# Veritas InfoScale™ Operations Manager 7.3.1 Frequently Asked Questions

**VERITAS**™

Last updated: 2017-11-05

## Legal Notice

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

http://www.veritas.com

## Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

| | |
|---|---|
| Worldwide (except Japan) | CustomerCare@veritas.com |
| Japan | CustomerCare_Japan@veritas.com |

## Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

## Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

doc.feedback@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

## Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

# Contents

# General

This chapter includes the following topics:

- Overview of Veritas InfoScale Operations Manager

- Reporting

- Performance statistics

## Overview of Veritas InfoScale Operations Manager

### What is Veritas InfoScale Operations Manager?

Veritas InfoScale Operations Manager is a comprehensive management platform, for Storage Foundation and Cluster Server environments, that helps you optimize your data center assets, with a solution to centralize visibility and control, ensure availability, scale operations, increase storage utilization, and maintain compliance.

### What documentation resources are available for Veritas InfoScale Operations Manager?

The following documentation resources are available for Veritas InfoScale Operations Manager:

| Online Help | Veritas InfoScale Operations Manager help is now provided in two modes – offline and online. The offline mode requires you to first download and install the Veritas InfoScale Operations Manager Help add-on on the Management Server. For the online mode, the help content in hosted on the web, and is accessed directly when you launch the product help. |
| | Visit Veritas Services and Operations Readiness Tools (SORT) to download the Veritas InfoScale Operations Manager Help add-on: |
| | https://sort.veritas.com/vom |
| Guides | The Veritas InfoScale Operations Manager user documentation is available on: |
| | https://sort.veritas.com/documents |
| Videos | Videos to get started using Veritas InfoScale Operations Manager are available on: |
| | http://www.veritas.com/community/videos/vom-videos |

## Does Veritas InfoScale Operations Manager need anything that is installed on the managed host to work with Storage Foundation High Availability 5.x?

Yes. Every version of Storage Foundation High Availability that Veritas InfoScale Operations Manager manages requires the VRTSsfmh package to be installed. However, a compatible version of this package is bundled with Storage Foundation High Availability 5.1, and later versions. Best practice is to upgrade that VRTSsfmh package to the same version as Management Server to get the latest features and fixes.

## Does Veritas InfoScale Operations Manager interfere with Storage Foundation High Availability's functionality?

No. The Veritas InfoScale Operations Manager agent is not dependent on the Storage Foundation High Availability product and can be added, removed, or upgraded without any disruption to the configured applications, Storage Foundation High Availability, or the operating system.

## Does Veritas InfoScale Operations Manager require the Veritas Enterprise Administrator?

Veritas Enterprise Administrator (VEA) service is only required on the managed host for Windows and HP-UX 3.5 discovery.

## How frequently is managed host information updated to the Veritas InfoScale Operations Manager Management Server database?

The discovery on each managed host is broken down into families to focus on a particular functional area that Veritas InfoScale Operations Manager discovers information about. For a table listing each family and its frequency of discovery, refer to the *Veritas InfoScale Operations Manager Management Server Installation and Configuration Guide*.

Additionally, Storage Foundation and Cluster Server (VCS) families are also event driven. For example, when a DMP path is disabled, or a service group becomes faulted, it triggers a discovery cycle so that the information is quickly updated in the Management Server database. This event-driven mechanism results in a near real-time reporting for Storage Foundation and VCS configurations.

With the exception of a small heartbeat communication occurring every 5 minutes, no additional data is sent across to the MS unless changes to the configuration are detected. Refer to the *Veritas InfoScale Operations Manager Management Server User Guide* for more information on Veritas InfoScale Operations Manager managed host discovery.

## Does Veritas InfoScale Operations Manager display localized (i.e. Japanese or Chinese) file system mount points?

Yes. The default encoding Veritas InfoScale Operations Manager uses is UTF-8. Any other encoding that is used requires that the xprtld daemon on the managed host be run under the locale/encoding that the mount point names were created. English, Japanese, Simplified Chinese, and all UTF-8 locales are generally supported.

## Does Veritas InfoScale Operations Manager support other non-Veritas volume managers and file systems?

Yes. Veritas InfoScale Operations Manager discovers Logical Volume Manager (LVM) information on Linux, HP-UX, and AIX managed hosts, as well as ZFS information on Solaris. Veritas InfoScale Operations Manager provides discovery of this information only; no administrative options are currently available. For Windows, it discovers both Basic and Dynamic Volumes.

For more information, refer to the *Veritas InfoScale Operations Manager Hardware and Software Compatibility List (HSCL)*.

