# Veritas InfoScale Patch Readme

## Windows

## 7.0.1

December 2015

VERITAS™

# Veritas InfoScale 7.0.1 Patch Readme

This document includes the following topics:



## Changes introduced in this patch

The InfoScale 7.0.1 patch is a maintenance-level release over InfoScale 7.0. It provides enhanced authentication using 2048-bit key and SHA-256 signature certificates and OpenSSL 1.0.1. This patch also includes several hot fixes that contain enhancements to the products and fixes for issues that were reported.

The following hot fixes are listed for this patch:

- Hotfix_7_0_00001_129_3853667
- Hotfix_7_0_00001_3851239
- Hotfix_7_0_00002_3855992

For details on these and the other related changes:

- See "Fixed issues" on page 10.
- See "Implementing enhanced security for clusters" on page 5.

# Before you install

Review and address the following requirements before you install the patch:

- Download the appropriate compressed patch file to a temporary location on your system. Then, extract the contents of this file to access the patch installer.
- Ensure that the logged-on user has privileges to install the patch on the system.
- Ensure that the **Startup Type** of the VCS Authentication Service is set to **Automatic**.
  This is applicable only if you have configured a secure cluster.
- In case of a clustered environment, Veritas recommends that you create any clusters that you need beforehand.
- One or more hot fixes that are included in a patch may require a restart. Ensure that you can restart the system without disrupting any ongoing operations.
- Close the Windows Event Viewer.
- Veritas recommends that you close the Cluster Manager (Java Console) and the Veritas Enterprise Administrator (VEA) before installing this patch.

# About Veritas Patch Installer

Veritas provides a wizard, the Veritas Patch Installer, to install or uninstall patches for the Veritas InfoScale products.

During installation, the wizard performs the following tasks:

- Extracts all the individual hot fix executable files to the following location:

  `%commonprogramfiles(x86)%\Veritas Shared\WxRTPrivates\`*`patchName`*

- Runs the preinstallation tasks
- Installs all the hot fixes sequentially

- Runs the post-installation tasks

See "Installing the patch" on page 4.

During uninstallation, the wizard performs the following tasks:

- Uninstalls the hot fixes that are part of the selected patch
- Runs the post-uninstallation tasks

See "Uninstalling the patch" on page 7.

---

**Note:** The patch installer identifies the product that is installed on the system and installs only those hot fixes or files that are applicable to that product. For example, if you run the patch installer on a system where InfoScale Storage is installed, it skips the InfoScale Availability-related hot fixes or files.

---

# Installing the patch

The following procedures describe how to install a patch using the wizard or from the command-line patch installer.

For information on the command-line batch utility for this task:

See "About the command-line utility for the patch" on page 8.

**To install the patch using the wizard**

1. Double-click the patch executable file to launch the Veritas Patch Installer.
2. On the Welcome panel, review the prerequisites, make sure that they are met, and then click **Next**.
3. On the Pre-install Summary panel, review the hot fixes that will be installed as part of the patch, and click **Install**.
4. On the Installation panel, watch the status of the installation as it happens, and click **Next** when it completes.

   Optionally, click **Save As Report** to save the installation report for your records.

   A message box displays the name and location of the report; click **OK** to close it.
5. On the Post-install Summary panel, review the installation status of the hot fixes that are part of the patch.

   Click the appropriate link to view the patch installation log or the hot fix installation log.

   Click **Finish** to close the installer.

**To install the patch from the command line**

1. Open the command prompt at the location where you extracted the patch installer files.
2. Run the following command to install the patch:

   *patchName*.exe /install

   Replace *patchName* with the patch file name, for example: Veritas_InfoScale_701.

   Alternatively, if you want to perform a silent installation, run the command:

   *patchName*.exe /install /silent
3. After the installation is complete, the installer prompts you to restart the system only if it has installed any hot fixes that require a system restart.

   If you see the prompt, type **Y** and press **Enter** to restart the system.

---

**Note:** You can use this command-line method to only install the patch or to extract the other related executable files. You cannot uninstall the patch or view the patch details in this manner.

