.0 base installation.

```
Setup.exe /s INSTALL_MODE=1 SOLUTION=1 REBOOT=1
```

Silent installation example: Remote Server

This command installs the rollup patch on a remote node. It states that the node it is installing to is SysA, and tells the system to reboot at the end of the installation. The rollup patch is installed to the same directory as the 5.0 base installation.

```
Setup.exe /s INSTALL_MODE=1 SOLUTION=1 NODE=SysA REBOOT=1
```

Installing support for Microsoft Exchange Server 2007

Complete the following steps to install the VCS application agent for Exchange 2007. This agent includes support for Exchange 2007 SP1 and fixes to some reported issues. Even if you already have Exchange 2007 set up in a VCS environment, it is recommended that you install this updated agent.

You do not need to install this agent if you do not have Exchange 2007 in your environment, or if you do not wish to configure Exchange 2007 in a VCS environment.

Before you proceed, ensure that you have installed 5.0 RP2.

See "Installing the rollup patch using the GUI" on page 32.

To install the VCS agent for Exchange Server 2007

1. Download the required packages.
   See "Download locations" on page 26.
2. Extract the packages to a temporary location on your system.
3. Navigate to the location of the extracted files and double-click **Setup.exe**.
4. On the Select product to install panel, click **VCS Agent for Exchange 2007 for Windows**.
5. Review the Welcome message and click **Next**.
6. Select the domain and the computers for the installation and click **Next**.

Domain	Select a domain from the list. Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.
Computer	To add a computer for installation, select it from the Computer list or type the computer's name in the Computer field. Then click **Add**. To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**. Click a computer's name to see its description.

When the domain controller and the computer running the installation program are on different subnets, the installer may be unable to locate the target computers. In this situation, after the installer displays an error message, enter the host names or the IP addresses of the missing computers manually.

7 The installer checks the prerequisites for the selected computers and displays the results. Review the information and click **Next**.
If a computer fails validation, address the issue, and repeat the validation. Click the computer in the list to display information about the failure. Click **Validate Again** to begin the validation process again.

8 Review the information and click **Install**. Click **Back** to make changes, if necessary.

9 The Installation Status screen displays status messages and the progress of the installation.
If an installation fails, click **Next** to review the report and address the reason for failure. You may have to either repair the installation or uninstall and then re-install.

10 When the installation completes, review the summary screen and click **Next**.

11 If you are installing on remote nodes, click **Reboot**. Note that you cannot reboot the local node now, and that failed nodes are unchecked by default. Click the check box next to the remote nodes that you want to reboot.

12 When the nodes have finished rebooting successfully, the Reboot Status shows Online and the **Next** button is available. Click **Next**.

13 Review the log files and click **Finish**.

14 Click **Yes** to reboot the local node.

If you already have Exchange 2007 set up in a VCS environment, you can now proceed with the Exchange 2007 SP1 upgrade steps.

See "Upgrading Exchange 2007 to Exchange 2007 SP1" on page 45.

To configure a new HA and DR environment for Exchange 2007, refer to the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange 2007*.

Post installation tasks

Perform the following post installation tasks depending on your site environment:

Note: If a feature is added after installing 5.0 Rollup Patch 2, reinstall the rollup patch to make sure the fixes in the rollup patch are applied to the new feature.

Re-installing VCS Management Console 5.1

If you have uninstalled the VCS Management Console 5.1 while preparing your environment for an upgrade to 5.0 RP2, follow the steps below to re-install the console.

Note: This procedure is not required if you have upgraded from RP1a to RP2.

To re-install VCS Management Console

1. Install VCS Management Console 5.1.
   Refer to the *Veritas Cluster Server Management Console Implementation Guide*.
2. Restore the backed up the VCS Management Console 5.1 data files.
   See "Removing VCS Management Console" on page 30.
3. Start the VCS Management Console. If the management console is clustered, bring the CMC_MS service group online.

Modifying Print Share service groups after installing the rollup patch

The PrintShare agent is modified to address performance issues in cases where a large number of PrintShare resources are configured in a service group.

In case you have upgraded from the 5.0 base version, you must thus run the Print Share Configuration Wizard to modify the existing Print Share service groups, after installing the rollup patch.

See "PrintShare agent changes" on page 23.

This will allow the wizard to make the required changes to the service group configuration.

Note: Do *not* add or remove any resources, or modify any other attributes in the Print Share service group for the first time you run the Print Share Configuration Wizard to modify the service group.

Before you modify the existing Print Share service group:

- Make sure that the VCS engine (HAD) is running on the cluster node.
- Mount the drives or LUNs that contain the spooler and the registry replication directories on the system on which you will run the wizard.

Note: This procedure is not required if you have upgraded from RP1a to RP2.

To modify the Print Share service group after an upgrade

1. Start the Print Share Configuration Wizard. (**Start > All Programs > Symantec > Veritas Cluster Server > Configuration Wizards > Print Share Configuration Wizard**)
2. Read the information on the Welcome panel and click **Next**.
3. On the Wizard Options panel, click **Modify service group**, select your existing Print Share service group, and then click **Next**.
4. Click **Next** on the subsequent wizard panels and complete the wizard steps. You can now bring the Print Share service group online.

Importing the VCS Management Pack

This rollup patch contains fixes for the VCS Management Pack. If you have deployed the VCS Management Pack for Microsoft Operations Manager 2005 in your cluster environment, you can re-import the updated VCS Management Pack after installing the rollup patch.

The updated VCS Management Pack is included with the rollup patch software. Import the appropriate VCS Management Pack (.akm file) using the MOM 2005 SP1 Administrator Console.

While importing the management pack, ensure that you select the **Update existing Management Pack** option in the Management Pack Import/Export Wizard.

Configuring LLT over UDP

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

The following procedure describes the LLT over UDP configuration options only. It does not include detailed instructions on how to configure the cluster using VCW. Refer to the *Veritas Cluster Server Administrator's Guide* for detailed cluster configuring steps.

Before you proceed, ensure that each cluster node has at least two NICs with static IP addresses configured and the NICs are connected to the network and are able to ping each other.

Note: VCW does not support converting LLT over ethernet to LLT over UDP and vice versa.

To configure LLT over UDP

1. Launch the Cluster Configuration Wizard. Click **Start > Programs > Symantec > Veritas Cluster Server > Configuration Tools > Cluster Configuration Wizard**.
2. Read the information on the Welcome panel and click **Next**.
3. Complete the subsequent wizard steps up to the **Private Network Configuration** panel.
   Refer to the *Veritas Cluster Server Administrator's Guide* for details.
4. On the **Private Network Configuration** panel complete the following options:
   - Select the **Configure LLT over UDP** check box.
   - Specify a unique UDP port in the **Port number for Link1** and **Port number for Link2** fields. You can use ports in the range 49152 to 65535. The default ports numbers are 50000 and 50001 respectively.

- Select the check boxes next to the two NICs to be assigned to the private network. Symantec recommends reserving two NICs exclusively for the VCS private network.
- For each selected NIC, verify the displayed IP address. If a selected NIC has multiple IP addresses assigned, double-click the field and choose the desired IP address from the drop-down list. Each IP address can be in a different subnet.
  The IP address is used for the VCS private communication over the specified UDP port.
- For each selected NIC, double-click the respective field in the Link column and choose a link from the drop-down list. Specify a different link (Link1 or Link2) for each NIC. Each link is associated with a UDP port that you specified earlier.

5 Click **Next** and then follow the subsequent wizard steps to complete the cluster configuration.
  Refer to the *Veritas Cluster Server Administrator's Guide* for details.

The wizard configures the LLT service (over UDP) on the selected network adapters and uses the specified UDP ports for the private network communication.

Upgrading Exchange 2007 to Exchange 2007 SP1

This section describes how to upgrade an existing Exchange 2007 installation to Exchange 2007 SP1 using the Exchange 2007 Upgrade Wizard for VCS. It is applicable only if you already have Exchange 2007 set up in a VCS cluster environment.

Note: For the latest updates on this procedure and for information about patches and software issues regarding this release, see the following TechNote: http://entsupport.symantec.com/docs/285845.

To configure a new HA and DR environment for Exchange 2007, refer to the *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange 2007*.

Before you proceed with the Exchange 2007 upgrade, note the following:

- Ensure that you have installed one of the following products on all the cluster nodes:
  - SFW HA 5.0 Rollup Patch 2
  - VCS 5.0 Rollup Patch 2 for Network Appliance SnapMirror for Windows

- Ensure that you have installed the updated VCS application agent for Exchange 2007.
  See "Installing support for Microsoft Exchange Server 2007" on page 40
- Ensure that the Exchange 2007 service group is offline in the cluster.
- While performing the upgrade the Exchange 2007 Upgrade Wizard renames and then restarts the cluster node. Exit all the other programs before you run the wizard on a cluster node.

Upgrade steps

Complete the following steps on all cluster nodes that are part of an Exchange 2007 service group, one node at a time.

To upgrade Exchange 2007 to Exchange 2007 SP1

1. On one of the cluster nodes, navigate to the directory `%VCS_HOME%\bin\Exch2007Setup` and double-click `Exch2007Upgrade.exe` to start the Exchange 2007 Upgrade Wizard.
   The variable *`%VCS_HOME%`* is the default installation directory for VCS, typically `C:\Program Files\Veritas\Cluster Server`.
2. Review the information on the Welcome panel and click **Next**.
3. On the Exchange Virtual Server Selection panel, select the Exchange virtual server that you wish to upgrade and then click **Next**.
   The Summary table provides the details of the Exchange virtual servers in the cluster and their upgrade status on each cluster node.
   The wizard performs the tasks required to set up the VCS environment for the Exchange upgrade. The Tasks table displays the progress of the various tasks.
4. After all the tasks are completed, click **Next**.
5. Review the information on the Cluster Node Reboot panel and then click **Reboot**. The wizard prompts you to reboot the node. Click **Yes** to reboot the node.
   The selected Exchange virtual server name is temporarily assigned to the cluster node. On rebooting the node, the Exchange 2007 Upgrade Wizard is launched automatically with a message that the Exchange pre-upgrade tasks are complete. Do *not* click **Continue** at this time. Wait until after the Exchange upgrade is complete.
6. Run the Microsoft Exchange 2007 SP1 installer to upgrade Exchange 2007 on the node.
   Type the following at the command prompt:
   `<drive letter>:\setup.com /mode:Upgrade`

Here <drive letter> is the drive where the Exchange 2007 SP1 installer is located.