## Does Veritas InfoScale Operations Manager support other non-Veritas multi-pathing solutions?

Yes. Besides support for Veritas DMP, Veritas InfoScale Operations Manager also supports the discovery of EMC PowerPath (for Windows and Linux), EMC PowerPath /Virtual Edition (VE) of ESX Server, Microsoft MPIO, HP Native multipathing, MPIO on Solaris, and DM-Multipathing on Linux. However, the DMP Management feature supports only Veritas DMP and Veritas DMP for VMware.

For more information, refer to the *Veritas InfoScale Operations Manager Hardware and Software Compatibility List (HSCL)*.

## Does Veritas InfoScale Operations Manager support other clustering solutions?

Yes. Veritas InfoScale Operations Manager supports discovery of Microsoft failover cluster (MSFOC) and VMware HA cluster.

For more information, refer to the *Veritas InfoScale Operations Manager Hardware and Software Compatibility List (HSCL)*.

## Can I adjust the session inactivity timeout in the Management Server console?

Yes. To define the web server session timeout, on the Management Server home page, click **Settings**, and click **Management Server**. In **Web Server Settings** you can set the timeout period.

Although the default value is set at 30 minutes, technically the session timeout happens after 60 minutes. In the first 30 minutes of inactivity or no mouse clicks, the browser session continues to poll the Management Server intermittently. After exactly 30 minutes a pop-up window appears. Click **Continue** in the pop-up window to continue the web server session without having to enter the user credentials. If the pop-up window is not acknowledged, then the 30-minutes timeout period of the Tomcat web server starts. After 30 minutes of inactivity, the session is terminated. If you now click **OK** in the pop-up window, you are asked to enter your user credentials.

It is not recommended to set a large timeout as that may increase the memory utilization on the Management Server. If many people log on to Veritas InfoScale Operations Manager simultaneously and do not explicitly log off, it could cause out-of-memory errors.

## When should I create a Business Application?

A Business Application should be created when, as an administrator, you want to show associated objects and faults with the base that you have defined. Business Application is more resource intensive as it automatically discovers associated

objects. So, it is recommended that you specify less than 100 base objects. Business Application also manages multi-tier applications and fault management using the Management Server console.

## Which VRTSsfmh package versions are bundled with various Veritas InfoScale Operations Manager and Storage Foundation High Availability releases

**Table 1-1** VRTSsfmh package versions bundled with Veritas InfoScale Operations Manager releases

| Veritas InfoScale Operations Manager release | VRTSsfmh version | SFHA release that it is bundled with |
|---|---|---|
| 2.1 (SFM) | 2.1.198.0 | SFHA AIX, Solaris, Linux 5.1 |
| | 2.1.210.0 | SFHA Windows 5.1SP1 |
| 2.1RP1 (SFM) | 2.1.229.0 | SFHA Linux 5.0MP4<br><br>SFHA UNIX 5.1RP1<br><br>SFHA Linux and Solaris 5.1RP2 |
| 3.0 | 3.0.357.0 | |
| | 3.0.358.0 | SFHA Windows 5.1 SP2<br><br>ApplicationHA VMware Linux 5.1<br><br>ApplicationHA VMware Windows 5.1SP1 |
| 3.0 RP1 | 3.0.402.0 | |
| 3.1 | 3.1.429.0 | SFHA Solaris, AIX 5.1SP1<br><br>ApplicationHA VMware Linux 5.1SP2 |
| 3.1RP1 | 3.1.830.0 | SFHA HP, Linux 5.1SP1 & 5.1SP1RP1<br><br>SFHA AIX, Solaris, Linux 5.1SP1RP2<br><br>ApplicationHA VMware Windows 5.1SP2 |
| 4.0 | 4.0.1097.0 | |
| 4.0RU1 | 4.0.1598.0 | ApplicationHA VMware 6.0 |

**Table 1-1**    VRTSsfmh package versions bundled with Veritas InfoScale
Operations Manager releases *(continued)*

| Veritas InfoScale Operations Manager release | VRTSsfmh version | SFHA release that it is bundled with |
|---|---|---|
| 4.1 | 4.1.119.0 | SFHA AIX, Linux, Solaris 6.0<br>Windows 6.0<br>ApplicationHA Unix 6.0 |
| 5.0 | 5.0.196.0 | SFHA AIX, Linux, Solaris 6.0 |
| 6.0 | 6.0.0.0 | SFHA AIX, Linux, Solaris 6.1<br>SFWHA Windows 6.1 |

### While navigating through Management Server views or performing operations, blank views are displayed. How should I rectify this error?