---

## Post-installation tasks

To verify whether the patch is installed, open the Programs and Features window and look for the patch name.

In case of a clustered environment, create any necessary clusters if you had not created them before you installed the patch. Then, run the following batch file:

```
C:\Program Files (x86)\Common Files\Veritas
Shared\WxRTPrivates\Hotfix_7_0_00001_3851239\InstallVMwareDisksType.bat
```

# Implementing enhanced security for clusters

The updated Cluster Server components use 2048-bit key and SHA-256 signature certificates. The VCS Authentication Service, which provides secure communication between cluster nodes, generates certificates with a 2048-bit key and an SHA-256 signature. This enhancement provides stronger security to VCS users.

The 2048-bit key and SHA-256 signature certificates are deployed when you install the 7.0.1 patch. If you configure a cluster after applying this patch, these certificates are used by default.

**Note:** If some of the clusters in a global cluster setup run on 6.x or earlier versions of the Cluster Server components, the inter-cluster communication fails.

To upgrade a global cluster setup to use enhanced security

1. Upgrade the clusters at all the sites to InfoScale Availability 7.0 or InfoScale Enterprise 7.0, if they were created using 6.x or older versions of the products.

   For more information about upgrading to 7.0, see the *Veritas InfoScale Installation and Upgrade Guide*.

2. Install the 7.0.1 patch.

   See "Installing the patch" on page 4.

3. Upgrade any existing cluster to use enhanced security.

   See "Upgrading clusters to use enhanced security" on page 6.

# Upgrading clusters to use enhanced security

If you have configured any secure clusters in your environment, upgrade them to use the 2048-bit key and SHA-256 signature certificates, which provide enhanced security. Make sure that you have installed the 7.0.1 patch.

**To upgrade a cluster to use enhanced security**

- Reconfigure the secure cluster using the Cluster Configuration Wizard.

  **Note:** On the **Reconfigure Cluster Options** panel, select **Configure/Reconfigure Single Sign-on**.

  For more information on reconfiguring a cluster, see the *Cluster Server Administrator's Guide*.

**To upgrade a cluster to use enhanced security on a Windows Server Core system**

**1** Back up your cluster configuration by creating a copy of the `main.cf` file.

**2** Use the `VCWsilent` utility to perform the following operations sequentially:

- Delete the cluster.
- Create a new cluster.

The syntax is as follows:

```
VCWsilent XML_file_name_including_path
```

For more information on the `VCWsilent` utility and the XML file formats to be used with it, see the *Cluster Server Administrator's Guide*.

3 Stop the cluster using the following command:

```
hastop -all -force
```

4 Manually restore your application configurations by copying only the relevant entries from the backed-up `main.cf` to newly created `main.cf`.

5 Start the cluster using the following command:

```
hastart
```

# Uninstalling the patch

The following procedure describes how to uninstall a patch using the wizard.

For information on the command-line utility options for this task:

See "About the command-line utility for the patch" on page 8.

---

**Caution:** Veritas recommends that you do not uninstall a patch unless there is a pressing reason to do so.

---

**To uninstall the patch using the wizard**

1 On the Programs and Features window, select the patch that you want to uninstall, and click **Uninstall/Change** to launch the Veritas Patch Installer.

2 On the Welcome panel, review the prerequisites, make sure that they are met, and then click **Next**.

3 On the Pre-uninstall Summary panel, review the hot fixes that are installed and the ones that cannot be uninstalled, and click **Uninstall**.

4 On the Uninstallation panel, watch the status of the uninstallation as it happens, and click **Next** when it completes.

Optionally, click **Save As Report** to save the uninstallation report for your records.

A message box displays the name and location of the report; click **OK** to close it.

5 On the Post-uninstall Summary panel, review the uninstallation status of the hot fixes that are part of the patch.

Click the appropriate link to view the patch uninstallation log or the hot fix uninstallation log.

Click **Finish** to close the installer.