Note: You can also run Setup.exe to launch the installer GUI for upgrading Exchange. If using the installer GUI, ensure that you do not select any other Exchange 2007 server role. Only the Mailbox server role must be upgraded.

Verify that the upgrade has completed successfully. In case there are errors or if the upgrade has partially succeeded or has failed, resolve the errors and ensure that the upgrade is successful.
Refer to the Microsoft Exchange documentation for more information.

7 Return to the Exchange 2007 Upgrade Wizard and click **Continue**.
If the wizard is not running, navigate to the directory `%VCS_HOME%\bin\Exch2007Setup` and double-click `Exch2007Upgrade.exe` to start the wizard and then click **Next**.
The variable *`%VCS_HOME%`* is the default installation directory for VCS, typically `C:\Program Files\Veritas\Cluster Server`.

8 The wizard performs the tasks required to set up the VCS environment after the Exchange upgrade. The Tasks table displays the progress of the various tasks. After all the tasks are completed, click **Next**.

9 Review the information on the completion panel and then click **Finish**.
The wizard displays the status of the Exchange virtual server upgrade. The Summary table provides the details of the Exchange virtual servers in the cluster and their upgrade status on each cluster node.

10 Repeat these steps on the remaining cluster nodes. After you have upgraded all the cluster nodes that are configured to host the Exchange virtual server, bring the Exchange 2007 service group online in the cluster.

Note: Do not bring the Exchange 2007 service group online until you have completed the upgrade on all the cluster nodes that are part of the service group.

Upgrade considerations in case of multiple Exchange virtual servers

Consider the scenario where there are multiple Exchange virtual server instances in the cluster (an any-to-any configuration).

Table 1-4 describes the configuration objects.

Table 1-4 Exchange 2007 SP1 upgrade configuration objects

Object	Description
Node1, Node2, Node3	Physical node names
EVS1, EVS2	Exchange virtual servers

The configuration is such that:

- EVS1 can fail over on Node1 and Node2.
- EVS2 can fail over on Node3 and Node2.

So, Node2 is the common failover node for EVS1 and EVS2.

In this case, Symantec recommends that you upgrade the Exchange virtual servers in the following order:

- Upgrade EVS1 on Node1.
- Upgrade EVS2 on Node3.
- And then upgrade either EVS1 or EVS2 on Node2.
  You must upgrade Node2 (the common failover node) only once; the Exchange virtual server (whether EVS1 or EVS2) does not matter.

In general, for multiple Exchange virtual servers, upgrade each Exchange virtual server on one cluster node first, and then upgrade any one of the Exchange virtual servers on the common failover nodes.

Re-enabling VCS resources after the update

Ensure that all service groups that were made offline prior to the update are made online again, in the appropriate order based on resource dependencies. For example, the RVG service group must be online before the application service group.

In a VVR environment, online application service groups only on the primary site.

Note: In case of a VCS for NetApp environment, Symantec recommends you to use non-persistent iSCSI connections (set "Automatically restore this connection when the system boots" to False) to avoid service group concurrency violation issue.

To bring a service group online

1. Bring the service groups online, in the appropriate order based on resource dependencies.
   - From the VCS Java Console, right-click the service group and select the **Online** menu option.
     or
   - From the command prompt, type:
     `hagrp -online group_name -sys system_name`
     where *group_name* is the name of the service group and *system_name* is the node on which the group is online.
2. Repeat for additional service groups.

Re-enabling VVR after the update

After upgrading an environment where VVR replicates data from a primary site to a secondary site, use the following procedures to begin replication.

- For sites with VVR and a VCS cluster, re-enable VVR before preparing the cluster.
  See“Re-enabling VVR in a cluster environment after the update” on page 49.
- For sites with VVR in a non-clustered environment, proceed to “Re-enabling VVR in an environment without clusters” on page 50.

Note: For a VVR environment with multiple secondary sites, any operation that needs to be performed on a secondary site must be repeated on all other secondary sites.

Re-enabling VVR in a cluster environment after the update

To enable the updated objects from the VCS Java Console

1. On the primary site, bring the RVG service group online. From the VCS Java Console, right-click the RVG service group and select the **Online** menu option.
2. On the secondary site, bring the RVG service group online. From the VCS Java Console, right-click the RVG service group and select the **Online** menu option.
3. On the primary site, bring the application service group online. From the VCS Java Console, right-click the application service group, and select the **Online** menu option.

4 If bringing the service groups online does not start the application, perform any necessary tasks to start the application. Depending on options available in your environment, these tasks may include mounting databases or manually starting the application.

To enable the updated objects from the command line

1 Open a command window by clicking **Start > Run** in the taskbar. In the Open field, enter **cmd**, and click **OK**.

2 On the primary site, run the **hagrp** command to bring the RVG service group online.

```
hagrp -online group_name -sys system_name
```

3 On the secondary site, run the **hagrp** command to bring the RVG service group online.

```
hagrp -online group_name -sys system_name
```

4 On the primary site, run the **hagrp** command to bring the application service group online.

```
hagrp -online group_name -sys system_name
```

5 If bringing the service groups online does not start the application, perform any necessary tasks to start the application. Depending on the options available in your environment, these tasks may include mounting databases or manually starting the application.

Re-enabling VVR in an environment without clusters

To re-enable VVR objects after the update in a non-clustered environment, you need to perform the following.

To enable the updated objects from VEA

1 Select the primary RVG, right-click, and select the **Enable Data Access** option from the menu.

2 Select the secondary RVG, right-click, and select the **Enable Data Access** option from the menu.

3 If needed, perform any necessary tasks to start the application. Depending on the options available in your environment, these tasks may include mounting databases or manually starting the application.

To enable the updated objects from the command line

1 Open the command window by clicking **Start > Run** in the taskbar. In the Open field, enter **cmd**, and click **OK**.

2 On the secondary site, enable data access to the volumes under RVG using the **vxrvg** command.

```
vxrvg -g diskgroup start rvg_name
```

3 On the primary site, enable data access to the volumes under RVG using the **vxrvg** command.

```
vxrvg -g diskgroup start rvg_name
```

4 If needed, perform any necessary tasks to start the application. Depending on the options available in your environment, these tasks may include mounting databases or manually starting the application.

Re-enabling DMP after the update

If you have disconnected DMP paths, reconnect them before the nodes have rebooted. For instructions about reconnecting DMP paths, refer to the *Veritas Storage Solutions 5.0 for Windows Installation and Upgrade Guide*.

Repairing the installation

The product installer provides a Repair option to repair the existing installation. This installer can only repair the local system.

To repair the installation

1. In the Windows Control Panel menu, select **Add or Remove Programs**.
   For Windows Server 2003, if it is not already selected, select **Change or Remove Programs** from the left-hand pane.
2. Click the SFW 5.0 Rollup Patch 2 entry and click **Change**.
3. The installer screen appears. Select **Repair** to restore the installation to its original state. Click **Next**.
4. The Validation screen appears. The installer checks the prerequisites for the system and displays the results. Review the information and click **Next**.
   If a system fails validation, click the system in the systems list to display information about the failure. Address the problem and click **Validate Again** to repeat the validation process.
5. The Summary screen appears. Review the information and click **Repair** to begin the repair process.
   The Repair Status screen appears. Status messages and the progress of the repair are displayed.
   If an installation fails, click **Next** to review the report and address the reason for failure. You may have to uninstall and re-install the software.
6. When complete, review the summary and click **Next**.
7. On the Thank You screen, click **Finish**.

In the message box, click **Yes** to reboot your system.

Note: In the Repair Option, only the missing files are added. Other changes like changes in the types.cf must be made manually.

Removing the rollup patch

This section provides information related to removing the 5.0 RP2 rollup patch.

Note: If you are removing the rollup patch and SFW, the patch must be removed first. After the rollup patch has been removed, refer to the Veritas Storage Solutions 5.0 for Windows Installation and Upgrade Guide for information on removing SFW 5.0.
Also, if you have an added support for Exchange Server 2007, you must first remove the VCS agent for Exchange 2007 before removing SFW HA 5.0 RP2.

Preparing the SFW HA cluster

Before removing the rollup patch, use the VCS Java Console to "save and close" the configuration. This operation involves saving the latest configuration to disk and changing the configuration state to read-only mode. You must also bring the service groups offline and stop VCS before removing the rollup patch.

Perform these steps on each cluster in a VCS configuration.

To save and close the configuration

- From the VCS Java Console, click **Save and Close Configuration** on the Cluster Explorer toolbar.

To bring the service groups offline

- From the VCS Java Console, right-click the service group and select the **Offline** menu option.
  or
  From the command prompt, type:
  ```
  hagrp -offline group_name -sys system_name
  ```
  where *group_name* is the name of the service group and *system_name* is the node on which the group is online.
  Repeat this command for all service groups that are online.

To stop VCS services

1 Stop HAD on all the cluster nodes. Type:

```
C:\> hastop -all -force
```

2 Stop the Veritas VCSComm Startup service on all the cluster nodes. Type:

```
C:\> net stop vcscomm
```

3 Stop GAB and LLT on all the cluster nodes. Type:

```
C:\> net stop gab
C:\> net stop llt
```

Removing the rollup patch using the GUI

This section describes the procedure to uninstall the RP2 rollup patch. After you uninstall the rollup patch, the system is restored to the version from where you had upgraded to 5.0 RP2.

Note: If you added support for Exchange Server 2007, you must first remove the VCS agent for Exchange 2007 before removing SFW HA 5.0 RP2.