To resolve this issue, you need to refresh the Web browser or clear the browser's cache. After this, retry to run the operation.

# Reporting

### What reports does Veritas InfoScale Operations Manager offer?

Veritas InfoScale Operations Manager offers reports in five different categories, such as Trend/Activity, Storage Utilization, Inventory, True up, and Exception. For a complete list of the reports available in Veritas InfoScale Operations Manager, refer to the *Veritas InfoScale Operations Manager User Guide*.

### Is Veritas InfoScale Operations Manager able to create comparisons between reports?

Veritas InfoScale Operations Manager does not have an explicit feature, but you can save the contents of a report as a comma-separated file, and use the same for further analysis. You can also use Veritas InfoScale Operations Manager Web services API to get data and create reports for analysis.

# Performance statistics

### What performance-related data does Veritas InfoScale Operations Manager track?

Veritas InfoScale Operations Manager tracks the following data that is displayed in the performance charts:

- Hosts - available memory, average CPU load, CPU utilization, Swap in Rate, and Used Swap

- Disks and volumes - read and write statistics

- File system - the size and the used space on the file system

- Initiator - the bytes read and written as well as read and write errors and queues lengths

- Path – read and write latency and average bytes read and written

- Virtualization server and virtual machine - available memory, CPU utilization, swap in rate, average CPU load, and used swap

- Path of a virtualization server – average read and write latency, and bytes read and written

- Storage array port, adapter, and enclosure – average read write latency, bytes read and written, IO operations and IO throughput

### Where are performance statistics stored?

The performance statistics data is not stored in the Management Server database, but on the managed host. If Management Server is not running, Veritas InfoScale Operations Manager continues to collect historic performance statistics on each managed host only if the managed host is configured with Management Server.

Data logs for host, volume, disk, file system, path, and initiator are stored on the managed host. The data logs for virtualization server, virtual machine, path, and initiator are stored on the Control Host. For storage array (port, adapter, and enclosure), data log for 1 day is stored on the discovery host, where as all the other logs are stored on Management Server.

The default directory on UNIX or Linux managed host is

`/var/opt/VRTSsfmh/stats`

For Windows 2003

`%ALLUSERSPROFILE%\Application Data\Symantec\VRTSsfmh\stats`

For Windows 2008/2008 R2

```
%ALLUSERSPROFILE%\Symantec\VRTSsfmh\stats
```

For Windows 2012

```
%ALLUSERSPROFILE%\Symantec\VRTSsfmh\stats
```

In case of storage array and VMware metering, Veritas InfoScale Operations Manager also stores the data in the shared folder.

- UNIX: `/var/opt/VRTSsfmh/shared/stats`

- Windows 2003: `%ALLUSERSPROFILE%\Application Data\Symantec\VRTSsfmh\shared\stats`

- Windows 2008/2008 R2: `%ALLUSERSPROFILE%\Symantec\VRTSsfmh\shared\stats`

- Windows 2012: `%ALLUSERSPROFILE%\Symantec\VRTSsfmh\shared\stats`

## Are performance graphs supported on Windows managed hosts?

Yes, Veritas InfoScale Operations Manager version 6.0 or later supports performance statistics collection for Windows managed hosts. The following performance statistics are collected for Windows managed hosts:

- Host

- Disk

- Volume

- Windows native file system
  Only read and write statistics are collected for file system.

For more information on performance metering, refer to *Veritas InfoScale Operations Manager User Guide*.

# Infrastructure

This chapter includes the following topics:

- Infrastructure overview

## Infrastructure overview

### Is xprtld a Web server?

Yes. It is a modified embedded Web server based on the popular open source shttpd that listens on port 5634. It only communicates via authenticated SSL. It also has a built-in role-based authorization mechanism. Anything with the URL containing "admin" can only be accessed by the root user or an OS account with admin privilege. All scripts within agent directory under *sfmh_bin_dir*/web/agent can be accessed from other managed hosts as "root". These scripts are hardened and use Perl with Taint mode turned on.

### Why does Veritas InfoScale Operations Manager use a separate Web server for the console when xprtld is also a Web server?

The xprtld Web server is a stripped down version of Web server which can only handle HTTP requests. Veritas InfoScale Operations Manager uses Apache Tomcat for the console as it provides the necessary servlet containers for the Java-based Web application to function.

### What is Xprtlc ?

Xprtlc, also known as Xprtl Client, is a CLI interface that communicates with xprtld.

