

Veritas InfoScale™ 7.0.1 Installation Guide - AIX

Veritas InfoScale Installation Guide

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

Product version: 7.0.1

Document version: 7.0.1 Rev 2

Legal Notice

Copyright © 2016 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

<http://www.veritas.com>

Technical Support

Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within the company to answer your questions in a timely fashion.

Our support offerings include the following:

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

For information about our support offerings, you can visit our website at the following URL:

www.veritas.com/support

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

Contacting Technical Support

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

www.veritas.com/support

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

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

- Product release level
- Hardware information
- Available memory, disk space, and NIC information

- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Technical Support
 - Recent software configuration changes and network changes

Licensing and registration

If your product requires registration or a license key, access our technical support Web page at the following URL:

www.veritas.com/support

Customer service

Customer service information is available at the following URL:

www.veritas.com/support

Customer Service is available to assist with non-technical questions, such as the following types of issues:

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

Support agreement resources

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

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Contents

Technical Support	4	
Chapter 1	Installing the products for the first time	9
	Supported types of Installation	9
	Installing the Veritas InfoScale software using the Install Bundles feature	9
Chapter 2	Preparing to upgrade to Veritas InfoScale 7.0.1	11
	Downloading required software to upgrade to 7.0.1	11
	Prerequisites for upgrading to 7.0.1	12
	Supported upgrade types for Veritas InfoScale 7.0.1	12
	Supported upgrade paths	12
	Preparing to upgrade Volume Replicator	13
	Planning an upgrade from the previous VVR version	14
	Downloading Veritas InfoScale 7.0.1	15
Chapter 3	Upgrading to 7.0.1 from releases earlier than 7.0	17
	Performing a full upgrade with Install Bundles	17
	Performing a full upgrade of VCS using Install Bundles	17
	Performing a full upgrade of SFHA using Install Bundles	19
	Performing a full upgrade of SFCFSHA using Install Bundles	22
	Performing a full upgrade of SF Oracle RAC using Install Bundles	25
	Performing an automated upgrade using response files with Install Bundles	28
Chapter 4	Upgrading to 7.0.1 from 7.0	30
	Performing a full upgrade to 7.0.1 on a cluster	30
	Performing a full upgrade to 7.0.1 on a Veritas Cluster Server	30
	Performing a full upgrade to 7.0.1 on an SFHA cluster	31

	Performing a full upgrade to 7.0.1 on an SFCFSHA cluster	34
	Performing a full upgrade to 7.0.1 on an SF Oracle RAC cluster	36
	Upgrading to 7.0.1 on a standalone system	39
	Verifying software versions	41
Chapter 5	Rolling back and removing Veritas InfoScale	42
	About rolling back Veritas InfoScale 7.0.1	42
	Rolling back using the uninstallmr script	42
	Rolling back manually	43
	Rolling back Storage Foundation or Storage Foundation and High Availability manually	44
	Rolling back Storage Foundation Cluster File System High Availability manually	46
	Rolling back SF for Oracle RAC manually	48
	Rolling back Veritas Cluster Server manually	50
	Removing the Veritas product	53
	Removing 7.0.1 on Veritas Storage Foundation or Veritas Storage Foundation Cluster File System High Availability	53
	Removing 7.0.1 on Veritas Storage Foundation for Oracle RAC	54
Appendix A	About the installation and the uninstallation scripts	56
	About the installation and the uninstallation scripts	56
	The installmr script options	56
	The uninstallmr script options	60
Index		63

Installing the products for the first time

This chapter includes the following topics:

- [Supported types of Installation](#)
- [Installing the Veritas InfoScale software using the Install Bundles feature](#)

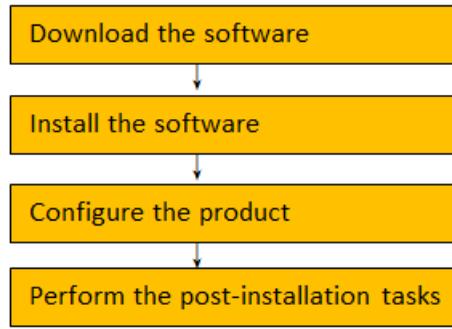
Supported types of Installation

You can use the script-based installer with install bundle method to install Veritas InfoScale 7.0.1.

Installing the Veritas InfoScale software using the Install Bundles feature

This section describes how to install a Veritas InfoScale product of 7.0 and 7.0.1 using the Install Bundles feature in one step.

Figure 1-1 Install flow of Veritas InfoScale



To install the Veritas InfoScale software 7.0.1 using Install Bundles:

- 1 Download 7.0 version of InfoScale product from <https://myveritas.com>.
- 2 Extract the tar ball into the `/infoscale7.0/` directory.
- 3 Download Veritas InfoScale 7.0.1 from <https://sort.veritas.com/patches>.
- 4 Extract it to the `/infoscale7.0.1` directory.
- 5 Change to the `/infoscale7.0.1` directory by entering:

```
# cd /infoscale7.0.1
```

- 6 Invoke the `installmr` script with `-base_path` option to install 7.0 and 7.0.1.
Enter:

```
./installmr -base_path /infoscale7.0/dvd1-aix/
```

Note: The actual path varies depending on your operating system.

- 7 In the Task Menu, enter `i` to install a product.

To configure the product, please see the 7.0 Configuration and Upgrade Guide.

Preparing to upgrade to Veritas InfoScale 7.0.1

This chapter includes the following topics:

- [Downloading required software to upgrade to 7.0.1](#)
- [Prerequisites for upgrading to 7.0.1](#)
- [Supported upgrade types for Veritas InfoScale 7.0.1](#)
- [Supported upgrade paths](#)
- [Preparing to upgrade Volume Replicator](#)
- [Downloading Veritas InfoScale 7.0.1](#)

Downloading required software to upgrade to 7.0.1

This section describes how to download the latest patches for the installer.

To download required software to upgrade to 7.0.1

- 1 Download InfoScale 7.0.1 from <https://sort.Veritas.com/patches>.
- 2 Extract it to a directory, say /infoscale.

Note: If you are upgrading from versions earlier than 7.0 to 7.0.1 using the Install Bundles, you must download both 7.0 and 7.0.1.

Prerequisites for upgrading to 7.0.1

If you are upgrading from 7.0, see the following list for prerequisites for upgrading to the 7.0.1 release:

- For any product in the Veritas Storage Foundation stack, you must have the 7.0.1 release binaries.
- Each system must have sufficient free space to accommodate patches.
- The full list of prerequisites can be obtained by running `./installmr -precheck`.
- Make sure to download the latest patches for the installer.
 See [“Downloading required software to upgrade to 7.0.1”](#) on page 11.

Supported upgrade types for Veritas InfoScale 7.0.1

Veritas InfoScale supports various ways of upgrading your cluster to the latest version. Choose a method that best suits your environment and supports your planned upgrade path.

[Table 2-1](#) lists the supported types of upgrade.

Table 2-1 Supported types of upgrade

Type of upgrade	Abstract
Full upgrade	A full upgrade involves upgrading all the nodes in the cluster at the same time. All components are upgraded during the process. The cluster remains unavailable for the duration of the upgrade.
Online upgrade	The online upgrade involves upgrading the whole cluster and supporting customer's application zero down time during the upgrade procedure. Now it only support VCS component.