To remove the rollup patch using the GUI

1 Open the Control Panel and select **Add/Remove Programs**.

2 Select the product to remove:

- Storage Foundation 5.0 Rollup Patch 2 for Windows
- Storage Foundation HA 5.0 Rollup Patch 2 for Windows
- VCS 5.0 Rollup Patch 2 for Network Appliance SnapMirror for Windows

3 Click **Remove**.

4 Review the Welcome message and click **Next**.

5 Select the systems where you want to remove the patch from the Domain and Computer drop-down menus and click **Add**. Optionally, type the computer's name in the Computer field. Repeat this step to add other computers to the list.

The local system is listed in the **Selected computers for uninstall** list by default.

To remove a system from the **Selected computers for uninstall** list, click the system and click **Remove**.

6 Click **Next**.

7 On the Validation screen, the installer checks the prerequisites for the selected systems and displays the results. Review the information and click **Next**.

If a system fails validation, click the system in the systems list to display information about the failure. Address the problem and click **Validate Again** to repeat the validation process.

8 Review the information and click **OK**.

9 The Summary screen appears and displays the settings and systems selected for removal. Click **Uninstall**.

10 The **Uninstall Status** screen displays status messages and the progress of the removal.

If a removal fails, the status screen shows a failed status. Click **Next** to review the report, address the reason for failure, and repeat the removal on that computer.

11 If the removal is successful on all computers, the removal report screen appears.

12 The Reboot Status screen appears and lists all computers selected for removal, along with the status of each removal. Click **Reboot** to reboot the remote nodes where the removal was successful.

For VCS 5.0 Rollup Patch 2 for Network Appliance SnapMirror, a reboot is not needed. However, VCS services and HAD must be stopped manually if the nodes are not rebooted.

13 Once the remote nodes have rebooted, click **Next**.

14 On the Thank You screen, click **Finish**.

15 Click **Yes** to reboot the local system.

Removing the rollup patch silently

This procedure removes 5.0 Rollup Patch 2. The system is restored to the 5.0 version level.

To remove the base product for 5.0, refer to the procedure in the *Veritas Storage Solutions 5.0 for Windows Installation and Upgrade Guide*.

Use the command `Setup.exe` to perform a silent removal. With a silent removal, you can remove the patch on only one computer at a time.

Note: You must specify the `Setup.exe` file located on the media or network share containing the patch binaries.

Examples showing the removal of the rollup patch are included at the end of this section.

See "Removing the rollup patch example: Local Server" on page 57.

See "Removing the rollup patch example: Remote Server" on page 57.

To remove the rollup patch silently from the command window

1. Open a command window by clicking **Start > Run**.
2. Enter **cmd** in the Open field and click **OK**.
3. In the command window, navigate to the location of the media or network share containing the **Setup.exe** file.
4. Use the following command to silently remove the rollup patch:

```
Setup.exe /s INSTALL_MODE=InstallMode SOLUTION=Solution
    [NODE=SysA] [REBOOT=RebootMode]
```

5. Reboot the system at the end of the removal to ensure that the rollup patch is removed correctly.
   For VCS 5.0 Rollup Patch 2 for Network Appliance SnapMirror, a reboot is not needed. However, VCS services and HAD must be stopped manually if the nodes are not rebooted.

Parameters for Setup.exe

Information about the possible parameter values follows:

/s	Set for silent mode.
INSTALL_MODE	Set to indicate to install or remove. ***1*** = To install ***5*** = To remove The default setting is ***1*** to install. Set this parameter to ***5*** to remove. Example: **INSTALL_MODE=*5***
SOLUTION	Set to the product for removal. ***1*** = Storage Foundation 5.0 Rollup Patch 2 for Windows ***2*** = Storage Foundation HA 5.0 Rollup Patch 2 for Windows ***6*** = VCS 5.0 Rollup Patch 2 for Network Appliance SnapMirror for Windows The default setting is ***1***. Example: **SOLUTION=*1***

NODE	Set the node name. Specify only one node at a time. The default setting is the local node. Example: **Node=*SysA***
REBOOT	Set the automatic reboot of the system at the completion of the removal. ***0*** = No reboot ***1*** = Reboot The default setting is ***0*** for no system reboot. Example: **REBOOT=*1***

Removing the rollup patch example: Local Server

The command removes the rollup patch from the local node, and tells the system to reboot at the end of the removal. The command must be run from the media or network share containing the patch binaries.

```
Setup.exe /s INSTALL_MODE=5 SOLUTION=1 REBOOT=1
```

Removing the rollup patch example: Remote Server

The command removes the rollup patch on a remote node, SysA and tells the system to reboot at the end of the removal. The command must be run from the media or network share containing the patch binaries.

```
Setup.exe /s INSTALL_MODE=5 SOLUTION=1 NODE=SysA REBOOT=1
```

Tasks after removing the rollup patch

Roll back from 5.0 RP2 to the 5.0 base version of the product requires you to perform the following tasks, depending on the environment at the site:

- "Restoring the Print Share service groups" on page 58
- "Modifying the cluster configuration (VCS for NetApp SnapMirror only)" on page 59

Restoring the Print Share service groups

After removing the rollup patch, the Print Share service group will fail to come online. The service group configuration must be restored to its earlier state (as was in version 5.0) before bringing it online.

Note: If desired, you can just delete the Print Share service group and recreate it using the Print Share Configuration Wizard.

Complete the following steps to restore the Print Share configuration, only if you had installed RP2 on top of the 5.0 base version. This procedure is not required if you had upgraded from RP1a to RP2.

To restore the Print Share service group

1. From the VCS Java Console, select the Print Share service group and from the Resources tab delete all the RegRep resources apart from the RegRepBase resource. Do *not* delete the RegRepBase resource.
   - Right-click the RegRep resource in the Resources tab and select **Delete** from the menu.
   - Click **Yes** on the confirmation dialog box.
2. Delete the Process resource in the same way as in step 1.
3. Modify the RegRepBase resource as follows.
   - Right-click the RegRepBase resource and then click **View > Properties View**.
   - Edit the **Keys** attribute and remove all the registry key entries from the list.
   - Edit the Keys attribute and add the following registry key:
     `HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\VCS\BundledAgents\PrintSpool\`*`PS_SG`*`-PrintSpool`
     here *PS_SG* is the name of your Print Share service group.
   - Click **OK** and then close the Edit Attribute window.

4 Bring the Print Share service group online. From the VCS Java Console, right-click the service group and select the **Online** menu option.

5 Save and close the configuration. From the VCS Java Console, click **File > Save** and **File > Close Configuration** on the Cluster Explorer toolbar.

Modifying the cluster configuration (VCS for NetApp SnapMirror only)

This is applicable only for VCS for NetApp. After removing VCS for NetApp SnapMirror Rollup Patch 2, you must manually modify the cluster configuration otherwise the cluster may go in to a STALE ADMIN WAIT state.

Note: Perform these steps only if you had installed RP2 on top of the 5.0 base version. This procedure is not required if you had upgraded from RP1a to RP2.

To modify the cluster configuration

1 Make sure that the cluster configuration is in read-only mode.
Type the following on the command prompt:
```
C:\> haconf -dump -makero
```

2 Stop the Veritas High Availability Engine (HAD) on all the cluster nodes.
Type the following on the command prompt:
```
C:\>hastop -all -force
```

3 On a cluster node, open the cluster configuration file main.cf from the `%VCS_HOME%\conf\config` directory and modify the NetAppSnapDrive section as follows:

- Delete the curly brackets enclosing the Initiator entry.
  The Initiator entry should resemble this:
  Initiator @THORPC126 =
  “iqn.1991-05.com.microsoft:THORPC126.veritas.com”
- Delete InitiatorMonitorInterval attribute entry, if it exists.

The variable *%VCS_HOME%* is the default installation directory for VCS, typically `C:\Program Files\Veritas\Cluster Server`.

4 Start the Veritas High Availability engine (HAD) on the node where main.cf was modified.
Type the following on the command prompt:
```
C:\> hastart
```
Make sure that HAD is in the RUNNING state on the node.

5 Start the Veritas High Availability engine (HAD) on the remaining cluster nodes.

Type the following on the command prompt:

```
C:\> hastart -all
```

You can now bring the service groups online.

Fixed issues

Rollup Patch 2 includes the fixed issues and enhancements that were in the RP1a release.

For information on new fixed issues and enhancements for RP2, see the following:

"Fixed issues in RP2" on page 61

For information on the fixes and enhancements included from RP1a, see the following:

"Fixed issues in RP1a" on page 75

Fixed issues in RP2

New fixed issues and software enhancement requests in RP2 are referenced by incident numbers and described briefly below.

Rollup Patch 2 also includes the fixed issues and enhancements that were in the RP1a release. For information on the RP1a fixes, see the following:

"Fixed issues in RP1a" on page 75

This section is divided into the following topics:

Veritas Storage Foundation (RP2)

The following table describes Veritas Storage Foundation for Windows fixed issues and enhancements that were added in the RP2 release.

RP2 also includes RP1a fixes and enhancements.

See "Fixed issues in RP1a" on page 75.

For information about fixed DMP DSM issues (or fixed MPIO provider issues), refer to the most recent DMP DDI that is available in the Technical Support

section of the Symantec website.
See http://entsupport.symantec.com

Table 1-5 Fixed issues (RP2): Veritas Storage Foundation

Incident Number	Description
929134	In a VCS cluster environment, the vxsnap CLI command fails to take a snapshot of a virtual SQL server. (Related to escalation incident 1236438.)
1128820	In a cluster environment, when connection to the public network fails, the VMdg resource does not come online on the secondary node.
1186627	Symantec Plug-in Host Service (PluginHost.exe) is not a valid win32 service
1198775	VEA does not provide a configurable port range for PBX. (Related to escalation incident 1194480.)
1206077	The list parameter of the vxtask CLI command should be a mandatory parameter and match the CLI help. (Related to escalation incident 1203175.)
1210274	During system reboot, the volume resynchronization operation starts before the volume becomes available.
1216160	In an MSCS cluster environment, the vxvm service may crash. This results in cluster resources failing. (Related to escalation incident 1215627.)
1219530	When editing a rule in Rule Manager, the pre-existing alert topics are not preserved.
1223901	Disks belonging to EMC Symmetrix arrays are not displayed under the correct enclosure in the VEA GUI. (Related to escalation incident 1223900.)
1230575	After installing SFW 5.0 RP1a on a system running a German version of Windows, the VEA operations fail with permission errors.

