Veritas Storage Foundation™ and High Availability Solutions for Windows README

5.0 Rollup Patch 1a

Veritas Storage Foundation and High Availability Solutions README

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

Third-party legal notices

Third-party software may be recommended, distributed, embedded, or bundled with this product. Such third-party software is licensed separately by its copyright holder.

Technical support

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

Select phone or email support. Use the Knowledge Base search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and our customer email notification service

Storage Foundation and High Availability Solutions 5.0 RP1a README

Introduction

This document provides important information about the Veritas Storage Foundation and HA Solutions 5.0 Rollup Patch 1a (RP1a). Review this entire document before installing this patch.

This rollup patch applies to the following products:

- Veritas Storage Foundation 5.0 for Windows
- Veritas Storage Foundation HA 5.0 for Windows
- Veritas Cluster Server 5.0 for Network Appliance SnapMirror
- Veritas Cluster Server 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 this release

This section describes changes introduced in this release. For information on the fixed issues, refer to the Fixed Issues section.

See "Fixed Issues" on page 44.

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 6.
- 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 18.
  See "Installing support for Microsoft Exchange Server 2007" on page 25.
  See "Upgrading Exchange 2007 to Exchange 2007 SP1" on page 31.

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 "Installing client components on Windows Vista systems" on page 27.

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.

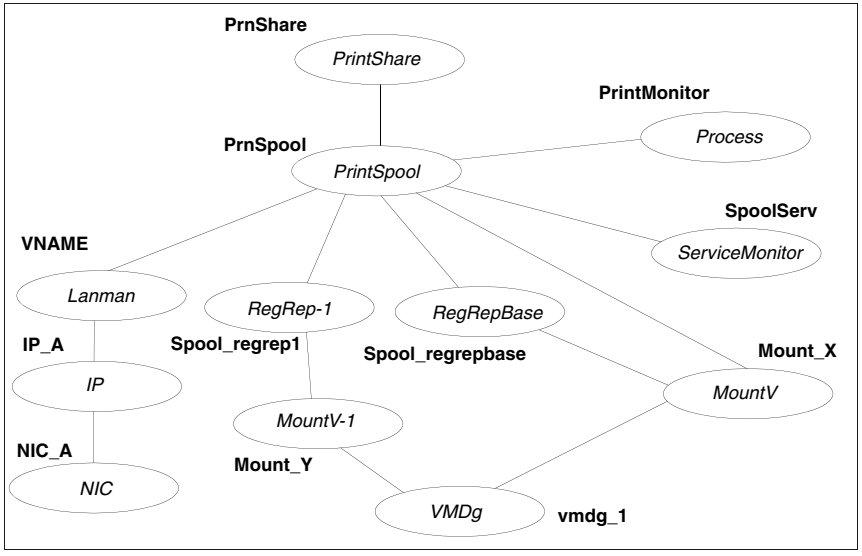
PrintShare agent changes

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 printshare 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 PrintShare 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 PrintShare 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 PrintShare service groups per the new changes to the PrintShare agent.

See "Modifying PrintShare service groups after installing the rollup patch" on page 30.

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

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

In addition to the software supported in release SFW HA 5.0, the Rollup Patch 1a includes support for the following:

- 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

  Note: Exchange 2007 SP1 is supported with SFW HA 5.0 Rollup Patch 1a only.

- Windows Vista

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 and removing the patch.

Download locations

Download packages for this release from the following locations:

Table 1-1 Download Paths

To install	Download packages from
SFW HA 5.0 RP1a (32-bit)	http://entsupport.symantec.com/docs/297166
SFW HA 5.0 RP1a (64-bit)	http://entsupport.symantec.com/docs/297167
Support for Exchange 2007	http://entsupport.symantec.com/docs/297165
Vista client (32-bit)	http://entsupport.symantec.com/docs/288604
Vista client (64-bit)	http://entsupport.symantec.com/docs/288607

Installation notes for Japanese locales

Storage Foundation for Windows 5.0 includes a Japanese language pack for Veritas Enterprise Administrator (VEA.) If you plan to install the language pack for VEA, you must do so before installing 5.0 RP1a.

Installing the language pack for VEA after installing SFW 5.0 RP1a is not supported.