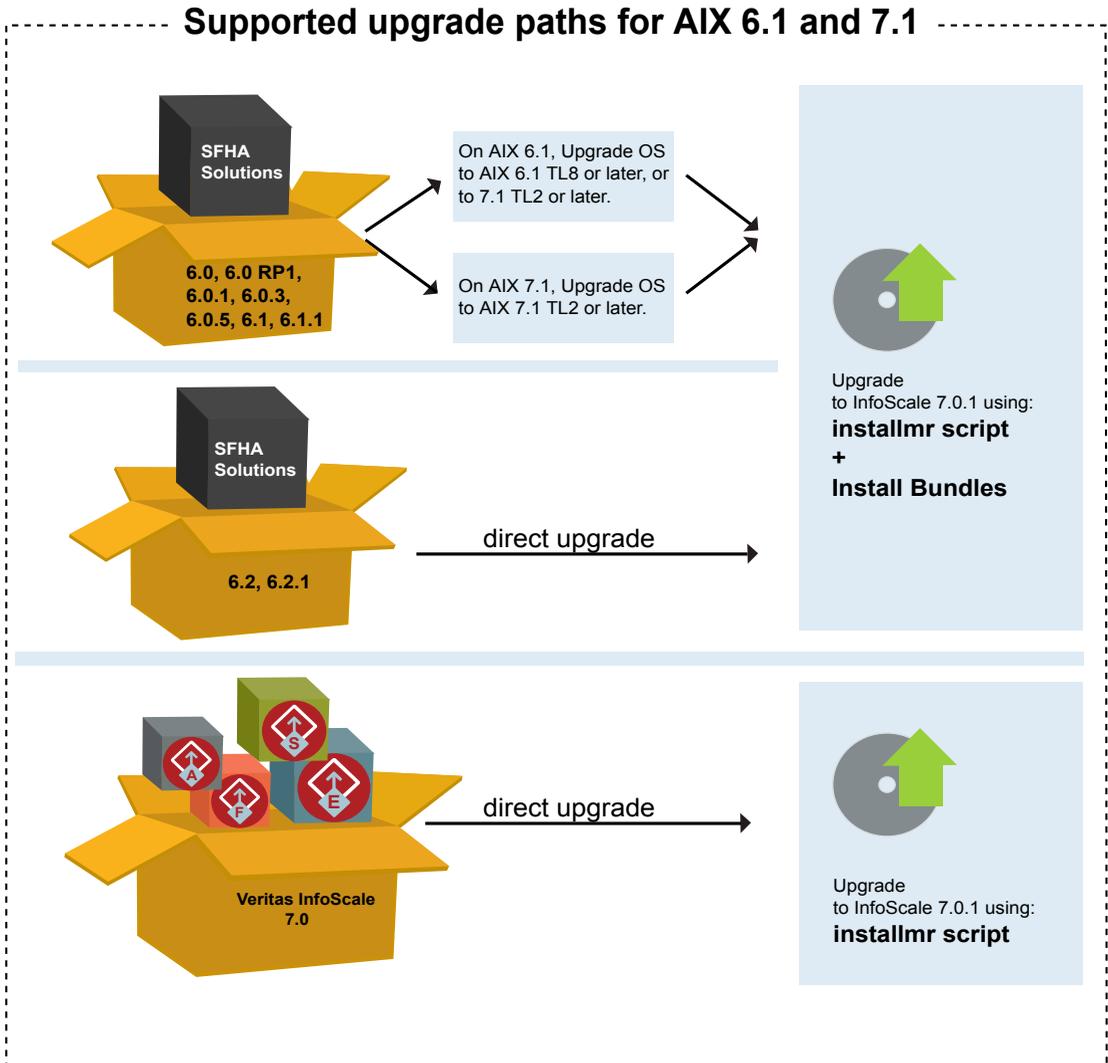
Supported upgrade paths

You can run the `installmr` script with Install Bundles to upgrade Veritas InfoScale to 7.0.1.

For information on operating systems that are supported for 7.0.1, see *System requirements in Veritas InfoScale 7.0.1 Release Notes*.

The following figure lists the supported upgrade paths to 7.0.1 on AIX 6.1 and 7.1.

Figure 2-1 Supported upgrade paths for InfoScale/SFHA solutions on AIX 6.1 and 7.1



Preparing to upgrade Volume Replicator

Before installing or upgrading Volume Replicator (VVR):

- Confirm that your system has enough free disk space to install VVR.
- Make sure you have root permissions. You must have root permissions to perform the install and upgrade procedures.
- If replication using VVR is configured, Veritas recommends that the disk group version is at least 110 prior to upgrading.
You can check the Disk Group version using the following command:

```
# vxdg list diskgroup
```

- If replication using VVR is configured, make sure the size of the SRL volume is greater than 110 MB.
Refer to the *Veritas InfoScale Replication Administrator's Guide*.
- If replication using VVR is configured, verify that all the Primary RLINKs are up-to-date on all the hosts.

```
# /usr/sbin/vxrlink -g diskgroup status rlink_name
```

Note: Do not continue until the primary RLINKs are up-to-date.

- If VCS is used to manage VVR replication, follow the preparation steps to upgrade VVR and VCS agents.

See the *Veritas InfoScale Replication Administrator's Guide* for more information.

See the *Getting Started Guide* for more information on the documentation.

Planning an upgrade from the previous VVR version

If you plan to upgrade VVR from the previous VVR version, you can upgrade VVR with reduced application downtime by upgrading the hosts at separate times. While the Primary is being upgraded, the application can be migrated to the Secondary, thus reducing downtime. The replication between the (upgraded) Primary and the Secondary, which have different versions of VVR, will still continue. This feature facilitates high availability even when the VVR upgrade is not complete on both the sites. Veritas recommends that the Secondary hosts be upgraded before the Primary host in the Replicated Data Set (RDS).

See the *Veritas InfoScale Release Notes* for information regarding VVR support for replicating across Storage Foundation versions.

Replicating between versions is intended to remove the restriction of upgrading the Primary and Secondary at the same time. VVR can continue to replicate an existing RDS with Replicated Volume Groups (RVGs) on the systems that you want to

upgrade. When the Primary and Secondary are at different versions, VVR does not support changing the configuration with the `vradmin` command or creating a new RDS.

Also, if you specify TCP as the network protocol, the VVR versions on the Primary and Secondary determine whether the checksum is calculated. As shown in [Table 2-2](#), if either the Primary or Secondary are running a version of VVR prior to 7.0.1, and you use the TCP protocol, VVR calculates the checksum for every data packet it replicates. If the Primary and Secondary are at VVR 7.0.1, VVR does not calculate the checksum. Instead, it relies on the TCP checksum mechanism.

Table 2-2 VVR versions and checksum calculations

VVR prior to 7.0.1 (DG version <= 140)	VVR 7.0.1 (DG version >= 150)	VVR calculates checksum TCP connections?
Primary	Secondary	Yes
Secondary	Primary	Yes
Primary and Secondary		Yes
	Primary and Secondary	No

Note: When replicating between versions of VVR, avoid using commands associated with new features. The earlier version may not support new features and problems could occur.

If you do not need to upgrade all the hosts in the RDS simultaneously, you can use replication between versions after you upgrade one host. You can then upgrade the other hosts in the RDS later at your convenience.

Note: If you have a cluster setup, you must upgrade all the nodes in the cluster at the same time.

Downloading Veritas InfoScale 7.0.1

- 1 Download Veritas InfoScale 7.0 from <https://myveritas.com>.
- 2 Extract the tar ball into a directory called `/infoscale7.0`.
- 3 Download Veritas InfoScale 7.0.1 from <https://sort.veritas.com/patches>.
- 4 Extract it to a directory called `/infoscale7.0.1`.

Note: If you are upgrading from versions earlier than 7.0 to 7.0.1 using the Install Bundles, you must download both 7.0 and 7.0.1.

Upgrading to 7.0.1 from releases earlier than 7.0

This chapter includes the following topics:

- [Performing a full upgrade with Install Bundles](#)
- [Performing an automated upgrade using response files with Install Bundles](#)

Performing a full upgrade with Install Bundles

The following procedure describes how to upgrade to 7.0.1 with Install Bundles from releases earlier than 7.0.

Note: If you are upgrading from releases earlier than 7.0, Veritas suggests you upgrade with Install Bundles.

- [Performing a full upgrade of VCS using Install Bundles](#)
- [Performing a full upgrade of SFHA using Install Bundles](#)
- [Performing a full upgrade of SFCFSHA using Install Bundles](#)
- [Performing a full upgrade of SF Oracle RAC using Install Bundles](#)

Performing a full upgrade of VCS using Install Bundles

You can use the installer to upgrade VCS.

To upgrade VCS using the product installer

- 1 Log in as superuser.
- 2 Change to the `/infoscale7.0.1` directory.

- 3 Invoke the `installmr` script with `-base_path` option to upgrade to 7.0.1:

```
# ./installmr -base_path /infoscale7.0/dvd1-aix/
```

Note: The actual path varies depending on your operating system version.

- 4 From the opening Selection Menu, choose: **G** for "Upgrade a Product."
- 5 Choose **1** for Full Upgrade.
- 6 Enter the names of the nodes that you want to upgrade. Use spaces to separate node names. Press the Enter key to proceed.

The installer runs some verification checks on the nodes.
- 7 When the verification checks are complete, the installer asks if you agree with the terms of the End User License Agreement. Press **y** to agree and continue.

The installer lists the filesets to upgrade.
- 8 The installer displays the following question before it stops the product processes, if the cluster is configured in secure mode and the previous product version is less than 6.2:

```
Do you want to grant read access to everyone? [y,n,q,?]
```

To grant read access to all authenticated users, type **y**.

To grant permissions to specific user group, type **n**.

```
Do you want to provide any usergroups that you would like to\grant read access?[y,n,q,?]
```

To specify user groups and grant them read access, type **y**.

To grant read access only to root users, type **n**. Then the installer grants read access read access to the root users.