### What is fault.pl?

There are several aspects of the system that Veritas InfoScale Operations Manager monitors as part of the VRTSsfmh package that is installed on the managed host.

However, this is not all encompassing. Users of Veritas InfoScale Operations Manager can choose to add their own discovery and exception detection scripts to augment our offering. Fault.pl lets you indicate if a host is faulted or at-risk, and it shows up in the Veritas InfoScale Operations Manager dashboard. A simple HTTP server monitoring script that runs as a cronjob, can call fault.pl if it stops running, and clear it when it starts running again. See the Veritas InfoScale Operations Manager documentation for more details.

## What is xdist?

xdist is a powerful command that lets you push a script to managed hosts in the Management Server domain, and run it. Typical use cases can include provisioning a server, updating a patch on multiple computers, or detecting compliance-related anomalies in your environment. This command can only be run as root on Management Server, and it runs commands as root on the target systems. It is secure and arbitrary commands cannot be called unless you bypass it using your own scripts. It uses a white listing mechanism for authorized commands similar to how sudo operates. See the Veritas InfoScale Operations Manager documentation for more details.

## What is xinfo?

xinfo allows you the options to get information about the state of the Veritas InfoScale Operations Manager infrastructure. See the Veritas InfoScale Operations Manager documentation for more details.

## What is xclusinfo?

xclusinfo interfaces with the Veritas InfoScale Operations Manager database and extracts information pertaining to the clusters and their associated objects that are discovered in the data center.

## What is vomadm?

The `vomadm` command lets you perform several operations such as listing all enclosures configured through Storage Insight Add-on, host management, deployment of hotfixes, business application management, service management, and domain management. The host-mgmt, domain-mgmt, and makeBE options can be used only on the Veritas InfoScale Operations Manager Management Server. These commands are supported on Linux and Windows operating system. For more information on vomadm command, refer to the *Veritas InfoScale Operations Manager User Guide*.

## Can I access the information discovered by Veritas InfoScale Operations Manager using the command-line interface (CLI)?

Yes, using Veritas InfoScale Operations Manager Web services API, you can access the information. Veritas InfoScale Operations Manager provides an API that can be accessed over the HTTP protocol using any standard HTTP client. The interface provides the ability to query Veritas InfoScale Operations Manager discovered data and to manage user-defined attributes for certain object types. The API can be used for searching the objects, listing their properties, and setting the extended attributes on them. These APIs can be invoked using the XPRTLC component or any other HTTP client like cURL. You have only Read-only access to the information. Operations such as creating or deleting a disk group are not supported.

You can also use the `vomadm` command-line interface (CLI) to perform tasks related to host management, business application management, application management, service management, and domain management.

For more information, refer to the *Veritas InfoScale Operations Manager User's Guide*.

# Settings and configuration

This chapter includes the following topics:

## Installation and upgrade

### Where can I find out how much space is required for Veritas InfoScale Operations Manager?

See the *Veritas InfoScale Operations Manager Management Server Installation and Configuration Guide* for information on how much space is required for Veritas InfoScale Operations Manager on Management Server and on managed hosts.

### I am running an older version of Veritas InfoScale Operations Manager, Storage Foundation Manager, or Cluster Server Management Console. How can I upgrade to Veritas InfoScale Operations Manager 7.3.1?

Upgrade to Veritas InfoScale Operations Manager 7.3.1 is only supported from Veritas InfoScale Operations Manager 4.1, or later versions. Users of Storage Foundation Manager need to upgrade to Veritas InfoScale Operations Manager 4.1 or later versions, and then upgrade to Veritas InfoScale Operations Manager 7.3.1. Users of Cluster Server Management Console need to start with a fresh installation of Veritas InfoScale Operations Manager.

### How can I upgrade Veritas InfoScale Operations Manager 5.0 Management Server on Solaris to Veritas InfoScale Operations Manager 7.3.1?

Veritas Operations Manager 5.0 is the last major version of Veritas InfoScale Operations Manager to support Solaris as a platform for Management Server. Before you upgrade your Management Server to a newer version, you need to migrate to a Management Server on Linux or Windows.

For information on Management Server Migration, refer to the *Veritas Operations Manager Management Server Migration Add-on 5.0 User Guide*.

### From which versions of managed host can I directly upgrade to Veritas InfoScale Operations Manager managed host 7.3.1?

The current release of VRTSsfmh package supports upgrades from version 2.x, or later. However, if a host has VRTSsfmh 2.0 package, it is recommended that you upgrade the VRTSsfmh package to 7.3.1 before managing the host using a 7.3.1 Management Server.