# Recovering a cluster after uninstalling this patch

If you accidentally uninstall a patch, or if you have to uninstall it for some unavoidable reason, your cluster may fail. You must perform certain tasks to recover your cluster configuration and the related operations.

**To recover a cluster configuration after uninstalling this patch**

1 Make sure that you have restarted the system after uninstalling the patch.

2 Repair the base product.

For more information, see the Veritas InfoScale Installation and Upgrade Guide.

3 Reconfigure the secure cluster using the Cluster Configuration Wizard.

---

**Note:** On the Reconfigure Cluster Options panel, select **Configure/Reconfigure Single Sign-on**.

---

For more information on reconfiguring a cluster, see the *Cluster Server Administrator's Guide*.

# About the command-line utility for the patch

Veritas provides a command-line utility, `VxHFBatchInstaller.exe`, that lets you perform various patch-related operations.

**To access the utility**

1. Open the command prompt at the location where you extracted the patch installer files and locate the *patchName*.exe file, for example: Veritas_InfoScale_701.exe.
2. Run the following command to extract the executables files for the patch:

   *patchName*.exe /x

   By default, the files are extracted to %commonprogramfiles(x86)%\Veritas Shared\WxRTPrivates*patchName*.

   The %commonprogramfiles(x86)% environment variable points to the default 32-bit Program Files location.
3. Make sure that you can locate the VxHFBatchInstaller.exe file.

## Installation options

VxHFBatchInstaller.exe /Patch:*patchName*
[/PreInstallScript:PreInstallScript.pl] [/silent [/forcerestart]]

Here, *patchName* represents the patch file name, for example: Veritas_InfoScale_701.

The PreInstallScript.pl file is a Perl script that includes the preinstallation steps. These steps forcefully kill the required services and processes if a graceful stop request does not succeed. Veritas recommends that you use this option only if the patch installer fails repeatedly while performing the preinstallation tasks.

Use the command as follows:

- To install a patch and provide specific responses to any questions that the installer prompts:

  VxHFBatchInstaller.exe /Patch:*patchName*
- To install a patch in the silent mode:

  VxHFBatchInstaller.exe /Patch:*patchName* /silent

  If you use the silent option, the installer does not prompt for any inputs during the installation.
- To restart the system automatically after the installation is complete:

  VxHFBatchInstaller.exe /Patch:*patchName* /silent /forcerestart

  You can use the forcerestart option only in combination with the silent option.

**Note:** Using the `forcerestart` option forces a system restart only if any hot fix in the patch requires it. If none of the hot fixes in the patch require a restart, this option has no effect on the system.

### Uninstallation options

```
VxHFBatchInstaller.exe /Uninstall [/Silent [/Suppress]]
```

Use the command as follows:

- To uninstall the patch:

  ```
  VxHFBatchInstaller.exe /Uninstall /Silent
  ```

  Note that the `Silent` option is mandatory.

- To suppress all the prompts during the installation:

  ```
  VxHFBatchInstaller.exe /Uninstall /Silent /Suppress
  ```

  Using the `Suppress` option provides an affirmative response to all the installation prompts in the background so that you do not have to respond manually. If any of the hot fixes in the patch require a restart, the system restarts automatically if you provide this option.

### Patch identification options

Additionally, you can also use the utility as follows to review information about the patch and its hot fixes:

- To view the latest patch installed on the system:

  ```
  VxHFBatchInstaller.exe /patchlevel
  ```

  This command displays the latest patch that is installed, the patch status, and a list of all the hot fixes that are a part of the patch but are not installed on the system.

- To view a list of all the patches installed on the system:

  ```
  VxHFBatchInstaller.exe /list
  ```

  This command displays a list of patches that are installed and the corresponding hot fixes. It also displays a list of hot fixes that are a part of a patch but are not installed on the system.