Enter the user group names that you want to grant read access and separate them by spaces. If you want to grant read access to a user group on a specific node, enter **usergroup@node**. If you want to grant read access to user groups on any cluster node, enter **usergroup**. If some user groups are not created yet, create the user groups after configuration if needed.

- 9 The installer asks if you want to stop VCS processes. Press the Enter key to continue.

The installer stops VCS processes, uninstalls filesets, installs or upgrades filesets, configures, and starts VCS.

The installer lists the nodes that Veritas recommends you to restart, if needed.

- 10 The installer asks if you would like to send the information about this installation to Veritas to help improve installation in the future. Enter your response.

The installer displays the location of log files, summary file, and response file.

Note: If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, from 7.0.1 onwards, CP server supports only HTTPS based communication with its clients and IPM based communication is no longer supported. CP server needs to be reconfigured if you upgrade the CP server with IPM-based CP server configured.

Performing a full upgrade of SFHA using Install Bundles

This section describes how to perform a full upgrade of SFHA using Install Bundles.

Upgrading SFHA to 7.0.1 with Install Bundles

This section describes upgrading SFHA products to 7.0.1 with Install Bundles.

To upgrade SFHA

- 1 Log in as superuser.
- 2 Unmount any mounted VxFS file systems.

The installer supports the upgrade of multiple hosts, if each host is running the same version of VxVM and VxFS. Hosts must be upgraded separately if they are running different versions.

If any VxFS file systems are mounted with the QuickLog feature, QuickLog must be disabled before upgrading.

- 3 If you are upgrading SFHA, take all service groups offline.

List all service groups:

```
# /opt/VRTSvcs/bin/hagrp -list
```

For each service group listed, take it offline:

```
# /opt/VRTSvcs/bin/hagrp -offline service_group \  
-sys system_name
```

- 4 If replication using VVR is configured, verify that all the Primary RLINKs are up-to-date:

```
# /usr/sbin/vxlink -g diskgroup status rlink_name
```

Note: Do not continue until the Primary RLINKs are up-to-date.

- 5 Change to the `/infoscale7.0.1` directory.

- 6 Run the `installmr` command.

```
#./installmr -base_path /infoscale7.0/dvd1-aix/
```

Note: The actual path varies depending on your operating system version.

- 7 Enter `g` to upgrade and select the **Full Upgrade**.

- 8 You are prompted to enter the system names (in the following example, "sys1") on which the software is to be installed. Enter the system name or names and then press Return.

```
Enter the system names separated by spaces on which to  
install SFHA: sys1  
                  sys2
```

Depending on your existing configuration, various messages and prompts may appear. Answer the prompts appropriately.

- 9 The installer asks if you agree with the terms of the End User License Agreement. Press `y` to agree and continue.

- 10 The installer lists the filesets to install or to update. You are prompted to confirm that you are ready to upgrade.

- 11** The installer displays the following question before it stops the product processes, if the cluster is configured in secure mode and the previous product version is less than 6.2:

```
Do you want to grant read access to everyone? [y,n,q,?]
```

To grant read access to all authenticated users, type **y**.

To grant permissions to specific user group, type **n**.

```
Do you want to provide any usergroups that you would like to\
grant read access?[y,n,q,?]
```

To specify user groups and grant them read access, type **y**.

To grant read access only to root users, type **n**. Then the installer grants read access read access to the root users.

Enter the user group names that you want to grant read access and separate them by spaces. If you want to grant read access to a user group on a specific node, enter **usergroup@node**. If you want to grant read access to user groups on any cluster node, enter **usergroup**. If some user groups are not created yet, create the user groups after configuration if needed.

- 12** Stop the product's processes.

```
Do you want to stop InfoScale Enterprise processes now? [y,n,q] (y) y
```

If you select **y**, the installer stops the product processes and makes some configuration updates before upgrading.

- 13** The installer stops, uninstalls, reinstalls, and starts specified filesets.
- 14** If the product is licensed with a stale (old) key, the installer would prompt users to update the key.
- 15** The SFHA software is verified and configured.
- 16** The installer prompts you to provide feedback, and provides the log location for the upgrade.

Note: If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, from 7.0.1 onwards, CP server supports only HTTPS based communication with its clients and IPM based communication is no longer supported. CP server needs to be reconfigured if you upgrade the CP server with IPM-based CP server configured.

Performing a full upgrade of SFCFSHA using Install Bundles

This section describes how to perform a full upgrade of SFCFSHA using Install Bundles.

Performing a full SFCFSHA upgrade with Install Bundles

Performing a full upgrade involves the following tasks:

- Ensuring that the file systems are clean
- Performing the upgrade

Ensuring the file systems are clean

Before upgrading to SFCFSHA 7.0.1, ensure that the file systems are clean. To ensure that the logs have been replayed and the file systems are marked clean:

To ensure the file systems are clean

- 1 Log in as superuser onto any node in the cluster.
- 2 Take the service group offline on each node of the cluster, which contains VxFS and CFS resources:

```
# hagr -offline group -any
```

where *group* is the VCS service group that has the CVMVolDg and CFMount resource.

Repeat this step for each SFCFSHA service group.

Note: This unmounts the CFS file systems.

- 3 Unmount all VxFS file systems not under VCS control:

```
# umount /mount_point
```

- 4 Check and repair each VxFS file system:

```
# fsck -V vxfs /dev/vx/dsk/diskgroup/volume
```

The `fsck` command in `/opt/VRTS/bin` accepts either the block or character device (`/dev/vx/dsk/dg/vol`) or (`/dev/vx/rdisk/dg/vol`). The operating system version of `fsck` may limit the device types it accepts.

For more information, see the `fsck` and `fsck_vxfs` man pages.

Repeat this step for each file system.

Performing the upgrade

To perform the upgrade

- 1 Log in as superuser.
- 2 Verify there are no VxFS file systems mounted on the nodes being upgraded:

```
# mount | grep vxfs
```

If any VxFS file systems are mounted, offline the group on each node of the cluster:

```
# hagr -offline group -sys system01
# hagr -offline group -sys system02
# hagr -offline group -sys system03
# hagr -offline group -sys system04
```

where *group* is the VCS service group that has the CVMVolDg and CFMount resource.

If VxFS are not managed by VCS then unmount them manually:

```
# umount /mount_point
```

Repeat this step for each SFCFSHA service group.

- 3 Change to the `/infoscale7.0.1` directory. Invoke the `installmr` script with `-base_path` option to upgrade to 7.0.1:

```
#!/installmr -base_path /infoscale7.0/dvd1-aix/
```

Note: The actual path varies depending on your operating system version.

- 4 From the opening Selection Menu, choose: **G for Upgrade a Product**. Choose **1 for Full Upgrade**.
- 5 You are prompted to enter the system names (in the following example, "sys1" and "sys2") on which the software is to be upgraded. Enter the system name or names and then press Return.

```
Enter the system names separated by spaces on which to
install SFCFSHA: sys1 sys2
```

- 6 At the prompt, specify whether you accept the terms of the End User License Agreement (EULA). Press **y** to agree and continue.

- 7 During the initial system check, the installer verifies that communication between systems has been set up.

If the installer hangs or asks for a login password, setup passwordless ssh or setup rsh from the system that run `installmr` to the system that need to be upgraded to 7.0.1. Then run the installer again.

- 8 After you accept EULA and the system checks complete, the installer displays a list of the filesets that will be upgraded. Press Enter to continue with the upgrade.
- 9 The installer displays the following question before it stops the product processes, if the cluster is configured in secure mode and the previous product version is less than 6.2:

```
Do you want to grant read access to everyone? [y,n,q,?]
```

To grant read access to all authenticated users, type **y**.

To grant permissions to specific user group, type **n**.

```
Do you want to provide any usergroups that you would like to\
grant read access?[y,n,q,?]
```

To specify user groups and grant them read access, type **y**.

To grant read access only to root users, type **n**. Then the installer grants read access read access to the root users.

Enter the user group names that you want to grant read access and separate them by spaces. If you want to grant read access to a user group on a specific node, enter **usergroup@node**. If you want to grant read access to user groups on any cluster node, enter **usergroup**. If some user groups are not created yet, create the user groups after configuration if needed.

- 10 Output shows information that SFCFSHA must be stopped on a running system. Enter **y** to continue.
- 11 The installer stops, uninstalls, reinstalls, and starts specified filesets.

- 12** Press **Enter** again for summary information about logs and reboots.

Do not remove the log files until the Veritas InfoScale products are working properly on your system. Technical Support will need these log files for debugging purposes.