### Is Veritas InfoScale Operations Manager backward-compatible with Storage Foundation Manager 2.x managed host?

Yes. Discovery will still work. However, new Veritas InfoScale Operations Manager features and details are not seen for these managed hosts. In addition, VCS operation support was added only in Veritas InfoScale Operations Manager 3.0, implying that managed hosts also need to be running VRTSsfmh package version 3.0, or later.

### Why does Veritas InfoScale Operations Manager give me the option to set the Management Server host name during configuration?

Veritas InfoScale Operations Manager suggests the Management Server host name and IP address on the configuration page. You need to verify whether the host name and IP address is accessible from all intended managed hosts.

If you plan to configure Management Server HA in future, you need to use virtual IP and virtual host name while configuring Management Server.

### Is Management Server HA supported for Windows Management Server?

Yes, Management Server HA is supported for Windows Management Server. Currently, Management Server DR is not supported for Windows Management Server.

## Can Veritas InfoScale Operations Manager Management Server be installed on a virtual machine?

Yes, all it requires is an operating system that is in the list supported by Veritas InfoScale Operations Manager Management Server. Veritas InfoScale Operations Manager requires a 64-bit operating system for Linux and Windows.

For more information, see the *Veritas InfoScale Operations Manager Management Server Installation and Configuration Guide*.

## What is Auto Configure and gendeploy.pl?

The Auto Configure option lets you add a managed host to the Veritas InfoScale Operations Manager Management Server domain using a script and with minimal user interaction. Click **Settings**, click **Host**, and click **Auto Configure** to download the script.

The script can also be created using the gendeploy.pl utility on Veritas InfoScale Operations Manager Management Server. Run the following commands to generate the script:

- UNIX/Linux-based Management Server:

  ```
  /opt/VRTSsfmh/bin/gendeploy.pl --out addvommh.pl
  ```

- Windows-based Management Server (VRTSsfmh install directory may vary):
  ```
  cd "C:\Program Files\Veritas\VRTSsfmh\bin"
  ```
  ```
  perl.exe gendeploy.pl --out addvommh.pl
  ```

addvommh.pl is the script name used as an example.

You can copy the script (addvommh.pl) that is downloaded from Management Server or created using gendeploy.pl to all the managed hosts that you want to add to the domain.

After you copy the script, you have to run it on each host. These hosts must have the VRTSsfmh package installed before you run the script.

Run the following command to execute the script:

- UNIX managed host:
  ```
  chmod +x addvommh.pl
  ```
  ```
  ./addvommh.pl
  ```

- Windows managed host (VRTSsfmh install directory may vary):
  ```
  cd "C:\Program Files\Veritas\VRTSsfmh\bin"
  ```
  ```
  perl.exe addvommh.pl
  ```

The gendeploy-generated script (addvommh.pl) has the Veritas InfoScale Operations Manager Management Server host name embedded in it. This is the name used to contact the Management Server during managed host configuration. In case

Management Server is not reachable from the managed host by this default name, an alternate hostname/IP address can be specified using the `domain` option of `addvommh.pl`. This option is available only for managed host version 4.0RU1, or later. You can use the `hostname` option of `addvommh.pl` script to specify an alternate name for the managed host.

### How to remove hosts from Veritas InfoScale Operations Manager using the command line?

The `host-mgmt` option of the vomadm utility can be used to remove a single host, or multiple hosts, from Veritas InfoScale Operations Manager. It is currently supported only for hosts that are configured as Agents (hosts that have the VRTSsfmh package installed). Run one of the following commands on Management Server:

■ Linux:

```
/opt/VRTSsfmh/bin/vomadm host-mgmt --remove --host hostname
```

■ Windows:

```
"C:\Program Files\Veritas\VRTSsfmh\bin\perl.exe"
"C:\Program Files\Veritas\VRTSsfmh\bin\vomadm" host-mgmt --remove
--host hostname
```

Where, *hostname* is the name of the host that you want to remove.

For more information, see the *Veritas InfoScale Operations Manager User Guide*.

# Networking

### What protocol is used for Veritas InfoScale Operations Manager?

Veritas InfoScale Operations Manager uses an HTTPS-based protocol. Essentially, it uses Web services as the underlying message exchange format.