# Fixed issues

The following table lists the issues that were fixed in this patch and the hot fixes that were used to deliver the fixes:

| Incidents | Details |
|---|---|

| Incidents | Details |
|---|---|
| Incident:<br>**3853667**<br>Tracking ID:<br>3853666 | **Symptom:** The VVRRVG resource fails intermittently during a takeover or a failback operation.<br>**Description:** The read-write permissions on a volume are changed when migrating it from one system to another. The VVRRVG agent was unable to handle this change. A volume is migrated during a takeover or failback operation. Therefore, during such operations, the agent reported the VVRRVG resource as Faulted.<br>**Resolution:** This hot fix addresses the issue by updating the VVRRVG agent, which now interprets the change of permissions on a volume based on the status of a flag. The agent is now able to handle the change, and the VVRRVG resource no longer faults.<br>**Changed file / version:**<br>vxconfig.dll / 7.0.1.129 |
| Incident:<br>**3787075**<br>Tracking ID:<br>3775638 | **Symptom:** After a failover, the VMDg resource in a File Server role hangs in an 'Online Pending' state.<br>**Description:** After a failover of VMDg resource in a File Server role, the resources are brought online in the following order: VMDg->File Server->Network name. During the online process, the VMDg resource queries the Network name to recreate the file shares. However, if the Network name resource hasn't restarted until then, the VMDg resource remains in an 'Online Pending' state and hangs after the resource hosting subsystem crashes due to the time out.<br>**Resolution:** This hot fix modifies the VMDg resource online process to address the issue. To recreate the file shares, the VMDg resource now queries the File Server resource instead of the Network name resource. After a failover, the File Server resource restarts before the VMDg resource queries it. This behaviour prevents the VMDg resource to go in an 'Online Pending' state.<br>**Changed file / version:**<br>vxres.dll / 7.0.1.129<br>cluscmd.dll / 7.0.1.129 |

| Incidents | Details |
|---|---|
| Incident:<br>**3821353**<br>Tracking ID:<br>3819634 | **Symptom:** The storage reclamation operation may hang or fail, and the system may become unresponsive on an array that supports the UNMAP command. These issues are seen only on Windows Server 2012/R2.<br>**Description:** SFW wizards and CLI commands provide support for reclaiming the unused storage from the disks that support reclamation. If these disks belong to an array that supports the UNMAP command, the SFW operations that are initiated for reclamation may fail.<br>As a result, the system becomes unresponsive. This issue may occur because of a deadlock in vxio.sys.<br>This issue may also occur when a TRIM command fails with status 'STATUS_DATA_OVERRUN'.<br>**Resolution:** The SFW behaviour to reclaim the unused storage has been modified as part of this hot fix.<br>SFW now overcomes the deadlock faced in the vxio.sys during the reclamation of the unused storage.<br>Also, a TRIM command with status 'STATUS_DATA_OVERRUN' is now considered as a successful operation.<br>**Changed file / version:**<br>vxio.sys / 7.0.1.129<br>vxconfig.dll / 7.0.1.129 |
| Incident:<br>**3850785**<br>Tracking ID:<br>3839096 | **Symptom:** SFW broadcasts the license keys over the network on the UDP port number 2164.<br>**Description:** Even though the network duplication check is disabled, SFW broadcasts the license keys on UDP port 2164 every 30 minutes. SFW broadcasts these license keys with LIC_CHECK_SEND in the header.<br>**Resolution:** This hot fix resolves the issue by disabling the broadcast if the network duplication check is disabled.<br>**Changed file / version:**<br>sysprov.dll / 7.0.1.129 |