Note: If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, from 7.0.1 onwards, CP server supports only HTTPS based communication with its clients and IPM based communication is no longer supported. CP server needs to be reconfigured if you upgrade the CP server with IPM-based CP server configured.

- 13** Find out which node is the CVM master. Enter the following:

```
# vxdctl -c mode
```

- 14** On the CVM master node, upgrade the CVM protocol. Enter the following:

```
# vxdctl upgrade
```

Performing a full upgrade of SF Oracle RAC using Install Bundles

This section describes how to perform a full upgrade of SF Oracle RAC using Install Bundles.

- [Preparing to perform a full upgrade to 7.0.1 on an SF Oracle RAC cluster](#)
- [Upgrading to SF Oracle RAC 7.0.1](#)

Preparing to perform a full upgrade to 7.0.1 on an SF Oracle RAC cluster

Perform the preparatory steps in this section if you are performing a full upgrade of the cluster. Before you upgrade, make sure that your systems meet the hardware and software requirements for this release.

Pre-upgrade tasks for migrating the SFDB repository database

Perform the following before upgrading SF Oracle RAC.

Note: The Sfua_Base repository resource group will be removed from the main.cf file. It is not required as a separate service group for SF Oracle RAC 7.0.1.

To prepare to migrate the repository database

- ◆ Resynchronize all existing snapshots before upgrading. As Oracle user, enter:

```
$ /opt/VRTS/bin/dbed_vmsnap -s $ORACLE_SID \  
-f SNAPPLAN -o resync
```

Warning: The Database Flashsnap clone database will not be able to be carried over after upgrading. You must create a new Database Flashsnap clone database after upgrading to 7.0.1.

Upgrading to SF Oracle RAC 7.0.1

This section provides instructions for upgrading to SF Oracle RAC 7.0.1.

- If required, upgrade the operating system.
- Upgrade to SF Oracle RAC 7.0.1.
- Bring the SF Oracle RAC online.

Upgrading the operating system

If you want to upgrade the operating system, perform the following steps:

- 1 Rename the `/etc/llttab` file to prevent LLT from starting automatically when the node starts:

```
# mv /etc/llttab /etc/llttab.save
```

- 2 Upgrade the operating system on all nodes in the cluster.
For instructions, see the operating system documentation.

- 3 After the system restarts, restore the `/etc/llttab` file to its original name:

```
# mv /etc/llttab.save /etc/llttab
```

Upgrading SF Oracle RAC using Install Bundles

Use the `installmr` script-based installation programs to upgrade SF Oracle RAC.

The installer performs the following tasks to upgrade SF Oracle RAC:

- Verifies the compatibility of the systems before the upgrade.
- Stops the SF Oracle RAC processes before the upgrade.
- Uninstalls SF Oracle RAC.
- Installs the SF Oracle RAC 7.0 filesets on the nodes.
- Installs the SF Oracle RAC 7.0.1 patches on the nodes.
- Starts the SF Oracle RAC processes after the upgrade.
- Displays the location of the log files, summary file, and response file.

Bringing the application database online

- 1 Start all applications that are not managed by VCS. Use native application commands to start the applications.
- 2
 - If the application database is managed by VCS, reset the AutoStart value to 1 to enable VCS to bring the database service group online automatically when VCS starts:
 - If the application database is not managed by VCS, change the management policy for the database to automatic:
 - For Oracle RAC 11g:


```
$ srvctl modify database -d db_name -y AUTOMATIC
```
 - For Oracle RAC 12c:


```
$ srvctl modify database -db db_name -policy AUTOMATIC
```
- 3 Complete other post-upgrade steps.

For instructions, see the chapter *Performing post-upgrade tasks* in *Storage Foundation for Oracle RAC 7.0 Installation and Configuration Guide*.

- 4 Upgrade application, if required.

For information on Oracle RAC support, see:

<http://www.Veritas.com/docs/DOC5081>

For instructions, see the chapter *Upgrading application* in 7.0 SF Oracle RAC Installation Guide.

Note: The procedure for Oracle RAC 12c is the same as that for Oracle RAC 11g Release 2.

- 5 If you want to upgrade all application clusters to version 7.0.1, make sure that you upgraded CP server systems that use VCS or SFHA to 7.0.1. Then, upgrade all application clusters to version 7.0.1.

For instructions to upgrade VCS or SFHA on the CP server systems, see the 7.0 VCS or SFHA installation guide.

Performing an automated upgrade using response files with Install Bundles

Typically, you can use the response file that the installer generates after you perform InfoScale upgrade with Install Bundles on one system to upgrade InfoScale on other systems.

To perform automated upgrade using response files

- 1 Make sure the systems where you want to upgrade meet the upgrade requirements.
- 2 Copy the response file to one of the systems where you want to upgrade Veritas InfoScale.
- 3 Edit the values of the response file variables as necessary.
- 4 Navigate to the folder that contains the installation program.
- 5 Start the upgrade from the system to the `/infoscale7.0.1` directory. For example:

```
# ./installmr -responsefile /infoscale7.0.1/response_file
```

Where `/infoscale7.0.1/response_file` is the response file's full path name.

- 6 Find out which node is the CVM master. Enter the following:

```
# vxdctl -c mode
```

- 7** On the CVM master node, upgrade the CVM protocol. Enter the following:

```
# vxdctl upgrade
```

- 8** Complete the post upgrade task as mentioned in the upgrade method for specific components.

Upgrading to 7.0.1 from 7.0

This chapter includes the following topics:

- [Performing a full upgrade to 7.0.1 on a cluster](#)
- [Upgrading to 7.0.1 on a standalone system](#)
- [Verifying software versions](#)

Performing a full upgrade to 7.0.1 on a cluster

Performing a full upgrade on a cluster requires stopping cluster failover functionality during the entire procedure.

Depending on your cluster's configuration, select one of the following procedures to upgrade to 7.0.1:

- [Performing a full upgrade to 7.0.1 on a Veritas Cluster Server](#)
- [Performing a full upgrade to 7.0.1 on an SFHA cluster](#)
- [Performing a full upgrade to 7.0.1 on an SFCFSHA cluster](#)
- [Performing a full upgrade to 7.0.1 on an SF Oracle RAC cluster](#)
See ["Downloading required software to upgrade to 7.0.1"](#) on page 11.

Performing a full upgrade to 7.0.1 on a Veritas Cluster Server

The following procedure describes performing a full upgrade on a Veritas Cluster Server (VCS) cluster.

Note: If you want to roll back to the original product version, make sure all the filesets are committed before upgrade.

To upgrade VCS

- 1 Make sure you have downloaded the latest software required for the upgrade.
- 2 Log in as superuser.

Note: Upgrade the Operating System and reboot the systems if required.

- 3 Check the readiness of the nodes where you plan to upgrade. From the directory that contains the extracted and untarred 7.0.1 rolling patch binaries, change to the directory that contains the installmr script. Start the pre-upgrade check:

```
# ./installmr -precheck sys1 sys2 ... nodeN
```

- 4 Resolve any issues that the precheck finds.
- 5 Start the upgrade:

```
# ./installmr sys1 sys2 ... nodeN
```

- 6 After the upgrade, review the log files for any issues.

Performing a full upgrade to 7.0.1 on an SFHA cluster

The following procedure describes performing a full upgrade on an SFHA and VCS cluster.

To perform a full upgrade to 7.0.1 on an SFHA cluster

- 1 Make sure you have downloaded the latest software required for the upgrade.
- 2 Log in as superuser.
- 3 Verify that `/opt/VRTS/bin` and `/opt/VRTSvcs/bin` are in your `PATH` so that you can execute all product commands.
- 4 On each node in the cluster, make the VCS configuration read only:

```
# haconf -dump -makero
```

5 Stop VCS.

To stop applications, unmount VxFS file systems and stop VxVM volumes managed by VCS.

```
# hastop -all
```

6 Stop all the applications that are using VxFS files systems and VxVM volumes which are not managed by VCS.

Use application's native commands to stop applications.

7 On each node, enter the following command to check if any Storage Checkpoints are mounted:

```
# mount | grep vxfs
```

If any Storage Checkpoints are mounted, on each node in the cluster, unmount all Storage Checkpoints.

```
# umount /checkpoint_name
```

8 On each node, enter the following command to check if any VxFS file systems are mounted.

Unmount the VxFS file systems that are not managed by VCS.

```
# mount | grep vxfs
```

If any VxFS file systems are present, on each node in the cluster, stop IOs on the file systems, unmount all of the VxFS file systems:

```
# umount /filesystem
```

9 If you have created any Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:

- Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.