### What are the networking requirements? What firewall ports need to be opened?

All communication between the managed hosts and Management Server occurs through TCP port 5634. If you have a firewall in your environment, this port needs to be opened (bi-directional). For the user interface, you need to open port 14161 between Management Server and the client desktop on which the Web browser runs. No other port is required. The Management Server host name needs to be resolvable from the managed host. It is recommended that DNS be used for this. If the host name is not resolvable, you can specify a valid IP address. However,

this may affect the usability of the product, as the IP is displayed as the Host name in the Management Server console.

### What kind of network traffic can be expected if Veritas InfoScale Operations Manager is deployed?

Managed hosts send an HTTP request (ping) every 5 minutes to the Management Server indicating that it is UP. This request has less than 1 KB of payload. When there is a change detected on the managed host, the managed host sends an HTTP POST to the Management Server indicating the change. However, only differences (diffs) are sent. So, in an environment that does not change, there is no traffic other than the 5-minutes pings from each managed host. When there is a change, the payload size depends on the amount of change, which is never more than a complete initial discovery of that host. On managed hosts with 15,000 LUNs and about 2,000 file systems and volumes, the full discovery payload can be as large as a few megabytes.

### What kind of SNMP support is there in Veritas InfoScale Operations Manager?

SNMP trap support is limited in Veritas InfoScale Operations Manager. Veritas InfoScale Operations Manager ships with an SNMP MIB as part of the Management Server package. You can select the specific events to be forwarded. To configure SNMP trap settings, on the Management Server home page, click **Settings** and click **Management Server**.

For near real-time discovery of VMware virtual machine states, ensure that port 162 is available as it is required by XTRAPD to listen to the SNMP traps.

For more information, refer to the *Veritas InfoScale Operations Manager Installation and Configuration Guide*.

# Add-ons

### What is a Veritas InfoScale Operations Manager add-on?

Veritas InfoScale Operations Manager add-ons allow the extension of the base functionality that is included in Veritas InfoScale Operations Manager. Refer to https://www.veritas.com/product/storage-management/infoscale-operations-manager for more information about the available add-ons.

### Do add-ons install anything on the managed host?

It depends on the add-on. Some add-ons are installed only on Management Server, while others are installed on both the managed host and Management Server. The managed host components are installed automatically as part of the add-on install.

### Which Veritas InfoScale Operations Manager Management Server and managed host versions are compatible with an add-on?

For information on Veritas InfoScale Operations Manager 7.3.1 add-on compatibility matrix, refer to *Veritas InfoScale Operations Manager Hardware and Software Compatibility List (HSCL)*.

# Security

### What privileges do you need on a managed host?

To add a host into a domain, you need to know the root user and password of the managed host or be an Administrator on Windows-based managed host. Once a host is added, a secure channel is setup between Management Server and the managed host using PKI/PKCS mechanisms. After the host is added to the domain, the password for the root user can be changed, and it does not affect the operation of Veritas InfoScale Operations Manager. Veritas InfoScale Operations Manager does not remember this password once the host has been configured.

### Does xprtld allow for PAM, Active Directory, or LDAP-based authentication?

This is allowed for xprtld running on Management Server. For the managed host, Veritas InfoScale Operations Manager allows native OS authentication for end users.

# Hot fixes, patches, and packages

### Is Veritas InfoScale Operations Manager able to show which SF/HA patches a specific host requires?

Veritas InfoScale Operations Manager integrates with Veritas Services and Operations Readiness Tools (SORT) to retrieve the latest information about hot fixes, point patches, and release patches on a per-server basis. This information provides a system administrator an efficient way to manage patches so that the server environments are up-to-date.

The information includes details on the criticality of the patch, whether the patch installation requires application downtime, whether the patch has kernel components, whether the patch installation requires system reboot, and the number of customers who have downloaded the patch. This information has to be present with the patch on SORT for Veritas InfoScale Operations Manager to show it.

### Is Veritas InfoScale Operations Manager able to show available and applicable Veritas InfoScale Operations Manager hot fixes, patches, and packages?

Veritas InfoScale Operations Manager Management Server console shows the applicable hot fixes, patches, and packages that are available on SORT.

The information includes details on the criticality of the hot fix, patch, or package, its status, and its release date. You can also view whether the installation requires application downtime, whether it has kernel components, and the download count number. This information has to be present with the patch on SORT for Veritas InfoScale Operations Manager to show it.

### My network does not allow for direct Internet access. Can I still access the Veritas Services and Operations Readiness Tools (SORT) functionality?

Yes. Veritas InfoScale Operations Manager Management Server supports the use of a proxy server to connect to SORT.

### Can I use Veritas InfoScale Operations Manager to deploy any type of hot fixes including Storage Foundation hot fixes?