Table 1-5 Fixed issues (RP2): Veritas Storage Foundation (Continued)

Incident Number	Description
1230736	Increasing the size of a LUN that is a dynamic GPT disk, makes basic volumes on the disk to fail or become missing. In addition, any mirrors on the disk become detached. (Related to escalation incident 1230734.)
1249152	Track alignment settings for dynamic volumes are not preserved after upgrading from SFW 5.0 to SFW 5.0 RP1.
1251335	Displaying statistics of subdisks with the vxstat -s CLI command, yields incorrect statistics of value zero. (Related to escalation incident 1248791.)
1251951	When enabling default track alignment settings, the operation fails and an error message is displayed (V-76-58645-117: The specified disk is not ready or usable). (Related to escalation incident 1247788.)
1262895	Changing a setting in the track alignment dialog incorrectly alters other track alignment settings. (Related to escalation incident 1422582.)
1265838	Increase the number of dynamic disk groups that SFW supports from a maximum of 128 to a maximum of 4096. (Related to escalation incident 1259816.)
1274755	Track alignment operation incorrectly recognizes some arrays as JBODs. (Related to escalation incident 1263680.)
1285191	Installing SFW 5.0 fails with Error 1406 (Could not write value Mode to key \SOFTWARE\Veritas\VxSvc\CurrentVersion).
1296345	Enabling the capacity monitoring feature causes Storage Agent to crash. (Related to escalation incident 1198173.)

Table 1-5 Fixed issues (RP2): Veritas Storage Foundation (Continued)

Incident Number	Description
1296613	In an MSCS cluster environment while bringing the cluster online, the error, Unable to create MountVolumeInfo, occurs. (Related to escalation incident 1290044.)
1296634	Cluscmd.log grows indefinitely without bound. (Related to escalation incident 1296439.)
1315651	SFW Scheduler Service, VxSchedService.exe, has a security issue that may allow an attacker to add, modify, or delete snapshots schedules. Consequently, malicious code may be run under the pretense of the system user. (Related to escalation incident 994752.)
1366038	The vxdg init and vxdg adddisk operations cause abnormal system termination.
1376806	Disks of StorageTek arrays do not appear under the correct enclosure in the VEA GUI. (Related to escalation incident 1371022.)
1409534	In SFW HA configurations, the Snapshot Scheduler may fail with error code -2147220211.
1413740	After system reboot, basic and dynamic volumes are not displayed in the VEA GUI but remain accessible through Windows Explorer. (Related to escalation incident 1388963.)
1416293	After disconnecting the dedicated LAN for VVR, the VEA GUI no longer displays updated information.
1427101	Add full folder mount support for the Quick Recovery Configuration Wizard
1434489	Disks of Hitachi arrays do not appear under the correct enclosure in the VEA GUI. (Related to escalation incident 1291001.)
1437978	SMTP settings are not preserved after system reboot. (Related to escalation incident 1433255.)

Table 1-5 Fixed issues (RP2): Veritas Storage Foundation (Continued)

Incident Number	Description
1452479	The Add Mirror wizard does not accept a value greater than 99 when setting the number of columns for a striped mirror. (Related to escalation incident 1441392.)
1453547	After a failover in an MSCS cluster environment, the mirror resynchronization process does not finish and the mirrors remain in a healthy, resynchronization state. (Related to escalation incident 1446412.)
1456604	The Disk Regions pane of the VEA GUI is not refreshed and cleared when there is no data to display. Data from an earlier selected disk region remains displayed. (Related to escalation incident 1414076.)
1466546	Unable to display LUN serial numbers. (Related to escalation incident 1466223.)
1468438	Disks of IBM arrays do not appear under the correct enclosure in the VEA GUI. (Related to escalation incident 1237815.)
1468445	Disks of EMC Clariion arrays do not appear under the correct enclosure in the VEA GUI. (Related to escalation incident 1370687.)
1468519	CLI tool is needed to change license keys. (Related to escalation incident 1385752.)
1470687	After using the Quick Recovery wizard to schedule snapshots, the schedules do not appear in the VEA GUI and the snapshot operations fail. (Related to escalation incident 1275372.)
1471501	Scheduled snapshots may fail with error 0x80010106 (Cannot change thread node after it is set). (Related to escalation incident 1441587.)
1471523	BSOD occurs when removing the last remaining path to an array. (Related to escalation incident 1424427.)

Table 1-5 Fixed issues (RP2): Veritas Storage Foundation (Continued)

Incident Number	Description
1471588	In a VCS environment, the MountV agents fail with errors that the file system is not clean. (Related to escalation incident 1372235.)
1473473	Incorrect CHAP status of iSCSI initiator displayed on VEA GUI. (Related to escalation incident 1442469.)
1479450	Unable to expand dynamic system/boot volume when the partition of the system/boot volume does not end at a cylinder boundary. (Related to escalation incident 1093867.)
1480511	Snapback operations may fail with error 0xe51500d3 - VXVM_TASK_IOERRO. (Related to escalation incident 1473623.)
1499998	Update JRE to address security vulnerability on Windows and DST fixes for Australia and New Zealand. (See http://www.securityfocus.com/bid/32608 and http://www.securityfocus.com/bid/32620 for more information about the issue.)
1503406	Using the VEA GUI or CLI to resize an MBR basic partition beyond the 2TB maximum should not be allowed. (Related to escalation incident 1501426.)

Veritas Cluster Server (RP2)

The following table describes Veritas Cluster Server fixed issues and enhancements that were added in the RP2 release.

RP2 also includes RP1a fixes and enhancements.

See "Fixed issues in RP1a" on page 75.

Table 1-6 Fixed issues (RP2): Veritas Cluster Server

Incident Number	Description
1186627	Symantec Plug-in Host Service (PluginHost.exe) is not a valid win32 service
1189431	Disaster Recovery wizard may not display the storage cloning summary
1193462	Disaster Recovery wizard fails to configure the Argument "Keys" for the RegRep resource when cloning the service group from the primary site
1203179	Disaster Recovery wizard running in a secure cluster is unable to proceed with VM discovery due to VM initialization failure
1276432	A SQL Server configured with VCS reports I/O errors while re-indexing databases. This issue required updates to the MountV agent. The MountV agent has been updated with a new mechanism that carries forward the CheckFSAccess action argument across new HAD restarts. This new mechanism ensures that if CheckFSAccess attribute is enabled or disabled, this attribute remains enabled or disabled until explicitly changed by the user. (Related to incident 1487942)
1487921	VCW currently supports LLT configuration only on Ethernet. (Related to escalation incident 1216934)
1500228	While updating the DNS entries, the Lanman resource faults if one or more DNS Servers fail to come online. (Related to escalation incident 1229217)

1500236	The VCS VMGetDrive Utility fails to retrieve information about cluster disk groups and configured volumes.
	The following error is displayed:
	`Getting Cluster DiskGroup and Volume info`
	`Failed to get diskgroup GUID 19:-1 073741819`
	(Related to escalation incident 1200960)

Table 1-6 Fixed issues (RP2): Veritas Cluster Server (Continued)

Incident Number	Description
1500237	After configuring an IIS service group and bringing it online, the IIS agent memory usage increases over a period of time making the cluster node unusable. (Related to escalation incident 1262548)
1500238	While updating the DNS entries, the Lanman resource updates a DNS server other than the one it is configured for. (Related to escalation incident 1235010)
1500231	Upgrade the VCS wizard to support Exchange 2007 SP1. (Related to escalation incident 1239935)
1487938	Upgrade the VCS Cluster Configuration Wizard (VCW) to include the support for configuring LLT over the User Datagram Protocol (UDP) layer. (Related to escalation incident 1251617)
1487942	A SQL Server configured with VCS reports I/O errors while re-indexing databases. Messages of the following type are displayed in the Windows Application logs and the SQL logs: `INFORMATION 833(0x40000341) MSSQL$CPSPRD01 NJIPWCPSDB01 SQL Server has encountered 1 occurrence(s) of I/O requests taking longer than 15 seconds to complete on file [<Database file name>] in database [<Database name>] (5). The OS file handle is 0x00000000000007D4. The offset of the latest long I/O is: 0x0000002b120000` (Related to escalation incident 1276432)

Table 1-6 Fixed issues (RP2): Veritas Cluster Server (Continued)

Incident Number	Description
1487944	This issue occurred in cases where the VCS Global Cluster Option (GCO) was configured in a disaster recovery setup. If the ClusterService group (with the Wide Area Connector resource) and a global service group were online on the same cluster node at a multi-node primary site and that node fails or is shut down, the service group tried to fail over locally. However, if a suitable failover node failed to exists at the primary site, the service group did not fail over to a node on the secondary site (DR site). Thus global failover was unsuccessful. The following error was logged by the VCS engine: `2008/06/15 16:21:02 VCS NOTICE V-16-1-52604 Global group <service group name> is no longer completely faulted in cluster. Canceling retry of cross-cluster failover.` (Related to escalation incident 1296465)
1487946	When a disk group was imported and the MountV resource was brought online, there were cases where volumes failed to arrive or were found missing. In such cases the MountV resource went into an UNKNOWN state and the service group was unable to fail over. (Related to escalation incident 1298362)
1487955	This issue was encountered with the Exchange Setup Wizard for VCS. If the volumes configured for Exchange were mounted as folder mount points, the Exchange Setup Wizard failed to discover such volumes and crashed intermittently. (Related to escalation incident 1298649)

Table 1-6 Fixed issues (RP2): Veritas Cluster Server (Continued)