- Use the `vrxvg stop` command to stop each RVG individually:

```
# vxrvg -g diskgroup stop rvg_name
```

- On the Primary node, use the `vxrlink status` command to verify that all RLINKs are up-to-date:

```
# vxrlink -g diskgroup status rlink_name
```

Caution: To avoid data corruption, do not proceed until all RLINKs are up-to-date.

- 10** Stop activity to all VxVM volumes that are not managed by VCS.

For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes. Use application specific commands to stop the applications.

- 11** On each node, stop all VxVM volumes by entering the following command for each disk group, which are not managed by VCS:

```
# vxvol -g diskgroup stopall
```

Verify that no volumes remain open:

```
# vxprint -Aht -e v_open
```

- 12** Deport all the disk groups which are not managed under VCS.

```
# vxdg deport diskgroup
```

- 13** If required, upgrade the Operating System and reboot the systems.

See IBM's documentation for the upgrade procedures.

- 14** On each node, stop the VCS command server:

```
# ps -ef | grep CmdServer
# kill -9 pid_of_CmdServer
```

pid_of_CmdServer is the process ID of CmdServer.

- 15** Check the readiness of the nodes where you plan to upgrade. From the directory that contains the extracted and untarred 7.0.1 rolling patch binaries, change to the directory that contains the `installmr` script. Start the pre-upgrade check:

```
# ./installmr -precheck sys1 sys2 ... nodeN
```

where *sys1* and *sys2* are nodes which are to be upgraded.

Resolve any issue that the precheck finds.

- 16** Start the upgrade.

```
# ./installmr [-rsh] sys1 sys2 ... nodeN
```

Review the output and follow the instructions to finish the upgrade.

- 17** Enter the following command on each node to take service groups online, if the groups are not in AutoStartList:

```
# hagrps -online service_group -sys nodename
```

- 18** If necessary, reinstate any missing mount points in the `/etc/filesystem` file on each node.

- 19** Import all the diskgroups that are not managed by VCS:

```
# vxvg import diskgroup
```

- 20** Restart all the volumes by entering the following command for each disk group that are not managed by VCS:

```
# vxvol -g diskgroup startall
```

- 21** If you stopped any RVGs in step 9, restart each RVG:

```
# vxrvrg -g diskgroup start rvg_name
```

- 22** Remount all VxFS file systems on all nodes, which are not managed by VCS:

```
# mount -V vxfs blockdevice
      mountpoint
```

- 23** Remount all Storage Checkpoints on all nodes:

```
# mount -V vxfs -o ckpt=name
      blockdevice
      checkpoint_name
```

- 24** Start all applications which are using VxFS files systems that are not managed by VCS.

Use application native commands to start the applications.

Performing a full upgrade to 7.0.1 on an SFCFSHA cluster

The following procedure describes performing a full upgrade on an SFCFSHA cluster.

To perform a full upgrade to 7.0.1 on an SFCFSHA cluster

- 1** Make sure you have downloaded the latest software required for the upgrade.
- 2** Log in as superuser.

- 3 Verify that `/opt/VRTS/bin` is in your `PATH` so that you can execute all product commands.
- 4 On each node, for mount points not controlled by VCS, enter the following command to check if any Storage Checkpoints or VxFS file systems are mounted:

```
# mount | grep vxfs
```

If any Storage Checkpoints or VxFS file systems are mounted, on each node in the cluster unmount all or VxFS file systems.

```
# umount /checkpoint_name
```

- 5 If you have created any Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:
 - Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.
 - Use the `vrxvg stop` command to stop each RVG individually:

```
# vxrvrg -g diskgroup stop rvg_name
```

- On the Primary node, use the `vxlink status` command to verify that all RLINKs are up-to-date:

```
# vxlink -g diskgroup status rlink_name
```

Caution: To avoid data corruption, do not proceed until all RLINKs are up-to-date.

- 6 Stop activity to all VxVM volumes.
 For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.
- 7 On each node, stop all VxVM volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

Verify that no volumes remain open:

```
# vxprint -Aht -e v_open
```

- 8 If required, apply the OS kernel patches.
 See IBM's documentation for the procedures.
- 9 From the directory that contains the extracted and untarred 7.0.1 rolling patch binaries, change to the directory that contains the `installmr` script.

```
# ./installmr sys1 sys2
```

where `sys1` and `sys2` are nodes which are to be upgraded.
- 10 After all the nodes in the cluster are upgraded, the processes restart. If the `installmr` script finds issues, it may require you to reboot the nodes.
- 11 If necessary, reinstate any missing mount points in the `/etc/filesystems` file on each node.
- 12 Bring the CVM service group online on each node:

```
# hagrps -online cvm -sys nodename
```
- 13 Restart all the volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup startall
```
- 14 If you stopped any RVGs in step 5, restart each RVG:

```
# vxrvrg -g diskgroup start rvg_name
```
- 15 Remount all VxFS file system and Storage Checkpoints on all nodes:

```
# mount /filesystem
```

Performing a full upgrade to 7.0.1 on an SF Oracle RAC cluster

The following procedure describes performing a full upgrade on an SF for Oracle RAC cluster.

To upgrade to 7.0.1 on a SF Oracle RAC cluster

- 1 Make sure you have downloaded the latest software required for the upgrade.
- 2 Log in as superuser.
- 3 Verify that `/opt/VRTS/bin` is in your **PATH** so that you can execute all product commands.

- 4** If the Oracle database is managed by VCS, set the AutoStart value to 0 to prevent the database service group from starting automatically when VCS starts:

```
# haconf -makerw
# hagrpl -modify oracle_group AutoStart 0
# haconf -dump -makero
```

If the Oracle database is not managed by VCS, change the management policy for the database to manual. Execute the following command with oracle database user credentials.

For Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y manual
```

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy MANUAL
```

- 5** From any node in the cluster, stop all Oracle RAC resources.
- If the database instances are managed by VCS, take the corresponding VCS service groups offline. As superuser, enter:

```
# hagrpl -offline group_name -any
```

- If the database instances are not managed by VCS, run the following on one node:

For Oracle RAC 11g:

```
$ srvctl stop database -d db_name
```

For Oracle RAC 12c:

```
# srvctl stop database -db db_name
```

- 6** Stop all applications on the cluster that are not configured under VCS. Use native application commands to stop the application.
- 7** Unmount the VxFS and CFS file systems that are not managed by VCS.

- Ensure that no processes are running that make use of mounted shared file system or shared volumes. To verify that no processes use the VxFS or CFS mount point, enter the following commands:

```
# mount | grep vx
# fuser -cu /mount_point
```

- Unmount the VxFS or CFS file system:

```
# umount /mount_point
```

- 8 Stop all VxVM and CVM volumes for each diskgroup that are not managed by VCS on the cluster:

```
# vxvol -g disk_group stopall
```

Verify that no volumes remain open:

```
# vxprint -Aht -e v_open
```

- 9 Stop VCS.

```
# hastop -all
```

- 10 From the directory that contains the extracted and untarred 7.0.1 rolling patch binaries, change to the directory that contains the installmr script. Start the upgrade.

```
# ./installmr sys1 sys2 ...
```

- 11 Manually mount the VxFS and CFS file systems that are not managed by VCS.

- 12 Start all applications on the cluster that are not configured under VCS. Use native application commands to start the application.

- 13 Relink the SF Oracle RAC libraries with Oracle.

Choose the option **Relink Oracle Database Binary** from the program menu.

- 14 Bring the Oracle database service group online.

- If the Oracle database is managed by VCS, enter:

```
# hagrps -online Oracle_group -any
```

- If the Oracle database is not managed by VCS:

For Oracle RAC 11g:

```
$ srvctl start database -d db_name
```

For Oracle RAC 12c:

```
$ srvctl start database -db db_name
```

- 15 ■ If the Oracle database is managed by VCS, reset the AutoStart value to 1 to enable VCS to bring the database service group online automatically when VCS starts:

```
# haconf -makerw
# hagrps -modify oracle_group AutoStart 1
# haconf -dump -makero
```

- If the Oracle database is not managed by VCS, change the management policy for the database to automatic:

For Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y AUTOMATIC
```

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy AUTOMATIC
```

- 16 Complete other post-upgrade steps.

For instructions, see the chapter *Performing post-upgrade tasks* in *Veritas™ Storage Foundation for Oracle RAC 7.0 Installation and Configuration Guide*.

- 17 Upgrade Oracle RAC, if required.

Note: Oracle RAC 11g Release 1 Clusterware is not supported. Make sure that you install Oracle RAC 11g Release 2 and later Grid Infrastructure in order to use the Oracle RAC 11g Release 1 database. All database versions starting from Oracle RAC 11g Release 2 and later are supported.

For instructions, see the chapter *Upgrading Oracle RAC* in 7.0 SF Oracle RAC Installation Guide.

Note: The upgrade procedure for Oracle 12c is the same as Oracle 11g.

Upgrading to 7.0.1 on a standalone system

You can use this procedure to upgrade on a standalone system that runs SF.

To upgrade to 7.0.1 on a standalone system

- 1 Make sure you have downloaded the latest software required for the upgrade.
- 2 Log in as superuser.

- 3 Verify that `/opt/VRTS/bin` is in your `PATH` so you can execute all product commands.
- 4 If required, apply the OS kernel patches.
See IBM's documentation for the procedures.
- 5 Enter the following command to check if any VxFS file systems or Storage Checkpoints are mounted:

```
# mount | grep vx
```

- 6 Unmount all Storage Checkpoints and file systems:

```
# umount /checkpoint_name  
# umount /filesystem
```

- 7 If you have created any Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:
 - Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.
 - Use the `vrxvg stop` command to stop each RVG individually:

```
# vxrvrg -g diskgroup stop rvg_name
```

- On the Primary node, use the `vxlink status` command to verify that all RLINKs are up-to-date:

```
# vxlink -g diskgroup status rlink_name
```

Caution: To avoid data corruption, do not proceed until all RLINKs are up-to-date.

- 8 Stop activity to all VxVM volumes. For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.
- 9 Stop all VxVM volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

Verify that no volumes remain open:

```
# vxprint -Aht -e v_open
```

- 10 Copy the patch archive downloaded from the patch central to temporary location and untar the archive and browse to the directory containing the installmr installer script. Enter the `installmr` script:

```
# ./installmr nodename
```

- 11 If necessary, reinstate any missing mount points in the `/etc/filesystems` file.
- 12 Restart all the volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup startall
```

- 13 If you stopped any RVGs in step 7, restart each RVG:

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

- 14 Remount all VxFS file systems and Storage Checkpoints:

```
# mount /filesystem  
# mount /checkpoint_name
```

Verifying software versions

To list the Veritas filesets installed on your system, enter the following command:

```
# lspp -L VRTS*
```

Rolling back and removing Veritas InfoScale

This chapter includes the following topics:

- [About rolling back Veritas InfoScale 7.0.1](#)
- [Rolling back using the `uninstallmr` script](#)
- [Rolling back manually](#)
- [Removing the Veritas product](#)

About rolling back Veritas InfoScale 7.0.1

This section describes how to roll back either by using the `uninstallmr` script or manually.

The `uninstallmr` script uninstalls all the patches associated with filesets installed, and starts the processes.

The `uninstallmr` script uninstalls all the 7.0.1 patches. A scenario wherein the product is upgraded from 7.0 to 7.0.1, after you run the `uninstallmr` script, all the 7.0.1 patches are uninstalled while the 7.0 filesets are retained.

Note: If you upgraded the products to 7.0.1 from 7.0 or versions earlier than 7.0, the products roll back to 7.0.

Rolling back using the `uninstallmr` script

Use the following procedure to roll back from any Veritas product to the previous version using the `uninstallmr` script.

To roll back

- 1 Browse to the directory that contains the `uninstallmr` script.
- 2 Unmount all the Storage Checkpoints and the file systems.

```
# umount /checkpoint_name  
# umount /filesystem
```

Verify that you unmounted the Storage Checkpoints and the file systems.

```
# mount | grep vxfs
```

- 3 Stop all the processes and services accessing the file systems. For each disk group enter:

```
# vxvol -g diskgroup stopall
```

Verify that no volumes remain open.

```
# vxprint -Aht -e v_open
```

- 4 Run the `uninstallmr` script to rollback patches, type:

```
# ./uninstallmr
```

- 5 The `uninstallmr` script removes 7.0.1 patches. After patch rollback completes, modules are loaded and processes are restarted. `uninstallmr` will also report any warning happened during the rolling back.

Rolling back manually

Use one of the following procedures to roll back to 7.0 manually.

- [Rolling back Storage Foundation or Storage Foundation and High Availability manually](#)
- [Rolling back Storage Foundation Cluster File System High Availability manually](#)
- [Rolling back SF for Oracle RAC manually](#)
- [Rolling back Veritas Cluster Server manually](#)

Note: You must reboot systems when you roll back manually at the end of the roll back procedure.

Rolling back Storage Foundation or Storage Foundation and High Availability manually

Use the following procedure to roll back to 7.0 manually.

To roll back SF or SFHA

- 1 Log in as superuser.
- 2 Verify that `/opt/VRTS/bin` is in your `PATH` so you can execute all product commands.

- 3 Unmount all Storage Checkpoints and file systems:

```
# umount /checkpoint_name  
# umount /filesystem
```

- 4 Enter the following command to check if any VxFS file systems or Storage Checkpoints are mounted:

```
# mount | grep vxfs
```

- 5 If you have created any Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:

- Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.
- Use the `vxrvg stop` command to stop each RVG individually:

```
# vxrvg -g diskgroup stop rvg_name
```

- On the Primary node, use the `vxrlink status` command to verify that all RLINKs are up-to-date:

```
# vxrlink -g diskgroup status rlink_name
```

Caution: To avoid data corruption, do not proceed until all RLINKs are up-to-date.

- 6 Stop activity to all VxVM volumes.

- 7** Stop all VxVM volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

To verify that no volumes remain open, enter the following command:

```
# vxprint -Aht -e v_open
```

- 8** Stop VCS and its modules manually.

```
# hastop -all
```

- 9** Stop I/O fencing on each node:

```
# /etc/rc.d/rc2.d/S97vxfen stop
```

- 10** Stop GAB:

```
# /etc/rc.d/rc2.d/S92gab stop
```

- 11** Stop LLT:

```
# /etc/rc.d/rc2.d/S701lt stop
```

- 12** Unmount `/dev/odm`:

```
# umount /dev/odm
```

- 13** Unload the ODM module:

```
# genkex | grep odm  
# vxkextadm vxodm unload
```

- 14** ■ Create a file that contains all the 7.0.1 patches. In this example, it is called `/reject.list`.
- Reject each patch from the patch list file, for example:

```
# installp -rBf /reject.list
```

- 15** Reboot the systems. On each system, run the following command.

```
# /usr/sbin/shutdown -r now
```

Rolling back Storage Foundation Cluster File System High Availability manually

Use the following procedure to roll back to 7.0 manually.

To roll back SFCFSHA manually

- 1 Log in as superuser.
- 2 Verify that `/opt/VRTS/bin` is in your `PATH` so you can execute all product commands.

- 3 Unmount all Storage Checkpoints and file systems:

```
# umount /checkpoint_name
# umount /filesystem
```

- 4 Enter the following command to check if any VxFS file systems or Storage Checkpoints are mounted:

```
# mount | grep vxfs
```

- 5 If you have created any Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:

- Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.
- Use the `vrxvg stop` command to stop each RVG individually:

```
# vxrvg -g diskgroup stop rvg_name
```

- On the Primary node, use the `vxrlink status` command to verify that all RLINKs are up-to-date:

```
# vxrlink -g diskgroup status rlink_name
```

Caution: To avoid data corruption, do not proceed until all RLINKs are up-to-date.

- 6 Stop activity to all VxVM volumes. For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.

- 7** Stop all VxVM volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

To verify that no volumes remain open, enter the following command:

```
# vxprint -Aht -e v_open
```

- 8** Stop VCS along with all the resources. Then, stop the remaining resources manually:

```
# /etc/rc.d/rc2.d/S99vcs stop
```

- 9** Unmount `/dev/odm`:

```
# umount /dev/odm
```

- 10** Unload the ODM module:

```
# genkex | grep odm  
# vxkextadm vxodm unload
```

- 11** Stop I/O fencing on each node:

```
# /etc/rc.d/rc2.d/S97vxfen stop
```

- 12** Stop GAB:

```
# /etc/rc.d/rc2.d/S92gab stop
```

- 13** Stop LLT:

```
# /etc/rc.d/rc2.d/S7011t stop
```

- 14** Remove the Storage Foundation Cluster File System High Availability 7.0.1 patches.

- Create a file that contains all the 7.0.1 patches. In this example, it is called `/reject.list`.
- Reject each patch from the patch list file, for example:

```
# installp -rBf /reject.list
```

- 15** Reboot the systems. On each system, run the following command.

```
# /usr/sbin/shutdown -r now
```

Rolling back SF for Oracle RAC manually

Use the following procedure to roll back to 7.0 manually.