| Incidents | Details |
|---|---|
| Incident:<br>**3850945**<br>Tracking ID:<br>3838759 | **Symptom:** A system crashes when excessive number of large write I/O requests are received on volumes mirrored using DRL.<br>**Description:** A system crashes when excessive number of I/O requests that involve more than 1MB of data write operations are received, on a volume that is mirrored using DRL. The issue occurs because of the excessive number of large write I/O requests that result in low System Page Table Entries (PTEs). As a result of low system PTE, the SFW driver fails to map the application I/O buffer to the system address space.<br>**Resolution:** The SFW behavior to map the application I/O buffer to the system address space has been modified as part of this hot fix. SFW now breaks the larger I/Os into smaller I/Os and then tries to map the application buffer into system address space.<br>**Changed file / version:**<br>vxio.sys / 7.0.1.129 |
| Incident:<br>**3851224**<br>Tracking ID:<br>3767110 | **Symptom:** Mirrored volumes with DCO log volumes and DRL logs are not resynchronized using DRL, after a system crash.<br>**Description:** This issue occurs for mirrored volumes with Disk Change Object (DCO) log volumes and Dirty region logging (DRL) logs in case of a system failure. Here, instead of using DRL to quickly resynchronize all the copies of a mirrored volume, the system restores all mirrors of the volume by copying the full contents of the volume between its mirrors. This is a lengthy and I/O intensive process.<br>**Resolution:** This hot fix resolves the issue by modifying SFW behaviour.<br>**Note:** If your existing mirrored volumes have DCO log volumes and DRL logs, you must delete and then recreate the DRL logs.<br>**Changed file / version:**<br>vxio.sys / 7.0.1.129<br>vxboot.sys / 7.0.1.129<br>vxconfig.dll / 7.0.1.129 |
| Incident:<br>**3851278**<br>Tracking ID:<br>3842736 | **Symptom:** Onlining or offlining of a Volume Manager Disk group (VMDg) resource causes the Resource Host Monitor (RHS.exe) service to crash.<br>**Description:** This issue occurs in a clustered environment with groups and VMDg resources. During the onlining or offlining of a VMDg resource, when the code tries to read memory beyond the allocated boundary, the RHS.exe service crashes.<br>**Resolution:** This hot fix resolves the issue by increasing the memory allocation to avoid the buffer over-run.<br>**Changed file / version:**<br>vxres.dll / 7.0.1.129 |

| Incidents | Details |
|---|---|
| Incident:<br>**3851722**<br>Tracking ID:<br>3826318 | **Symptom:** When you add a large number of disks and perform a Rescan, the VEA GUI hangs on the 'Disks View'.<br>**Description:** This issue occurs when you add a large number of Logical Units (LUNs) or disks to the host and perform a Rescan. When you select the 'Disks View' on the VEA GUI, the GUI stops responding.<br>**Resolution:** This issue has been resolved by adding two VEA Refresh Timeout tunables.<br>You can use the following tunables to control the intervals in which the view is refreshed:<br>■ `Quick Refresh Timeout`<br>It is the minimum time interval after which any change will reflect in GUI. The `Quick Refresh Timeout` value can range in between 20 to 2500 milliseconds.<br>■ `Delayed Refresh Timeout`<br>It is used to optimize these refreshes in case of a large number of events or notifications. If a large number of notifications come in the 'quick refresh timeout' time interval, then instead of refreshing the view in the 'quick refresh timeout' time interval, the 'delayed refresh timeout' time interval is used. The `Delayed Refresh Timeout` value can range in between 100 to 25000 milliseconds.<br>For example, suppose the Quick Refresh Timeout is set at 20ms, and the Delayed Refresh Timeout is set at 100ms. When the first update notification comes, the view is refreshed after 20ms. However, if more than one update notifications come in the 20ms time interval, then instead of refreshing the view after 20ms, the view is refreshed after 100ms.<br>To access these tunables, select **Preferences** from the **VEA Tools** menu. In the dialog box that appears, select the Advanced tab.<br>**Note:** The value for the VEA Refresh Timeout tunables will vary depending on your environment.<br>**Changed file / version:**<br>VxVmCE.jar / 7.0.1.1<br>OBGUI.jar / 7.0.1.1<br>ci.jar / 7.0.1.1<br>obCommon.jar / 7.0.1.1 |