Currently, you can deploy Veritas InfoScale Operations Manager-specific hot fixes and VBS packages. Patch Installer Add-on adds the capability of deploying Storage Foundation High Availability (SFHA) hot fixes that are configured as VOM deployable.

# Organization and permissions

### Can I add secondary authentication broker to Veritas InfoScale Operations Manager?

No, in Veritas InfoScale Operations Manager 7.3.1 you cannot add secondary authentication broker.

### Which types of authentication domains are supported in Veritas InfoScale Operations Manager?

Veritas InfoScale Operations Manager supports the authentication mechanism that is configured in the operating system, including Pluggable Authentication Modules (PAM), Network Information Service (NIS), or NIS+, with the exception of multi-factor authentication mechanisms. In addition to the native operating system authentication,Veritas InfoScale Operations Manager supports Lightweight Directory Access Protocol (LDAP) and Active Directory (AD). You can view the following

authentication domain types on the Veritas InfoScale Operations Manager log in page:

- Unixpwd

- Network (NT) Domain

- LDAP

- AD

## What are the predefined roles in Veritas InfoScale Operations Manager?

Veritas InfoScale Operations Manager has three predefined roles: Admin, Operator, and Guest.

A user group with Admin role can perform tasks such as creating or deleting a disk group, bringing a service group online, or performing thin reclamation on thin pools in an enclosure.

Operator role is available only in the Availability perspective. A user group with operator role can perform operations such as switching a service group or auto enabling a service group.

A user group with Guest role can only view the information displayed in the perspective.

## How do I assign permissions to user groups in Veritas InfoScale Operations Manager?

Veritas InfoScale Operations Manager makes use of the existing user groups within Lightweight Directory Access Protocol (LDAP), Active Directory (AD), or the native operating system authentication of Windows or UNIX. The root user can configure LDAP or AD using the Management Server console. Click **Settings** > **Security** to configure LDAP or AD.

Click **Settings** > **Permissions** tab to assign permissions to the user groups on a perspective.

To assign permissions on Organizations and objects, right-click on the Organization or object and open **Properties** > **Permissions** tab.

## What are Organizations in Veritas InfoScale Operations Manager?

Organization is a collection of objects in a perspective that can be secured and managed as a group. Organizations can be created in all perspectives except in the Management Server perspective. The objects within the Organization may or may not represent the physical organization of the objects in the actual data center. You can also create nested Organizations.

## Why should I create an Organization?

In a real-life data center, an UNIX administrator may want to see all the UNIX hosts in a single location to facilitate operations. The UNIX administrator can create an Organization which is a virtual folder for all UNIX hosts. Similarly the Windows administrator can create an Organization having Windows hosts.

## Why should I assign permissions on Organizations?

Assigning permissions restricts unauthorized operations on an object. In a real-life data center, an UNIX administrator, who has created an Organization consisting of UNIX hosts will want a group of users to perform relevant task on the hosts. This group can be assigned the Admin role. The user group which works on Windows hosts can have a Guest role on this Organization. This will allow them to view the hosts but will be restricted from performing any actions.

# Server

This chapter includes the following topics:

- Centralized Storage Foundation administration

# Centralized Storage Foundation administration

## What are the Storage Foundation operations that are available through the centralized console of Veritas InfoScale Operations Manager?

**Table 4-1** Storage Foundation operations

| Object | Type of Operation |
|---|---|
| Disk groups | Creating disk groups |
| | Recovering disk groups |
| | Deporting disk groups |
| | Destroying disk groups |
| | Importing disk groups |
| | Adding disks to disk groups |
| | Removing disks from disk groups |
| | Resizing disks in disk groups |
| | Renaming disks in disk groups |
| | Upgrading disk groups |
| | Splitting disk groups |
| | Moving disk groups |
| | Joining disk groups |
| | Enabling/disabling Flexible Storage Sharing on disk groups |

**Table 4-1**        Storage Foundation operations *(continued)*

| Object | Type of Operation |
|--------|-------------------|
| Disks  | Disconnecting disks |
|        | Initializing disks |
|        | Recovering disks |
|        | Replacing disks |
|        | Bringing disks online |
|        | Taking disks offline |
|        | Evacuating disks |
|        | Setting disk usage |
|        | Running or scheduling Trim |
|        | Rescanning disks |
|        | Exporting and un-exporting disks for Flexible Storage Sharing |
|        | Creating, modifying, and deleting SmartIO cache |
|        | Enabling and disabling SmartIO cache |