Incident Number	Description
1487943 1303538 1487956	This issue occurs in a disaster recovery setup where the Microsoft iSCSI connection to the NetApp filers is configured with the setting "Automatically restore this connection when the system boots" set to True. If a node on which a global service group is online is shut down, the service group tries to fail over locally. If there isn't a suitable failover node at the primary site, the service group fails over to the DR site, as expected. However, when the node at the primary site is powered up, the NetApp storage resources in the service group come online on that node. This causes the service group to come partially online on the primary site. As the service group is already online at the DR site, it results in a concurrency violation. (Related to escalation incident 1293890)
1487961	This is an enhancement to the Exchange Setup wizard for VCS. The details of the enhancement are as follows: While moving the Exchange database to shared storage, the Exchange Setup Wizard provided an option (Advanced button) to add the Exchange Virtual Server name to an Organization Unit. The wizard discovered all the Organization Units in the domain and populated them in a drop-down list. You could specify an OU by selecting the OU name from this drop-down list. The enhanced Exchange Setup Wizard now allows you to type the Organization Unit name or search the OU name in the domain using the Windows "Find Organizational Units" dialog box. This makes searching and specifying an OU significantly easier in cases where there are a large number of Organizational Units in the domain and where the OU structure is deeply nested. (Related to escalation incident 1319212)

Table 1-6 Fixed issues (RP2): Veritas Cluster Server (Continued)

Incident Number	Description
1487965	After configuring a print share service group with printers added in the virtual server, subsequent deletion of printers was not reflected upon failover to another nodes. This occurred due to RegRep agent's behavior of not processing the keys that were deleted. The printers were stored under a registry hive and the hive corresponding to the deleted printer was ignored by RegRep agent. (Related to escalation incident 1369751)
1487967	This issue occurred when Exchange was deployed in an Any-to-Any configuration with a front-end/back-end scenario, and the Exchange back-end server was clustered with VCS. When the Calendaring options for the Exchange protocols (POP3 and IMAP4) were configured to use the Exchange front-end server (Calendaring tab > Use front-end server option), VCS failed to bring the Exchange Protocol resources online. The Exchange Protocol agent log displayed the following message: 2008/07/23 11:53:30 VCS DBG_21 V-16-50-0 ExchProtocol:V03-IMAP4SVC-1:online:_UpdateMetabaseInformation() returned 100, 0x00000003 ExchProtocolRes.cpp:CExchProtocolRes::Online[207] (Related to escalation incident 1371162)
1487970	While upgrading to 5.0 RP1a, if the IIS agent attribute Site Type was set to APPPOOL, the IIS resource did not probe. (Related to escalation incident 1372034)
1487971	This issue occurred when the VCS Global Cluster Manager was configured in any-to-any failover set up. After the reboot, the regrep drive was not mounted since the "Automatically Restore the connection after reboot" was not selected for iSCSI Initiator. The wizard also failed to mount it because the initiator was renamed. (Related to escalation incident 1373467)

Table 1-6 Fixed issues (RP2): Veritas Cluster Server (Continued)

Incident Number	Description
1487972	A node could not be added to a cluster which had ClusterService service group configured and the node had only 1 Public NIC enabled using HP NIC teaming. (Related to escalation incident 1382400)
1487974	After configuring a Process resource inside a service group and bringing it online, the Process agent memory usage increased with each offline, online, offline monitor operation. The memory usage pattern indicated leakage in these entry points. This leakage was observed only on Windows IA64 and Windows X64 based systems. (Related to escalation incident 1383348)
1487975	After configuring the SQL2005 agent, HTC agent, GCO, CMC 5.0 ClusterConnector, and VxAT, the handle counts from had.exe increased with each offline and online operation. The increase in handle count indicated a slow handle leak in had.exe (Related to escalation incident 1391121)
1487977	This is an enhancement to the Veritas Hitachi TrueCopy agent. You can now configure the agent to generate notifications depending on the state of the configured HTC devices. (Related to escalation incident 1461320)
1487979	The SFW-HA 5.0 RP1a SQL Configuration Wizard ignored the settings of 'ADUpdateRequired' and 'ADCriticalForOnline' that were configured in 'Lanman Advanced Configuration'. The Lanman resource when created, would always set the 'ADUpdateRequired' and 'ADCriticalForOnline' attributes to 'True'. In absence of proper admin rights, the Lanman resource would fault and the user was required to manually reset the 'ADUpdateRequired' and 'ADCriticalForOnline' attributes to 'False' (Related to escalation incident 1398535)

Table 1-6 Fixed issues (RP2): Veritas Cluster Server (Continued)

Incident Number	Description
1487980	On a MOM 2005 SP1 server, the state monitoring script generated alerts, when a service group was taken offline from online state or online from offline state, if the VCS MOM script was called during the transition period. (Related to escalation incident 1436651)
1487981	Due to the presence of unrecognized resources inside the printshare service group the Print Share Configuration Wizard was unable to detect externally modified printshare service groups in the modify mode. (Related to escalation incident 1437841)
1487982	This issue was encountered in SFW-HA 5.0 RP1a on Win2k3 SP2. The VCSAgDriver.exe associated with the RemoteGroup resource type showed an increase in the handle count. The handles were not released and memory was not reallocated unless the resource was taken offline. (Related to escalation incident 1451314)
1455542	Disaster Recovery wizard fails with exception error “Failed to discover "Veritas Volume Manager' on node” after specifying the primary system name (1427895)

1517221	This issue was encountered in Storage Foundation and High Availability Solutions 5.0 RP1a for Windows and Veritas Cluster Server 5.0 RP1a for Windows.
	The Process Agent failed to probe when the configured user account password contained spaces.
	The following error was logged:
	`VCS ERROR V-16-10051-6531`
	`Process:monitor:Failed to get the password`
	(Related to escalation incident 1481743)

Veritas Volume Replicator (RP2)

The following table describes Veritas Volume Replicator fixed issues and enhancements that were added in the RP2 release.

RP2 also includes RP1a fixes and enhancements.

See "Fixed issues in RP1a" on page 75.

Table 1-7 Fixed issues (RP2): Veritas Volume Replicator

Incident Number	Description
1483566	Creation of RDS fails with error message "The configuration server may be busy or down." (Related to escalation incident 1410129.)
1483567	'My Computer' applet does not display the correct volume label for VVR related volumes. (Related to escalation incident 1202525.)
1483569	Attempt to add a secondary RVG fails with no secondary RVG found error. (Related to escalation incident 1207834.)
1483572	Unable to select RVG in an MSCS RVG resource while creating a cluster resource. (Related to escalation incident 1202082.)
1483573	Currently, the frequency with which the errors get added to the vxobjserver.log is 16 times per second. Need to reduce the frequency of logging errors so that the log file does not overflow.
1485531	VRAdvisor is unable to properly monitor the mount points. Details pertaining to a single volume shown even when data is collected for multiple volumes. (Related to escalation incident 1088187.)
1487143	Sync snapshot on a secondary fails if the first 7 characters of a volume in an RVG are same. In RP2, the last 7 characters of a volume name will be used to generate the snapshot volume name on the secondary. If synchronized snapshot has already been done on the secondary before installing RP2, then synchronized snapback on the secondary is not possible after installing RP2. This is because the naming convention for snapshotted volumes on the secondary has now changed. In such a scenario, you will need to do a manual snapback.

Table 1-7 Fixed issues (RP2): Veritas Volume Replicator (Continued)

Incident Number	Description
1487145	Application fault in VVRDCOMBridge.exe (Related to escalation incident 1177327.)

Fixed issues in RP1a

Rollup Patch 2 includes the fixed issues and enhancements that were in the RP1a release.

These are referenced by incident numbers and described briefly below. This section is divided into the following topics:

- Veritas Storage Foundation (RP1a)
- Veritas Cluster Server (RP1a)
- Veritas Volume Replicator (RP1a)

For information on the new fixes added in RP2, see the following:

"Fixed issues in RP2" on page 61

Veritas Storage Foundation (RP1a)

Rollup Patch 2 includes the fixed issues and enhancements that were in the RP1a release. The following table describes Veritas Storage Foundation for Windows fixed issues and enhancements in RP1a.

For information on new fixes added for Veritas Storage Foundation in RP2, see the following:

"Veritas Storage Foundation (RP2)" on page 61

Note: For information about fixed DMP DSM issues (or fixed MPIO provider issues), refer to the most recent DMP DDI that is available in the Technical Support section of the Symantec website.
See http://entsupport.symantec.com

Table 1-8 Fixed issues (RP1a): Veritas Storage Foundation

Incident Number	Description
603972	Enhancement: Provide support for Microsoft System Center Operations Manager 2007.
930291	The CLI command, vxdisk diskinfo, returns an incorrect signature value of zero. (Related to escalation incident 607019.)
962400, 1096696	The delete snapshot operation fails for VSS snapshots.
965990	Memory leaks occur during VSS snapshot operations. **Note:** This is a known Microsoft issue (KB 933653).
969428	Services do not to start when a file with filename = "Program" exists in the system's root directory. (Related to escalation incident 969387.)
974047	Enhancement: VSS backup and restore support for Exchange 2007.
1000236	CLI command, vxdg rmdisk, gives an inaccurate invalid argument error message when attempting to remove missing disks. (Related to escalation incident 998943.)
1004399	Mirrored volume operations performed in the VEA GUI are not reflected in the DISKPART utility. (Related to escalation incident 793161.)
1005208	I/O hang occurs when the server is low on free kernel memory. (Related to escalation incident 996007.)

Table 1-8 Fixed issues (RP1a): Veritas Storage Foundation (Continued)

Incident Number	Description
1010886	CLI command, vxprint, does not give the same output as in earlier SFW release. (Related to escalation incident 1005234.)
1010975	An incorrect label set for a snapshot volume occurs when the original volume appears as RAW and snapshot volume appears as NTFS. (Related to escalation incident 966428.)
1025547	Track Alignment feature does not properly detect array due to ProductID mismatch. (Related to escalation incident 1025220.)
1045433	When vxdg fails in a cluster environment that is using third-party clustering software, an unexpected failover occurs. (Related to escalation incident 1042089.)
1047867	On 64-bit systems, an RPC error (RPC_E_CHANGED_MODE) may occur.
1056695	VDS generates error messages in the system event log when a rescan is performed. (Related to escalation incident 1043600.)
1059086	Memory leak occurring with snapshot operation of Exchange database causes subsequent snapshots to fail. (Related to escalation incident 1011786.)
1077608	In the VEA GUI, creating a mirrored volume, while specifying the maximum size, and then canceling the operation results in a false resynchronization object in the VEA GUI. (Related to escalation incident 1074566.)
1093865	Incorrect track alignment value for IBM DS8000 storage array displayed in VEA GUI. (Related to escalation incident 1038446.)