| Incidents | Details |
|---|---|
| Incident:<br>**3852370**<br>Tracking ID:<br>3849187 | **Symptom:** The VEA GUI displays incorrect status for the historic data collection even after you have disabled it.<br>**Description:** When you stop the historical data collection, the VVR provider records the state in the ISIS bus. The ISIS bus gets updated whenever an event, like RLINK disconnect, is triggered. During this update cycle, the default Started state of the historical data collection is populated in the ISIS bus. Due to this, even though the historical collection is stopped, the VEA GUI displays 'Stop Historical Data Collection'.<br>**Resolution:** This hot fix resolves the issue by ensuring that the ISIS bus picks up the correct state of the historical data collection.<br>**Changed file / version:**<br>vvr.dll / 7.0.1.129<br>vxrlink.exe / 7.0.1.129<br>vvrcli_msgs.dll / 7.0.1.129 |
| Incidents:<br>**3851239**<br>and<br>**3855992**<br>Tracking ID:<br>- | **Symptom:** The Cluster Server components use older authentication and security mechanisms<br>**Description:** The Cluster Server components use 1024-bit key and SHA-1 signature certificates and a vulnerable version of OpenSSL, due to which the security of clustered systems might be compromised.<br>**Resolution:** The Cluster Server authentication components are now updated to use enhanced security provided by 2048-bit key and SHA-256 signature certificates and OpenSSL 1.0.1.<br>**Changed file / version:** Several files related to the Cluster Server components are updated. |
| Incident:<br>**3810019**<br>Tracking ID:<br>3773915 | **Symptom:** The Lanman resource fails to come online due to certain DNS settings.<br>**Description:** This issue occurs if your setup uses CNAME records instead of HOST (A) records for the virtual name. The Lanman agent faults when it performs a duplicate name check, because it incorrectly looks at non-HOST records.<br>**Resolution:** This hot fix addresses the issue by updating the Lanman agent to look at only the HOST records from a DNS query.<br>**Changed file / version:**<br>Lanman.dll / 7.0.1.104 |

| Incidents | Details |
|---|---|
| Incident:<br>**3850735**<br>Tracking ID:<br>3521503 | **Symptom:** When bringing the Lanman resource online, the Lanman agent checks whether the virtual server name is alive. If the virtual server name is alive, the resource faults.<br>**Description:** This issue occurs if your setup contains DNS entries that point to a virtual IP address that is online. The Lanman agent faults when it performs a duplicate name check.<br>**Resolution:** This hot fix addresses the issue by updating the Lanman agent to skip the duplicate name check.<br>After you apply this ho tfix, perform the following tasks on all the nodes in the cluster<br>**1** Open the registry editor.<br>**2** Navigate to the registry key:<br>`HKLM\SOFTWARE\VERITAS\VCS\BundledAgents\Lanman\`*`lanmanResourceName`*<br>or<br>`HKLM\SOFTWARE\VERITAS\VCS\BundledAgents\Lanman\__GLOBAL__`<br>**3** Create the DWORD key 'DisablePingCheckForDND' with the value '1'.<br>**Note:** If you create this tunable parameter under the '__GLOBAL__' key, it applies to all the Lanman resources configured in the cluster.<br>**Changed file / version:**<br>Lanman.dll / 7.0.1.104 |

| Incidents | Details |
|---|---|
| Incident:<br>**3850737**<br>Tracking ID:<br>3615728 | **Symptom:** VMwareDisks agent supports only 'persistent' virtual disk mode.<br>**Description:** The VMwareDisks agent currently supports only 'persistent' virtual disk mode. If you have configured the disk in 'independent' mode, in the event of a failover, the VMwareDisks agent sets the mode to 'persistent'.<br>**Resolution:** The behaviour of VMwareDisks agent is modified through this hot fix. The VMwareDisks agent now supports 'independent' disk mode. An attribute 'VirtualDiskMode' is now added to the VMwareDisks agent's attributes. You can set the value of this attribute to 'persistent', 'independent_persistent' or 'independent_nonpersistent'. By default the value is set to 'persistent'. You must modify the value after you configure application monitoring.<br>**Note:** The VMwareDisks agent does not detect the mode in which the disk is configured. After a fail over the disk is attached in the mode as that defined in the attribute value. For more details about the disk modes, refer to VMware documentation.<br>To modify the value use the VCS Java Console or perform the following steps through command line<br>**1** If you have configured the disk in 'persistent' mode, bring the service group offline:<br>`hagrp -offline service_group -sys systemName`<br>**2** Change the cluster configuration to read-write mode:<br>`haconf -makerw`<br>**3** Modify the attribute value:<br>`hares -modify resourceName VirtualDiskMode independent_persistent`<br>**4** Save the cluster configuration and change the mode to read-only:<br>`haconf -dump -makero`<br>**Changed file / version:**<br>VMwareDisks.dll / 7.0.1.104<br>VMwarelib.dll / 7.0.1.104<br>VMwareDisks.xml / - |