To roll back SF for Oracle RAC manually

- 1 Stop Oracle and CRS on each node of the cluster.
 - If Oracle Clusterware is controlled by VCS, log in as superuser on one of the cluster nodes and enter the following command:

```
# hastop -all
```

- If Oracle Clusterware is not controlled by VCS, enter the following command on each node of the cluster to stop Oracle Clusterware:

```
# crsctl stop crs -f
```

Unmount all VxFS file system used by a database or application and enter the following command to each node of the cluster:

```
# hastop -local
```

- 2 Verify the output of the `gabconfig -a` command to ensure that VCS has been stopped. In the `gabconfig -a` command output, the VCS engine or high availability daemon (HAD) port h is not displayed. This indicates that VCS has been stopped.

```
# /sbin/gabconfig -a
```

Sample output:

```
GAB Port Memberships
=====
Port a gen 5c3d0b membership 01
Port b gen 5c3d10 membership 01
Port d gen 5c3d0c membership 01
Port o gen 5c3d0f membership 01
```

3 Bring down the rest of the stack:

Stop vcsmm:

```
# /etc/rc.d/rc2.d/S98vcsmm stop
```

Stop lmx:

```
# /etc/rc.d/rc2.d/S71lmx stop
```

Stop odm:

```
# /etc/rc.d/rc2.d/S99odm stop
```

Stop vxgms:

```
# /etc/methods/gmskextadm unload
```

Stop vxglm:

```
# /etc/methods/glmkextadm unload
```

Stop vxfen:

```
# /etc/rc.d/rc2.d/S97vxfen stop
```

Stop gab:

```
# /sbin/gabconfig -U
```

```
# /etc/methods/gabkext -stop
```

Stop llt:

```
# /sbin/lltconfig -U
```

4 Remove the Storage Foundation for Oracle RAC 7.0.1 patches.

- Enter the following command to get the list of patches which can be rollback:

```
# ls1pp -L | grep VRTS | grep " A "
```

- Reject each patch from the patch list, for example:

```
# installp -rBf /tmp/reject.list
```

5 Reboot the systems. On each system, run the following command.

```
# /usr/sbin/shutdown -r now
```

Rolling back Veritas Cluster Server manually

Use the following procedure to roll back VCS 7.0.1 to VCS 7.0 on your cluster manually. To uninstall VCS, see the *Veritas Cluster Server 7.0 Installation Guide*.

Note: Use this procedure only when rolling back VCS. Do not roll back VCS when it is part of other products that rely on VCS, for example Storage Foundation Clustered File System High Availability or Storage Foundation for Oracle RAC.

To roll back 7.0.1:

- 1 Verify that all of the VCS 7.0.1 patches are in the APPLIED state. Create a text file called `filesets.to.reject` that contains the name and version of each fileset, one per line, exactly as shown below.

```
VRTSvcs          7.0.1.0
VRTScps          7.0.1.0
VRTSvxfen        7.0.1.0
```

- 2 On each node, make a local copy of `filesets.to.reject` and then type:

```
# nohdr='^Z$'
# while read pkg ver; do
  lslpp -l $pkg | egrep -v "$nohdr"
  nohdr='^ Fileset +Level State '
done < filesets.to.reject
```

Note: Any updates that are in COMMITTED state cannot be rejected (undone). You must remove each one and then re-install it.

- 3 List the service groups in your cluster and their status. On any node, type:

```
# hagrps -state
```

- 4 If there is some service group is created, for example ClusterService service group, take the ClusterService service group offline if it is running. On any node, type:

```
# hagrps -offline -force ClusterService -any
```

- 5 Make the VCS configuration writable. On any node, type:

```
# haconf -makerw
```

- 6 Freeze all service groups except the ClusterService service group. On any node, type:

```
# hagrps -list | sort -u +0b -1 | \  
  while read grp sys ; do  
    hagrps -freeze $grp -persistent  
  done
```

You can safely ignore the warning about the failure to freeze the ClusterService group.

- 7 Save the configuration (main.cf) file with the groups frozen. On any node, type:

```
# haconf -dump -makero
```

- 8 Make a backup copy of the current main.cf and all types.cf configuration files. For example, on one node in the cluster, type:

```
# cp /etc/VRTSvcs/conf/config/main.cf \  
  /etc/VRTSvcs/conf/main.cf.save  
# cp /etc/VRTSvcs/conf/config/types.cf \  
  /etc/VRTSvcs/conf/types.cf.save
```

- 9 Shut down VCS. On any node, type:

```
# /opt/VRTSvcs/bin/hastop -all
```

- 10 Shut down CmdServer. On each node, type:

```
# /opt/VRTSvcs/bin/CmdServer -stop
```

- 11 Verify that VCS has shut down.

- On any node, type:

```
# /sbin/gabconfig -a
```

The output resembles:

```
GAB Port Memberships  
Port a gen 23dc0001 membership 01
```

Output for membership for port h does not appear.

- On each node, run the command:

```
# ps -ef | egrep "had|hashadow|CmdServer"
```

Terminate any instances of had, hashadow, or CmdServer that still run after 60 seconds.

12 Stop AMF, fencing, GAB, and LLT.

```
# /etc/init.d/amf.rc stop
# /etc/init.d/vxfen.rc stop
# /etc/methods/vxfenext -stop
# /etc/init.d/gab.rc stop
# /etc/methods/gabkext -stop
# /etc/init.d/llt.rc stop
```

13 Preview the patch removal selection and validity tests. On each node, type:

```
# installp -pr -gXv -f filesets.to.reject
```

Confirm that the patches to be removed are exactly the same as those listed in the filesets.to.reject file that you created in step 1.

14 Perform the patch removal. On each node, type:

```
# installp -r -gXv -f filesets.to.reject
```

Review the summaries at the end of each run and confirm that all of the intended patches removed successfully.

15 Reboot all nodes in the cluster.

16 After VCS has started, perform the following steps:

- Verify all resources have been probed. On any node, type:

```
# hastatus -summary
```

- Unfreeze all service groups. On any node, type:

```
# haconf -makerw
# hagr -list | sort -u +0b -1 | \
  while read grp sys ; do
    hagr -unfreeze $grp -persistent
  done
# haconf -dump -makero
```

You can safely ignore the warning about the failure to unfreeze the ClusterService group.

- 17 Bring the ClusterService service group online, if necessary. On any node, type:

```
# hagr -online ClusterService -sys system
```

where system is the node name.

Removing the Veritas product

Use one of the following procedures to remove the Veritas product.

Removing 7.0.1 on Veritas Storage Foundation or Veritas Storage Foundation Cluster File System High Availability

You can use the following procedure to uninstall 7.0.1 on SF or SFCFSHA.

To uninstall 7.0.1 on Veritas Storage Foundation or Veritas Storage Foundation Cluster File System High Availability

- 1 Log in as superuser.
- 2 Verify that `/opt/VRTS/bin` is in your `PATH` so you can execute all product commands.
- 3 Unmount all Storage Checkpoints and file systems:

```
# umount /checkpoint_name  
# umount /filesystem
```

- 4 Enter the following command to check if any VxFS file systems or Storage Checkpoints are mounted:

```
# mount | grep vxfs
```

- 5 If you have created any Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:
 - Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.
 - Use the `vrxvg stop` command to stop each RVG individually:

```
# vxrv -g diskgroup stop rvg_name
```

- On the Primary node, use the `vxrlink status` command to verify that all RLINKs are up-to-date:

```
# vxrlink -g diskgroup status rlink_name
```

Caution: To avoid data corruption, do not proceed until all RLINKs are up-to-date.

- 6 Stop activity to all VxVM volumes. For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.

- 7 Stop all VxVM volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

To verify that no volumes remain open, enter the following command:

```
# vxprint -Aht -e v_open
```

- 8 To shut down and remove the installed Veritas filesets, use the appropriate command in the `/opt/VRTS/install` directory. For example:

```
# ./installer -uninstall
```

You can use this command to remove the filesets from one or more systems.

- 9 After uninstalling the Veritas software, refer to the appropriate product's 7.0 Installation Guide document to reinstall the 7.0 software.

Removing 7.0.1 on Veritas Storage Foundation for Oracle RAC

You can use the following procedure to uninstall the 7.0.1 on Storage Foundation for Oracle RAC systems.

Note: This procedure will remove the complete SF for Oracle RAC stack from all nodes.