This release of Veritas Cluster Server (VCS) does not include support for Japanese. After upgrading to 5.0 RP1a, VCS wizards display content in English.

Preparing to install the rollup patch

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.

- Only one instance of Veritas Storage Foundation 5.0 for Windows should be running on a system.

Preparing a VVR Environment

If you have VVR to replicate data from a primary site to a secondary site, use the following procedures to stop the replication. For additional information, refer to the *Veritas Volume Replicator 5.0 Administrator's Guide*.

- For sites with VVR and a cluster (either VCS or MSCS) the VVR steps in "Preparing a clustered VVR environment" on page 15 must be completed before preparing the cluster.
- For VVR sites without a cluster (VCS or MSCS), proceed to "Preparing a non-clustered VVR environment" on page 15.

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 sites in a clustered 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.

Preparing the cluster

- For a VCS cluster, proceed to "Preparing an SFW HA environment" on page 17.
- For an MSCS cluster, proceed to "Preparing an MSCS environment" on page 16.

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 DMP environment

If you have a previous installation of DMP on your system, disconnecting DMP paths should not be necessary for this Rollup Patch 1a update.

Always back up your data before upgrading.

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

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 18 or "Installing the rollup patch silently" on page 22.
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

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 RP1a.

See "Re-installing VCS Management Console 5.1" on page 29.