| Incidents | Details |
|---|---|
| Incident:<br>**3850742**<br>Tracking ID:<br>3820747 | **Symptom:** The NativeDisks agent takes longer than expected to bring a NativeDisks resource online or to take it offline.<br>**Description:** In large configurations with systems that have many high-capacity disks attached, the NativeDisks agent does not work efficiently.<br>**Resolution:** This hot fix addresses the issue by enhancing the NativeDisks agent to work more efficiently in large configurations.<br>**Note:** Veritas recommends that you set the NumThreads attribute of the NativeDisks agent to 1; otherwise, the agent may fail intermittently.<br>**Changed file / version:**<br>NativeDisks.dll / 7.0.1.104 |
| Incident:<br>**3851046**<br>Tracking ID:<br>3820747 | **Symptom:** The VMwareDisks agent takes longer than expected to bring a VMwareDisks resource online or to take it offline.<br>**Description:** In large ESX or vCenter configurations with lots of datastores, the VMwareDisks agent does not work efficiently.<br>**Resolution:** This hot fix addresses the issue by enhancing the VMwareDisks agent to work more efficiently in large ESX or vCenter configurations.<br>**Note:** Veritas recommends that you set the NumThreads attribute of the VMwareDisks agent to 1; otherwise, the agent may fail intermittently.<br>**Changed file / version:**<br>VMwareDisks.dll / 7.0.1.104<br>VMwarelib.dll / 7.0.1.104 |
| Incident:<br>**3850743**<br>Tracking ID:<br>3831005 | **Symptom:** The Disaster Recovery Configuration Wizard does not set the AutoStartList attribute when creating an RVG service group.<br>**Description:** The Disaster Recovery Configuration Wizard creates an RVG service group as part of configuring disaster recovery (DR) for a cluster. However, when creating the RVG service group, the wizard does not automatically populate its AutoStartList attribute with the names of the nodes in that cluster. If, for some reason, all the cluster nodes restart at the same time, the cluster does not know which node to bring the RVG online on, because AutoStartList is empty. Since the RVG is not online, the replication does not start automatically. In such a scenario, the AutoStartList attribute needs to be updated manually so that the replication can start automatically.<br>**Resolution:** The Disaster Recovery Configuration Wizard is now enhanced to set the value of the AutoStartList attribute automatically while creating the RVG service group.<br>**Changed file / version:**<br>DRPluginProxy.dll / 7.0.1.104 |

# Known issues

After applying this patch, you need to reconfigure any existing secure clusters so that they can use the 2048-bit key and SHA-256 signature certificates.

See “Implementing enhanced security for clusters” on page 5.

However, even after you successfully reconfigure an existing cluster, you may encounter the following issues:

- Login attempts to the Cluster Manager (Java Console) may fail.
  This issue occurs due to the cached credentials whenever VCW is used to reconfigure a cluster. It does not occur if you configure a new cluster using the VCW after installing the patch.
  Workaround: Log off from the system and log in again. Then, you should be able to log in to the Cluster Manager to perform further operations.
- The HA commands may not work. For example, if you run the 'hasys -state' command, the following error appears:
  'VCS ERROR V-16-1-53006 Unable to connect to VCS engine securely'
  Workaround: If you encounter this issue, kill the HAD process manually using the Task Manager. The process restarts automatically after a few seconds, and then you can run the HA commands.