Table 1-8 Fixed issues (RP1a): Veritas Storage Foundation (Continued)

Incident Number	Description
1116953	Memory leak in the MountV resource and the VmDg resource. (Related to escalation incident 1072179.)
1125418	A runtime error occurs and the vxsvc service crashes after completing a vxsnapsql snapshot operation. (Related to escalation incident 1119269.)
1132460	Unable to mirror the boot volume with track alignment disabled during the mirror creation. (Related to escalation incident 1123368.)
1136612	Storage Agent terminates unexpectedly. (Related to escalation incident 1096950.)
1143845	The VSS provider terminates abnormally when an application deletes VSS snapshots.
1146738	On non-English Windows operating systems, the vxcbr command fails. (Related to escalation incident 1095207.)
1150011	After upgrading a system configured for DMP ASLs for IBM storage devices to SFW MP2, the system reports the serial number of the storage device in hexadecimal. (Related to escalation incident 1084469.)
1152475	VM dynamic disk group resource fails to come online after failover.
1152524	Enhance CLI commands: ■ Enable the upgrade of a system/boot disk to a dynamic disk using vxdg init. ■ Enable the specification of maximum size when creating a volume using vxassist make. ■ Enable the specification of preferred hot relocation targets using vxdisk. (Related to escalation incident 990322.)

Table 1-8 Fixed issues (RP1a): Veritas Storage Foundation (Continued)

Incident Number	Description
1152527	After applying patch to address a memory leak (incident 1016719), the vxdg list command fails. (Related to escalation incident 1128034.)
1153107	Uninitialized disk group object ID causes abnormal system termination. (Related to escalation incident 1094278.)
1153456	Adjusting the dgarrivaltimeout registry key with the MSCS GUI has no effect. (Related to escalation incident 1140367.)
1154202	Windows Resource Monitor (resrcmon.exe) causes abnormal system termination due to heap corruption. (Related to escalation incident 1153216.)
1167858	Parallel requests from MSCS concerning VmDg resources causes Windows Resource Monitor (resrcmon.exe) to crash. (Related to escalation incident 1180784.)
1175532	SMTP configuration settings are not saved. (Related to escalation incident 1174611.)
1181958	Using the SFW GUI or the vxsnap CLI command to take a snapshot results in the message, "VSS Provider reached an unexpected provider error."
1185230	The VxBridge service fails to start with the following message: "VxBridge is not a valid Win32 application." (Related to escalation incident 1181212.)
1185392	The VSS Snapshot Wizard and the VSS Snapshot Scheduler Wizard incorrectly display the same subcomponent name for all subcomponents. (Related to escalation incident 1173833.)

Veritas Cluster Server (RP1a)

Rollup Patch 2 includes the fixed issues and enhancements that were in the RP1a release. The following table describes Veritas Cluster Server fixed issues and enhancements in RP1a.

For information on new fixes added for Veritas Cluster Server in RP2, see the following:

"Veritas Cluster Server (RP2)" on page 66

Table 1-9 Fixed issues (RP1a): Veritas Cluster Server

Incident Number	Description
964973	Using standard license on Windows 2003 Standard Edition gives the following error about the license key: VCS ERROR V-16-1-52539 [Licensing] License key cannot be used on this OS platform.
899632	Unable to online multiple Lanman resources bound to the same IP in the x64 edition.
1014750	Unable to switch a global service group to a remote cluster using the Cluster Management Console (CMC).
1016719	Memory leak in VCSAgDriver process.
1027045	While configuring a 32-bit SQL Server on a 64-bit SFW HA system, the SQL Configuration Wizard for VCS fails with error V-16-13-3010.
1039744	In a SFW HA 5.0 cluster, while trying to online a print share service group with around 500 printers, it is observed that the regrepmonitor.exe process goes almost upto 100% CPU usage, causing either a significant delay in completing the task or failure of the task. Also the printspool resource goes offline for some time and then comes online.
1071916	In a SFW HA 5.0 secure cluster on non-English operating system, while starting or stopping HAD, the following error is displayed: "Error V-16-1-50105 Command (MSG_CLUSTER_STOP_ALL) failed. Cluster admin or Group admin privilege is required." These errors are displayed even if the user account has the required privileges.

Table 1-9 Fixed issues (RP1a): Veritas Cluster Server (Continued)

Incident Number	Description
1077622	In a SFW HA 4.3 MP2 cluster on 32-bit Windows 2003 SP2 R2 servers, when a remote File share or Print share is accessed from the node on which the print share service group was online, the spooler service crashes causing the print share service group to fail over. The PrintSpool log displays the following error: “VCS Error V-16-10051-7019 PrintSpool: Print-Share-PrintSpool:monitor: The helper process for this resource exited automatically”.
1101865	The Lanman resource deletes reverse entries for some of the DNS servers if PurgeDuplicate is enabled and BIND servers are being updated. This occurs only while updating BIND (Q-IP DNS) servers.
1126677	The SQL Configuration Wizard for VCS fails during the discovery process and the following error is displayed: “An unhandled win32 exception occurred in hadiscover.exe(668) VCS Error V-16-13-1044 A required discovery function could not be located from the command client DLL”.
1094153	Access Violation (AV) causes VCW to crash while attempting to add a node to a two node cluster.
1147399	Memory leak in the VCSAgDriver.exe process running for the IIS agent. A significantly large memory leak is observed within a short period of time.
1143343	While importing VCS management pack for SQL 2005 (vcs_sql2005_mom2005.akm), the rules and scripts are disabled and replaced with older versions. An error message is displayed that warns that the current rule version is being downgraded.
1145156	MOM server gets alerts stating that VCS resource has failed or is unavailable.
1156332 1160780	VCW should allow user names with special characters such as “$” on the User selection page.

Table 1-9 Fixed issues (RP1a): Veritas Cluster Server (Continued)

Incident Number	Description
1169405 1193375	HTC agent monitor cycle spams the engine log. It generates two lines of logging per minute into the engine log.
1174911 1193059	Group switch/failover logic does not complete if parent group gets autodisabled in between.
1170305 1190397	MirrorView resource does not set the recovery policy to automatic after a fail over.
1182931	While setting up an Exchange 2007 cluster in the child domain of a multi-domain environment with a parent-child configuration, the Exchange Setup Wizard fails on the second cluster node during the pre-installation tasks. There are no errors while configuring Exchange 2007 on the first cluster node.
1176305	In SFW HA 5.0 with MirrorView agent, after a site failover, the recovery policy is set to manual.
1189577 1190097	SQL 2000 and SQL 2005 detail monitoring script fails to run due to lack of resources, but does not fault the resource as configured.
1190317	SQL service group does not fail over if detail monitoring script fails.
994343	Using VCW, Notifier and Web Console cannot be set to use same NIC resource.
1118265	The VCS MOM packs do not collect health informaton about the virtual server.
1169442	VCS state script should generate alerts at resource level.
1183714	SQL - OLAP resource fails to come ONLINE for multiple SQL instances.

Table 1-9 Fixed issues (RP1a): Veritas Cluster Server (Continued)

Incident Number	Description
1203002	In a VCS cluster with a MOM 2005 monitoring environment, the VCS state monitoring script logs service group offline Information messages as alerts. The service group is online on a cluster node. The Information messages indicate that the service group is offline on the remaining cluster nodes. This results in a large number of "Information" alerts on the MOM server.

Veritas Volume Replicator (RP1a)

Rollup Patch 2 includes the fixed issues and enhancements that were in the RP1a release. The following table describes Veritas Volume Replicator fixed issues and enhancements in RP1a.

For information on new fixes added for Veritas Volume Replicator in RP2, see the following:

"Veritas Volume Replicator (RP2)" on page 73

Table 1-10 Fixed issues (RP1a): Veritas Volume Replicator

Incident Number	Description
1154266	When VVR is enabled, the server eventually becomes unresponsive. Event log shows 2019 nonpaged pool error. DMIO.SYS is consuming up to 45MB of nonpaged pool memory.
1154267	RVG Primary resource hangs when attempting to offline Port to MP2. No issues reported while onlining the resource.
1154272	MSCS cluster with three or more RVG resources shows continuous disconnect/reconnect cycle while replicating when the resource groups are moved from one node to the other.
1154273	Servers are experiencing vxsvc.exe crashing with no particular pattern.

Table 1-10 Fixed issues (RP1a): Veritas Volume Replicator (Continued)

Incident Number	Description
1154282	Fault in the volume Replicator performance module VVRPERF.DLL causing memory leak. Servers using VERITAS Storage Foundation™ 4.1 or 4.2 for Windows with Volume Replicator option may experience a memory leak.
1154262	Memory leak in HA server.
1154264	Unable to discover RLINKS. Multiple warning messages reported by vvrperf.
1162665	Engine log is filled with VCS INFO V-16-1-53001 and V-16-1-53003 messages. The logs are unusable due to the frequency of these messages.

Known issues

This section lists known issues for this release.

Error occurs during login on a system that had SFW 5.0 RP1a previously uninstalled (1214088)

On a system that had SFW 5.0 RP1a previously uninstalled, an error occurs during login. If the system had SFW 5.0 RP1a installed, uninstalling SFW 5.0 RP1a results in the system unable to download SFW extension files.

Workaround

After uninstalling SFW 5.0 RP1a, delete all client extension and message catalog files, then restart the vxvm service.

- Delete the client extension files located at

  %ALLUSERSPROFILE%\Application Data\VERITAS\VRTSbus\cedownloads

- Delete the message catalog files located at

  %ALLUSERSPROFILE%\Application Data\VERITAS\VRTSbus\mcdownloads

Vxob service may terminate abnormally during upgrade to SFW 5.0 RP1a (1176351)

During the upgrade process from SFW 5.0 to SFW 5.0 RP1a, the vxob service may terminate abnormally and generate a dump. This abnormal termination does not affect the upgrade process to SFW 5.0 RP1a. Ignore the abnormal termination of the service and allow the upgrade process to complete.