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
```

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 14.

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

For more information about installation and upgrades, refer to the *Veritas Storage Foundation and High Availability Solutions 5.0 for Windows Installation and Upgrade Guide*.

Setting Windows driver signing options

When installing on remote or local systems running Windows Server 2003, you must 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.

With the Group Policy Object, the driver signing options can be changed using Microsoft's Group Policy Object in a Windows 2000 or Windows Server 2003 domain.

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.

To install the rollup patch

1 Download the required packages.
See "Download locations" on page 13.

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, select one of the following options:

- Storage Foundation 5.0 Rollup Patch 1a for Windows
- Storage Foundation HA 5.0 Rollup Patch 1a for Windows
- VCS for Network Appliance SnapMirror Release Update Rollup Patch 1a 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 19 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 36.
- Repeat Rollup Patch 1a installation on that computer.
  See "Setting Windows driver signing options" on page 18 or "Installing the rollup patch silently" on page 22.

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 18.

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 1a 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.

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 "Tasks after installing the rollup patch" on page 29.

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 14.

Use the command `Setup.exe` to perform a silent installation. With a silent installation, you can install on only one computer at a time. The rollup patch is installed to the same directory as the 5.0 base installation.

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

To start the installation from the command window

1. Download the required packages.
   See "Download locations" on page 13.
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 1a:

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

7. Reboot the system at the end of installation to ensure that the rollup patch is installed correctly.

Parameters for Setup.exe

Information about the possible parameter values 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 1a for Windows ***2*** = Storage Foundation HA 5.0 Rollup Patch 1a for Windows ***6*** = VCS 5.0 Rollup Patch 1a 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=*1***

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 RP1a.

See "Installing the rollup patch using the GUI" on page 18.

To install the VCS agent for Exchange Server 2007

1. Download the required packages.
   See "Download locations" on page 13.
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 31.

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*.

Installing client components on Windows Vista systems

This section describes how to install client components on Windows Vista systems.

To install the SFW 5.0 or SFW HA 5.0 client components on Windows Vista

1. Download and required packages.
   See "Download locations" on page 13.
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. When the Product Selection screen appears, select one of the three options for installation:
   - Storage Foundation 5.0 for Windows Vista (Client Components)
   - Storage Foundation HA 5.0 for Windows Vista (Client Components)
   - VCS 5.0 for NetApp SnapMirror for Windows Vista (Client Components) - This option is not available when installing on a 64-bit machine.

   Click **Next** when done.
5. Review the prerequisites listed in the Welcome screen and click **Next**.
6. In the Computer Selection screen, select the domain and computer for the installation by using one of the following options:
   - Using the dropdown boxes, select the **Domain** and **Computer**, and then click **Add**.
   - Type the Computer name in the text box and then click **Add**.

   Note: It could take a few minutes for the domain and computer names to appear in the dropdown boxes. Once you select a computer, its name and its operating system appear onscreen, and the computer name, OS, and install path appear in the Description panel. In addition, the default installation path appears in the Install Path box as C:\Program Files\Veritas\. To change the path, click **Change** and type the desired path.

   When you are done, click **Next**.
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 Once the computer has been validated and you have reviewed any comments, click **Next**.

9 In the Summary screen, review the information and click **Install**. Click **Back** to make changes, if necessary.

10 The Installation Status progress meter displays status messages and the progress of the installation.
If the 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 re-install.

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

12 Click **Finish** to complete the process and close the window.

Tasks after installing the rollup patch

Tasks after installing the rollup patch may include the following tasks, depending on the environment at the site:

Note: If a feature is added after installing 5.0 Rollup Patch 1a, 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

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 17.
3. Start the VCS Management Console. If the management console is clustered, bring the CMC_MS service group online.

Modifying PrintShare service groups after installing the rollup patch

After installing the rollup patch, you must run the Print Share Configuration Wizard to modify existing printshare service groups. 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.

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 printshare 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.

Upgrading Exchange 2007 to Exchange 2007 SP1

This section describes how to upgrade an existing Exchange 2007 installation to Exchange 2007 SP1. 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*.

Prerequisites

- Ensure that you have installed one of the following products on all the cluster nodes:
  - SFW HA 5.0 Rollup Patch 1a
  - VCS 5.0 Rollup Patch 1a 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 25.

Upgrade steps

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

This procedure assumes a single Exchange virtual server instance configured on a two-node cluster configuration.

Table 1-2 Exchange 2007 SP1 upgrade configuration objects

Object	Description
Node1, Node2	Physical node names
EVS1	Exchange virtual server name

To upgrade Exchange 2007 to Exchange 2007 SP1

1 Take the Exchange 2007 service group offline in the cluster.
   - From the VCS Java Console, right-click the service group and select the **Offline** menu option.

2 Delete the Exchange virtual server computer object, EVS1, from the Active Directory.
   - Open Active Directory Users and Computers console and click **Computers** in the left pane.
   - From the right pane, right-click the Exchange virtual server computer object, EVS1, and then click **Delete**.
   - Click **Yes** to confirm the deletion.

3 Rename the cluster node, Node1. The new name of the node should be the Exchange virtual server name, EVS1.
   Make a note of the actual physical name of the node. We will restore the node name later in this procedure.

4 Restart the cluster node.

5 Stop the Veritas High availability daemon, HAD, on all the cluster nodes.
   Type the following at the command prompt:
   ```
   C:\>hastop -all -force
   ```

6 Install Exchange 2007 SP1 in the upgrade mode.
   Type the following at the command prompt:
   ```
   <drive letter>:\setup.com /mode:Upgrade
   ```
   where <drive letter> is the drive where the Exchange software is located.

7 Verify that the installation has completed successfully. Refer to the Microsoft Exchange documentation for more information.

8 From the services console, set the startup type of all the Exchange 2007 services to Manual, and ensure that the services are stopped.

9 Rename the cluster node, EVS1, to its original physical name, Node1.

10 Restart the cluster node.