To uninstall the 7.0.1 on Veritas Storage Foundation for Oracle RAC

- 1 Stop Oracle and CRS on each node of the cluster.
 - If CRS is controlled by VCS, log in as superuser on each system in the cluster and enter the following command:

```
# hastop -all
```

- If CRS is not controlled by VCS, enter the following command on each node of the cluster to stop CRS:

```
# crsctl stop crs -f
```

Unmount all VxFS file system used by a database or application and enter the following command to each node of the cluster:

```
# hastop -local
```

- 2 Verify the output of the `gabconfig -a` command to ensure that VCS has been stopped. In the `gabconfig -a` command output, the VCS engine or high availability daemon (HAD) port `h` is not displayed. This indicates that VCS has been stopped.

```
# /sbin/gabconfig -a
```

Sample output:

```
GAB Port Memberships
=====
Port a gen 5c3d0b membership 01
Port b gen 5c3d10 membership 01
Port d gen 5c3d0c membership 01
Port o gen 5c3d0f membership 01
```

- 3 Uninstall Storage Foundation for Oracle RAC.

```
# cd /opt/VRTS/install
# ./installer -uninstall MyNode1 MyNode2
```

- 4 After uninstalling the filesets, refer to the *Veritas™ Storage Foundation for Oracle RAC 7.0 Installation and Configuration Guide* to reinstall the 7.0 software.

About the installation and the uninstallation scripts

This appendix includes the following topics:

- [About the installation and the uninstallation scripts](#)

About the installation and the uninstallation scripts

Veritas™ Veritas InfoScale 7.0.1 provides an installation and upgrade script. To install or upgrade the patches that are included in this release, you can use the `installmr` script. The `installmr` script lets you install or upgrade all the patches that are associated with the packages installed.

For more information regarding installation,

Veritas has introduced a new Install Bundles feature to help you install or upgrade directly to maintenance level with one execution. You can use the `-base_path` option to install or upgrade base and maintenance bundles. There are a few prerequisites for using Install Bundles feature for installation and upgrade of 7.0.1 mentioned below:

The `installmr` script options

The following table lists the command line options for the `installmr` and `upgrade` script:

Table A-1 The command line options for the product installmr script

Command Line Option	Function
<i>system1 system2...</i>	Specifies the systems on which to run the installation options. A system name is required for all options. If not specified, the command prompts for a system name.
-base_path	The <i>-base_path</i> option is used to define the path of a base level release to be integrated with a maintenance level release in order for the two releases to be simultaneously installed.
-patch_path	Defines the path of a patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed.
-patch2_path	Defines the path of a patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed.
-patch3_path	Defines the path of a patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed.
-patch4_path	Defines the path of a patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed.
-patch5_path	Defines the path of a patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed.
-precheck	Performs a preinstallation check to determine if systems meet all installation requirements. Veritas recommends doing a precheck before installing a product.
-postcheck	Checks any issues after installation or upgrading on the system.

Table A-1 The command line options for the product installmr script
(continued)

Command Line Option	Function
<code>-responsefile <i>response_file</i></code>	Automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. The <i>response_file</i> must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file.
<code>-logpath <i>log_path</i></code>	Specifies a directory other than <code>/opt/VRTS/install/logs</code> as the location where installer log files, summary files, and response files are saved.
<code>-tmppath <i>tmp_path</i></code>	Specifies a directory other than <code>/var/tmp</code> as the working directory for the installation scripts. This destination is where initial logging is performed and where filesets are copied on remote systems before installation.
<code>-timeout <i>timeout_value</i></code>	The <code>-timeout</code> option is used to specify the number of seconds that the script should wait for each command to complete before timing out. Setting the <code>-timeout</code> option overrides the default value of 1200 seconds. Setting the <code>-timeout</code> option to 0 will prevent the script from timing out. The <code>-timeout</code> option does not work with the <code>-serial</code> option.
<code>-keyfile <i>ssh_key_file</i></code>	Specifies a key file for secure shell (SSH) installs. This option passes <code>-i <i>ssh_key_file</i></code> to every SSH invocation.
<code>-hostfile <i>full_path_to_file</i></code>	Specifies the location of a file that contains a list of hostnames on which to install.
<code>-nim</code>	Produces a NIM configuration file for installing with NIM.
<code>-require</code>	The <code>-require</code> option is used to specify a installer patch file.

Table A-1 The command line options for the product installmr script
(continued)

Command Line Option	Function
-serial	Specifies that the installation script performs install, uninstall, start, and stop operations on each system in a serial fashion. If this option is not specified, these operations are performed simultaneously on all systems.
-rsh	Specifies this option when you want to use RSH and RCP for communication between systems instead of the default SSH and SCP.
-redirect	Displays progress details without showing the progress bar.
-pkgset	Discovers and displays the fileset group (minimum, recommended, all) and filesets that are installed on the specified systems.
-pkgtable	Displays product's filesets in correct installation order by group.
-listpatches	The <code>-listpatches</code> option displays product patches in correct installation order.
-comcleanup	The <code>-comcleanup</code> option removes the secure shell or remote shell configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of the shell are abruptly terminated.
-version	Checks and reports the installed products and their versions. Identifies the installed and missed filesets and patches where applicable for the product. Provides a summary that includes the count of the installed and any missed filesets and patches where applicable. Lists the installed patches and available updates for the installed product if an Internet connection is available.

Table A-1 The command line options for the product installmr script
(continued)

Command Line Option	Function
-nolic	Allows installation of product filesets without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.
-disable_dmp_native_support	Disables Dynamic multi-pathing support for native the LVM volume groups/ZFS pools during an upgrade. Retaining Dynamic multi-pathing support for the native LVM volume groups/ZFS pools during an upgrade increases fileset upgrade time depending on the number of LUNs and native LVM volume groups/ZFS pools configured on the system. The <code>-disable_dmp_native_support</code> option is supported in upgrade scenario only.
-noipc	Disables the installer from making outbound networking calls to Veritas Operations Readiness Tool (SORT) in order to automatically obtain patches and release information updates.

The uninstallmr script options

The following table lists the command line options for uninstallmr script:

Table A-2 The command line options for the product uninstallmr script

Command Line Option	Function
<i>system1 system2...</i>	Specifies the systems on which to run the installation options. A system name is required for all options. If not specified, the command prompts for a system name.

Table A-2 The command line options for the product `uninstallmr` script
(continued)

Command Line Option	Function
<code>-responsefile response_file</code>	Automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. The <code>response_file</code> must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file.
<code>-logpath log_path</code>	Specifies a directory other than <code>/opt/VRTS/install/logs</code> as the location where installer log files, summary files, and response files are saved.
<code>-tmppath tmp_path</code>	Specifies a directory other than <code>/var/tmp</code> as the working directory for the installation scripts. This destination is where initial logging is performed and where filesets are copied on remote systems before installation.
<code>-timeout timeout_value</code>	The <code>-timeout</code> option is used to specify the number of seconds that the script should wait for each command to complete before timing out. Setting the <code>-timeout</code> option overrides the default value of 1200 seconds. Setting the <code>-timeout</code> option to 0 will prevent the script from timing out. The <code>-timeout</code> option does not work with the <code>-serial</code> option.
<code>-keyfile ssh_key_file</code>	Specifies a key file for secure shell (SSH) installs. This option passes <code>-i ssh_key_file</code> to every SSH invocation.
<code>-hostfile full_path_to_file</code>	Specifies the location of a file that contains a list of hostnames on which to install.
<code>-serial</code>	Specifies that the installation script performs install, uninstall, start, and stop operations on each system in a serial fashion. If this option is not specified, these operations are performed simultaneously on all systems.
<code>-rsh</code>	Specifies this option when you want to use RSH and RCP for communication between systems instead of the default SSH and SCP.

Table A-2 The command line options for the product `uninstallmr` script
(continued)

Command Line Option	Function
<code>-redirect</code>	Displays progress details without showing the progress bar.
<code>-listpatches</code>	The <code>-listpatches</code> option displays product patches in correct installation order.
<code>-comcleanup</code>	The <code>-comcleanup</code> option removes the secure shell or remote shell configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of the shell are abruptly terminated.
<code>-version</code>	Checks and reports the installed products and their versions. Identifies the installed and missed filesets and patches where applicable for the product. Provides a summary that includes the count of the installed and any missed filesets and patches where applicable. Lists the installed patches, hotfixes, and available updates for the installed product if an Internet connection is available.
<code>-require</code>	The <code>-require</code> option is used to specify a installer patch file.
<code>-noipc</code>	Disables the installer from making outbound networking calls to Veritas Operations Readiness Tool (SORT) in order to automatically obtain patches and release information updates.
<code>-comsetup</code>	Sets up the ssh or rsh communication between systems without requests for passwords or passphrases.

Index

I

installsfrac
 upgrading SF Oracle RAC 26

P

planning to upgrade VVR 13
preinstallation 13

S

SF Oracle RAC upgrade
 using installsfrac 26

U

upgrading VVR
 from 4.0 14
 planning 13

V

Veritas InfoScale upgrade
 preparation 25
VVR 4.0
 planning an upgrade from 14