Vxsnap restore operation fails with "Pre-Restore failed by Writer" error (1512728)

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

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

Workaround

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

Upgrading from SFW 5.0 RP2 to SFW 5.1 results in a corrupt plugin component message when selecting a diskgroup. (1533682)

After upgrading from SFW 5.0 RP2 to SFW 5.1, selecting a diskgroup causes a message to appear stating that a plugin component may be corrupt. This message appears because the GUI cache needs to be cleaned.

Workaround

To clean the GUI cache:

1. Close the VEA GUI.
2. In a command window, enter
   net stop vxvm
3. In Windows Explorer, delete all files in the directory
   %ALLUSERSPROFILE%\Application Data\VERITAS
   \VRTSbus\Temp\extensions
4. In a command window, enter
   net start vxvm
5. Launch the VEA GUI and continue with normal operations.

VVRDCOMBridge fails to start after upgrading to SFW HA 5.0 RP1a (1175646)

VVRDCOMBridge service fails to start after upgrading to SFW HA 5.0 RP1a. This is happening due to the Path Environment Variable being truncated to 1024 bytes on a Windows Server 2003 system. Due to this, the services are not getting the required VEA dll's path from the Path Environment Variable and fail to start. Additionally, the VxBridge, Veritas VSS Provider, and Veritas DG Delayed Import Service also fails to start. The path changes after upgrading to SFW HA 5.0 RP1a.

The two paths that get appended to the end of the Path Variable after upgrade are:

- C:\Program Files (x86)\Veritas\VRTSobc\pal33\bin
- C:\Program Files (x86)\Veritas\Veritas Object Bus\bin

Note: Before upgrade, these paths were at the beginning of the path variable.

Workaround

Copy the SFW related path before the 1024 bytes

OR

Install the service pack mentioned in the KB article from http://support.microsoft.com/kb/906469.

Error while performing Exchange post-installation steps (1200931)

After installing Exchange and rebooting the node, the Veritas High Availability Engine (HAD) may fail to start. As a result, while performing the Exchange post-installation tasks, the Exchange Setup Wizard may either fail to launch or may display the following error message:

```
Failed to get the cluster information. Make sure that VCS
Engine (HAD) is in running state. Start HAD and click Retry
to continue. Click Cancel to exit the wizard.

Error V-16-13-4207
```

This issue may occur in a secure cluster environment.

Workaround

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

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

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

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

   The state should display as RUNNING.

3. Click **Retry** on the Exchange Setup Wizard panel and proceed with the Exchange post-installation steps.

Issue with the rollup patch installer (1205171)

If you have installed the VCS agent for Exchange 2007 after installing the rollup patch and then you wish to remove the rollup patch, the installer does not prompt you to remove the VCS agent for Exchange 2007 and proceeds with the rollup patch uninstallation. This may make your Exchange 2007 cluster configuration invalid.

If you wish to remove the rollup patch, you must first remove the VCS agent for Exchange 2007 and then proceed with the rollup patch uninstallation.

Exchange service group does not fail over after installing ScanMail 8.0 (1071168)

This issue occurs when you try to install ScanMail 8.0 in an Exchange cluster. After installing ScanMail on one node in a cluster, when you switch the service group to another node to install ScanMail, the service group does not come online.

You can complete the ScanMail installation by making changes to the registry keys and bring the Information Store online. But the Exchange services continue to stop intermittently, causing the resources and the service group to fault and fail over.

To make changes in the registry keys

1. Bring the Exchange service group online.
2. Click **Start** and then click **Run.**
3. In the dialog box, enter ***regedit*** and click **OK**.
4. In the Registry Editor, locate the following subkey in the registry: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan`
5. In the right pane, double-click **Enabled**.
6. Click **Decimal**, enter **0**, and then click **OK**.
7. On the File menu, click **Exit** to quit Registry Editor.

Print Share service group fails to come online after removing the rollup patch

Rollup patch is installed on a cluster which had Print Share service groups configured. After the installation, the existing Print Share service groups are modified using the Print Share Configuration Wizard to update the service group configuration with PrintShare agent changes.

After the configuration is modified, if the rollup patch is removed from the cluster, the cluster state is reverted to its earlier state. But the Print Share service group fails to come online. If you run the Print Share Configuration Wizard, the wizard fails to recognize the service group.

Workaround

You have to manually restore the Print Share service group configuration before bringing it online.

See “Restoring the Print Share service groups” on page 58 for instructions.

Print Share Configuration Wizard fails to recognize Print Share service groups after removing the rollup patch

This issue is similar to the Print Share issue mentioned earlier. After removing the rollup patch, the Print Share service group fails to come online. If you run the Print Share Configuration Wizard, it fails to recognize the service group.

Workaround

You have to manually restore the Print Share service group configuration before bringing it online or modifying it using the Print Share Configuration Wizard.

See "Restoring the Print Share service groups" on page 58 for instructions.

Switching the SQL service group in DR environment with SEP11.0MR1 installed, causes systems to hang (1203009)

In a secure DR environment with Symantec Endpoint Protection 11.0MR1 installed on the domain controller and the cluster nodes, switching within the cluster or between two clusters causes the server to hang. This problem occurs only when VVR/GCO is configured.

Symantec Endpoint Protection Manager is installed on the domain controller while Client is installed on the cluster node.

DR, QR, and FD wizards do not support Exchange 2007

In this release you cannot use the Disaster Recovery, Quick Recovery, and Fire Drill wizards to configure Exchange 2007.

Data on regrep drive gets corrupted (1202282)

In a secure cluster, configure a Print Share service group with 1000 print shares on it. The service group is brought online but some of the registry key names may get corrupted.

Workaround

- Rename the directory in which the regrep keys get dumped and then create a directory with the same name on the drive.
- Take the service group offline. This will force the agent to dump the regrep keys again on the drive. Now the regrep keys are created properly.

VCS Management Console Single Cluster Mode and the VCS Management Server 5.1 cannot co-exist on the same Windows system (1113954)

If you install the VCS Management Console version 5.1 in multi-cluster mode (MCM) on a node where the Management Console was installed in a single-cluster mode (SCM), the management server 5.1 installer uninstalls SCM as a part of management server upgrade process. After the installation, all SCM files and settings are lost, and you cannot run the SCM console.

If you run the VCS Cluster Configuration Wizard to configure the Web Console resource, the wizard will configure the Web Console resource but will not be able to bring the Web Console resource online.

VCWSilent does not support LLT over UDP configuration

VCS provides a silent configuration utility, VCWSilent.exe, to configure a new VCS cluster from the command line. You can specify the cluster details in an xml file and run the utility to configure the cluster without using the Veritas Cluster Configuration Wizard (VCW). However, VCWSilent does not support configuring Low Latency Transport (LLT) over User Datagram Protocol (UDP) from the command prompt. VCWSilent only supports configuring LLT over Ethernet. You must use VCW to configure LLT over UDP.

For more information about VCWSilent utility, refer to the *Veritas Cluster Server Administrator's Guide*.

VCW does not support converting LLT over ethernet to LLT over UDP and vice versa

VCW does not support *converting* your existing cluster configuration to use UDP ports for the private network communication. If you already have a cluster where LLT is configured over ethernet, you will have to delete the cluster and then recreate it to configure LLT over UDP.

This also applies in case you have already configured LLT over UDP. You will have to delete the cluster and then recreate it to configure LLT over ethernet.

VCW does not support configuring broadcasting for UDP

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

Network adapters teamed using the HP Network Configuration Utility not tested on Windows IA64 systems

Symantec has not tested UDP over LLT cluster configurations with network adapters teamed using the HP Network Configuration Utility on Windows IA64 systems.

VCW incorrectly allows configuration of DHCP enabled network adapters for private network communication

If there are DHCP enabled teamed network adapters on the systems, VCW displays those network adapters and allows you to configure them for the VCS private network communication.

DHCP enabled network adapters are not supported. You must not select DHCP enabled network adapters for cluster configuration.

VCW incorrectly resets the UDP port while editing the cluster configuration

If you have configured LLT over UDP and you run VCW to edit the cluster configuration, VCW automatically resets the port number for the UDP links to 50000. This may happen if network adapters teamed using the HP Network Configuration Utility are used in the configuration.

While editing the cluster configuration, you must re-select the network adapters and specify the port number for the link, as per your original configuration.

VCW incorrectly configures LLT over network adapters that may be disconnected from the network

While configuring LLT over UDP, if a network adapter selected for the LLT communication is disconnected from the network, VCW displays the IP address of that NIC as 0.0.0.0. If you proceed with the cluster configuration, VCW configures the LLT service on the selected network adapter with 0.0.0.0 as the IP address.

This will result in an invalid cluster configuration.

Teamed NIC configurations may break VCS LLT communication or cause NIC resource to go into an UNKNOWN state (1522757)

Certain NIC teaming software allow configuring network adapters such that each participating NIC in the team is assigned a separate MAC address. Depending on the configuration, any of the individual NIC MAC address is used as the MAC address of the teamed NIC.

This NIC teaming configuration may cause the following issues:

- A VCS NIC resource configured for such a teamed NIC may go into an UNKNOWN state. This may happen if on server reboot the MAC address of the teamed NIC changes from what is specified in the MACAddress attribute of the NIC resource. In such cases, the NIC resource cannot be probed.
- Change in the MAC address may break the Low Latency Transport (LLT) private communication in the VCS cluster.

VCS does not support such NIC teaming configurations. If you are using NIC teaming then ensure that the MAC address for the teamed NIC remains the same.

Exchange 2007 database LUNs cannot be mounted after installing Exchange 2007 on a failover cluster node (1515156)

This issue may occur in a VCS for NetApp environment.

Exchange 2007 installer requires that the Exchange database LUN should be mounted on the node when installing Exchange 2007 in RecoverServer install mode.