11 From the command prompt, run the Exchange 2007 Setup wizard for VCS to update the registry information on the node. Type the following command:
   ```
   <%vcs_home%>:\bin\Exch2007Setup>Exch2007Setup.exe
   /UpdateExchVersion
   ```
   The variable %VCS_HOME% is the default installation directory for VCS, typically C:\Program Files\Veritas\cluster server.

12 Repeat step 3 to step 11 on the remaining cluster node, Node2.
   If there are additional nodes, 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.

13 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

If there are multiple Exchange virtual server instances in the cluster (an any-to-any configuration), the upgrade flow varies slightly. Referring to the example used earlier, let's consider another Exchange virtual server, EVS2, configured on Node3. The configuration is such that:

- EVS1 can failover on Node1 and Node2.
- EVS2 can failover on Node3 and Node2.

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

In this case, run the upgrade steps for EVS1 on Node1 and Node2. Then, run the upgrade steps for EVS2 on Node3 only.

You do not need to upgrade Node2 (the common failover node) for EVS2, as Exchange 2007 SP1 is already installed on Node2, while upgrading for EVS1.

In general, for every Exchange virtual server instance in the cluster, you must run the upgrade steps on at least one physical node in the cluster.

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.

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 begin replication.

- For sites with VVR and a cluster (either VCS or MSCS), re-enable VVR before preparing the cluster.
  See"Re-enabling VVR in a cluster environment after the update" on page 34.
- For sites without a cluster (VCS or MSCS), proceed to "Re-enabling VVR in an environment without clusters" on page 35.

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 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*.

Removing the rollup patch

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.

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 RP1a.

Preparing the SFW HA 5.0 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 procedure removes 5.0 Rollup Patch 1a. 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*.

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 RP1a.

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 1a for Windows
   - Storage Foundation HA 5.0 Rollup Patch 1a for Windows
   - VCS 5.0 Rollup Patch 1a 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.

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 1a. 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.

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.

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 1a for Windows ***2*** = Storage Foundation HA 5.0 Rollup Patch 1a for Windows ***6*** = VCS 5.0 Rollup Patch 1a 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

Tasks after removing the rollup patch may include the following tasks, depending on the environment at the site:

- "Restoring the printshare service groups" on page 40
- "Modifying the cluster configuration (VCS for NetApp SnapMirror only)" on page 41

Restoring the printshare service groups

After removing the rollup patch, the printshare 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 printshare service group and recreate it using the Print Share Configuration Wizard.

Complete the following steps to restore the printshare configuration:

To restore the printshare service group

1. From the VCS Java Console, select the printshare 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 printshare service group.

- Click **OK** and then close the Edit Attribute window.

4 Bring the printshare 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 1a, you must manually modify the cluster configuration otherwise the cluster may go in to a STALE ADMIN WAIT state.

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.

Repairing the installation

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

Caution: You can only repair SFW. Do not attempt to repair SFW HA or VCS for Network Appliance SnapMirror.

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 1a 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.

Fixed Issues

Fixed issues and software enhancement requests are referenced by incident numbers and described briefly below.

This section is divided into the following topics:

Veritas Storage Foundation

The following table describes Veritas Storage Foundation for Windows fixed issues and enhancements included in this release.

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 1-3 Fixed issues: 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.)

Table 1-3 Fixed issues: Veritas Storage Foundation

Incident Number	Description
1005208	I/O hang occurs when the server is low on free kernel memory. (Related to escalation incident 996007.)
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.)

Table 1-3 Fixed issues: Veritas Storage Foundation

Incident Number	Description
1093865	Incorrect track alignment value for IBM DS8000 storage array displayed in VEA GUI. (Related to escalation incident 1038446.)
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.

Table 1-3 Fixed issues: Veritas Storage Foundation

Incident Number	Description
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.)
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.)

Table 1-3 Fixed issues: Veritas Storage Foundation

Incident Number	Description
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

This section lists fixes and enhancments for Veritas Cluster Server.

Table 1-4 Fixed issues: 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 1-4 Fixed issues: 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 1-4 Fixed issues: 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 1-4 Fixed issues: 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

This section lists fixes and enhancements for Veritas Volume Replicator.

Table 1-5 Fixed issues: 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.
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

Error while performing Exchange post-installation steps (1200931)

The Exchange Setup Wizard displays the following error when you click **Continue** during the Exchange post-installation:

```
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 occurs 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.

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.

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.

Printshare service group fails to come online after removing the rollup patch

Rollup patch is installed on a cluster which had printshare service groups configured. After the installation, the existing printshare 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 printshare 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 printshare service group configuration before bringing it online.

See "Restoring the printshare service groups" on page 40 for instructions.

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

This issue is similar to the Print Share issue mentioned earlier. After removing the rollup patch, the printshare 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 printshare service group configuration before bringing it online or modifying it using the Print Share Configuration Wizard.

See "Restoring the printshare service groups" on page 40 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 printshare service group with 1000 printshares 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.

Disaster Recovery wizard may not display the storage cloning summary (1189431)

While configuring a disaster recovery setup using the DR wizard, the Storage Configuration Cloning Summary panel may not display the storage cloning summary.

The following message is displayed:

```
The XML page cannot be displayed.

Cannot view XML input using XSL style sheet. Please correct
the error and then click the Refresh button, or try again
later.

The specified resource name cannot be found in the image
file.
```

However, you can click **Next** and continue with the DR configuration tasks.

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.

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 README	README.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.