After the Exchange installation is complete, you must dismount the Exchange database LUN before you perform the Exchange post-installation tasks on the node. If you do not dismount the LUNs before the post-installation tasks, then after post-installation, you may not be able to mount those LUNs on any cluster node. This occurs only if the NetApp LUNs are mounted using iSCSI initiators.

In such a case, you have to then manually remove the corresponding LUN mappings on the NetApp filer and then mount the LUNs.

Symantec recommends the following:

- In general, while configuring Exchange 2007 on additional nodes, if there are any other LUNs (not necessarily for Exchange) mounted on the node, ensure that you dismount them before you perform the Exchange post-installation tasks on that node.
- Rename the Microsoft iSCSI initiator such that the initiator name does not contain any references to the node names.

VCS High Availability Engine (HAD) may either restart or crash when two service groups are simultaneously failed over to the same node (1526876)

This issue occurs when two service groups, configured in an Any-to-Any cluster configuration, are switched or failed over to the common failover node simultaneously. One of the service groups succeeds to come online on the node. However, as the other service group tries to come online, HAD may restart or crash on the node from which the service group was failed over.

In a non-secure cluster, HAD may restart; in case of a secure cluster, HAD may either fail to respond or crash.

Workaround

In case of a secure cluster, you must manually end the HAD process from the Windows Task Manager and then bring the service groups online on their respective nodes (not the common failover node).

Symantec recommends that you do not attempt to bring service groups, configured in an Any-to-Any configuration, online on the common failover node simultaneously.

The installer fails to install RP1a after RP2 is uninstalled (1529871)

This issue occurs if you had upgraded to 5.0RP2 from 5.0 base version, and later chose to uninstall RP2 and install RP1a.

While installing RP1a, the installer throws the "`The product already exists`" error.

Workaround

For the latest information and updates on this issue, see the following information on the Symantec Technical Support website:

http://entsupport.symantec.com/320347

The VCS Cluster Configuration Wizard (VCW) may crash while reconfiguring a cluster (1512683)

This issue occurs when network adapters that are already configured in a cluster are later teamed using the HP Network Configuration Utility. After teaming the network adapters, when you run VCW to reconfigure them in the cluster, VCW may crash.

Exchange 2007 Setup Wizard may fail during the move database operation (1531711)

While performing the move databases operation, the Exchange 2007 Setup Wizard for VCS may fail. This occurs if while installing Exchange on the first cluster node, the wizard failed to create the required forward and reverse lookup entries for the Exchange virtual server, in the DNS.

Workaround

Manually update the DNS with the forward and reverse lookup entries for the Exchange virtual server and then run the wizard to perform the move database operation.

Veritas Enterprise Administrator (VEA) may fail to respond or may freeze (1533885)

This issue occurs if the vxob service is stopped abdruptly thereby causing a crash in the associated vxsvc service. The VEA GUI may either fail to respond or may freeze. As a result, all server connections from the VEA GUI are broken.

Workaround

Complete the following steps:

1. Stop the Veritas Storage Agent service.
   Type the following at the command prompt:
   ```
   net stop vxvm
   ```
2. Start the Veritas Enterprise Administrator Service.
   Type the following at the command prompt:
   ```
   net start vxob
   ```
3. Start the Veritas Storage Agent service.
   Type the following at the command prompt:
   ```
   net start vxvm
   ```

Unable to select RVG in an MSCS RVG resource while creating cluster resource (1483572; escalation incident: 1202082)

This issue occurs if you have upgraded from 5.0 and 5.0 RP1a to 5.0 RP2 on a Japanese Operating System that has VVR and MSCS installed. After upgrading to 5.0 RP2, the user is unable to select the RVG in an MSCS RVG resource.

To avoid this, the user needs to register the `mscsrvgresourceex.dll` by running the following commands:

- `regsvr32 mscsrvgresourceex.dll`
- `cluster /regext:mscsrvgresourceex.dll`

SQL instance running on 64-bit machine is not discovered by MOM 2005 server

A SQL Server 2005 instance running on a 64-bit cluster node is not discovered by the Microsoft Operations Manager (MOM) 2005 server. This problem occurs because the MOM 2005 agent is 32-bit while the SQL instance is 64-bit.

Workaround

Create the following registry key if it does not exist already in the 32-bit registry hive:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Microsoft SQL Server\Instance Names\SQL

Note: You need not create any registry value under this key.

Version conflict error while importing the VCS 5.1 SQL management pack for MOM 2005

A management pack version conflict error occurs when you try to import the VCS 5.1 management pack for SQL server in a Microsoft Operations Manager (MOM) 2005 monitoring environment. This occurs if you have already imported the Microsoft SQL Server 2005 management pack before you import the VCS management pack.

The following error is displayed:

Version of Rule Group 'State Monitoring and Service Discovery' - '09.0.3043.0000' should be newer than '10.1.0001.0000'.

Workaround

You can ignore the error and click **Continue** to proceed with the VCS management pack import process. There is no change in the SQL 2005

monitoring scripts included in the Microsoft SQL management pack version 10.1.0001.0000. The VCS management pack file (VCS_SQL2005_MOM2005.akm) version 09.0.3043.0000 will work as it is with Microsoft SQL management pack version 10.1.0001.0000.

Symantec Endpoint Protection security policy may block the VCS Cluster Configuration Wizard

While configuring a cluster, the VCS Cluster Configuration Wizard (VCW) may fail to ping systems that are selected to be a part of the cluster. As a result, you cannot configure the cluster.

This may happen in case Symantec Endpoint Protection (SEP) client is installed on the selected systems. VCW uses Internet Control Message Protocol (ICMP) to ping systems and ICMP traffic is blocked in SEP, by default.

Workaround

Create a custom rule in SEP to allow ICMP traffic in both directions. Ensure that you create this rule on all the systems that are going to be part of the cluster. Refer to the SEP documentation for instructions.

VCS cluster configuration fails if Symantec Endpoint Protection 11.0 MR3 version is installed

The VCS Cluster Configuration Wizard (VCW) fails to configure the cluster on systems where Symantec Endpoint Protection (SEP) 11.0 MR3 version is installed.

The following error is displayed:

Failed to start the cluster. Error=FFFFFFFF. Failed to start services on all the nodes.

Workaround

Perform the following steps to resolve this issue:

1. Create a custom rule in the SEP firewall rules table.
   Specify the following details for the rule:
   - Rule type: Application
   - Application name: llt.sys
   - Action: allow
2. Move this rule to the top of the firewall rules table and then apply the firewall policy again.
3. Ensure that the SEP clients on the systems receive this policy and then proceed with the cluster configuration task.

Refer to the SEP documentation for detailed instructions on creating custom firewall rules.

The Disaster Recovery Configuration Wizard may fail to perform the required disaster recovery configuration tasks (1536352)

This issue occurs while configuring disaster recovery using the Disaster Recovery Configuration Wizard (DR wizard). After specifying the storage cloning, service group cloning, replication and global cluster details when you click Next on the Summary panel, the DR wizard skips the Implementation panel and directly goes to the Finish panel. As a result, the wizard may fail to complete the required DR configuration tasks.

Workaround

Perform the following steps:

1. At the primary site, restart the Symantec Plug-in Host Service on the node on which the target service group is online.
   Type the following at the command prompt:
   net stop Plugin_Host
   net start Plugin_Host
2. Run the DR wizard again and complete the required steps.

Documentation Errata

The information in this section contains updated information that may be missing or are incorrect in the product documentation for Veritas Storage Foundation 5.0 for Windows.

Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide

This refers to Chapter 3, Upgrading to SFW 5.0, in the guide.

This chapter contains instructions for "Upgrading from previous 4.x versions." Certain steps are missing from the procedures mentioned for section "Re-enabling VVR in an environment without clusters" on page 87 of this guide.

The correct sequence in which these steps should be performed are as follows:

Re-enabling VVR in an environment without clusters

After you upgrade to SFW 5.0 from a 4.3 x version, you must re-enable VVR. Follow the procedures in the given order.

Warning: A full autosynchronization will be required if the procedures listed below are not performed in the given order.

To enable the updated objects

1 To associate the dissociated replicator log again, perform the following actions:

- From the VEA console on the primary site, expand the RDS. Right-click on the RVG and select the **Associate Replicator Log** option. Select the correct replicator log volume from the dialog box and click **OK**.
  or
- From the command line, type
  `vxrvg [-g <diskgroup_name>] [-f] aslog <rvg_name> <volume_name>`
  This command associates the specified replicator log volume with the RVG.
  Note that replication is not possible without the replicator log.

2 To attach the RLINK, run the following command:
`vxrlink -f [-g <diskgroup_name>] att <rlink_name>`
This command attaches one or more RLINKs to an RVG. If the `-f` option is used, then it forcefully associates the volumes.

The RLINK must already be associated with the RVG before the attach as show in step 1. For the attach to succeed, ensure that the data volumes on the secondary site are of the same name and size as on the primary site.

Warning: Use the `-f` option only when you are sure that the secondary site is completely up-to-date with the primary. Otherwise, this option can cause data corruption.

---

3 To enable data access and prepare the volumes to receive the writes from the application, perform one of the following actions:

- From the VEA console, select the primary RVG and then select **Enable Data Access** option from the right-click menu.

  or

- From the command line, type

  ```
  vxrvg [-g <diskgroup_name>] start <rvg_name>
  ```

  This command enables Input/Output access to the specified data volumes.

4 Repeat step 1 through step 3 on the secondary site.

5 If needed, perform any necessary tasks to start the replication. Depending on options available in your environment, these tasks may include mounting databases or manually starting the application.

Documentation

Product guides are available on the documentation disc in the PDF format. We recommend copying pertinent information, such as installation guides and release notes, from the disc to your system directory

This release includes the following documents.

Title	File Name
Veritas Storage Foundation™ and High Availability Solutions for Windows Release Notes	SFWHA_ReleaseNotes.pdf
Veritas Storage Foundation™ and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange 2007	SFW_HA_DR_E2K7_Solutions.pdf

Documentation feedback

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions to sfwha_docs@symantec.com.

Include the title and part number of the document (located in the lower left corner of the title page), and chapter and section titles of the text on which you are reporting.

Getting help

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

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