**Table 4-1**      Storage Foundation operations *(continued)*

| Object | Type of Operation |
|---|---|
| Volumes | Creating volumes |
| | Stopping volumes |
| | Recovering volumes |
| | Reactivating volumes |
| | Deleting volumes |
| | Moving volumes |
| | Adding mirrors to volumes |
| | Removing the mirrors of volumes |
| | Creating instant volume snapshots |
| | Creating space optimized snapshots for volumes |
| | Creating mirror break-off snapshots for volumes |
| | Dissociating snapshots |
| | Reattaching snapshots |
| | Resizing volumes |
| | Restoring data from the snapshots of volumes |
| | Refreshing the snapshot of volumes |
| | Configuring a schedule for volume snapshot refresh |
| | Adding snapshot volumes to a refresh schedule |
| | Removing the schedule for volume snapshot refresh |
| | Setting volume usage |
| | Splitting snapshots |
| | Starting synchronization of snapshots |
| | Renaming volumes |
| | Enabling FMR |
| | Disabling FMR |

**Table 4-1** Storage Foundation operations *(continued)*

| Object | Type of Operation |
|---|---|
| File systems | Creating file systems |
| | Enabling change logs |
| | Disabling change logs |
| | Synchronizing change logs |
| | Removing change logs |
| | Defragmenting file systems |
| | Unmounting non-clustered file systems from hosts |
| | Mounting non-clustered file systems on hosts |
| | Unmounting clustered file systems |
| | Mounting clustered file systems on hosts |
| | Remounting file systems |
| | Checking file systems |
| | Creating file system snapshots |
| | Remounting file system snapshot |
| | Mounting file system snapshot |
| | Unmounting file system snapshot |
| | Removing file system snapshot |
| | Monitoring capacity of file systems |
| | Running or scheduling Trim |
| Volume replication | Configuring replications |
| | Adding a secondary |
| | Pausing the replication to a Secondary |
| | Resuming the replication of a secondary |
| | Starting replication to a Secondary |
| | Stopping the replication to a Secondary |
| | Switching a primary |
| | Taking over from an original Primary |
| | Removing a secondary |
| | Monitoring replications |

## Do we need any managed host components to be installed to perform centralized Storage Foundation operations?

VRTSsfmh 4.0, or later package must be installed on the SFHA hosts to perform centralized Storage Foundation operations. No other component is required to be installed on these hosts to perform the centralized Storage Foundation operations.

## What are the Storage Foundation High Availability (SFHA) supported versions?

- SFHA on Windows: Versions 5.x or later.

- SFHA on UNIX/Linux: Versions 4.1.x or later.

For more information, refer to the *Veritas InfoScale Operations Manager Hardware and Software Compatibility List (HSCL)*.

## Which Storage Foundation operations are not supported on a Windows host?

Following are the Storage Foundation operations that are not supported on Windows host:

Disk and disk group operations:

- Resizing disks in a disk group

- Moving disk groups

Volume operations:

- Moving volumes

- Starting synchronization of a snapshot

- Creating instant volume snapshots

- Creating space optimized snapshots for volumes

- Creating mirror-breakoff snapshots for volumes

- Restoring data from the snapshots of volumes

- Refreshing the snapshot of volumes

- Recovering volumes

- Reattaching snapshots

- Dissociating snapshots

- Splitting snapshots

- Renaming volume

- Enabling FastResync on volumes

- Disabling FastResync on volumes

File system operations:

- Creating file systems
- Defragmenting file systems
- Checking file systems
- Remounting file systems
- Mount file system
- Unmount file system
- Creating file system snapshots
- Mounting file system snapshot
- Unmounting file system snapshot
- Remounting file system snapshot
- Removing file system snapshot
- Enabling change logs
- Disabling change logs
- Synchronizing change logs
- Removing change logs

## Which file systems are supported for the mount and the unmount operations?

Mount operation: Supported file systems are VxFS, UFS, Ext2, Ext3, and Ext4.

Unmount operation: Supported file systems are VxFS, UFS, Ext2, Ext3, and Ext4, except for the root or the ZFS file system.

# Availability

This chapter includes the following topics:

- ApplicationHA management

- Cluster Server (VCS) fire drill

- Virtual Business Services

- Multi-Site Management

- VCS failover reporting and alerting

## ApplicationHA management

### What are the Veritas InfoScale Operations Manager components which are part of ApplicationHA support?

- The VRTSsfmh package that is part of Storage Foundation High Availability (SFHA), which performs the discovery on the virtual machine to support ApplicationHA and adds the necessary support on the virtualization infrastructure node.

- The Control Host Add-on that needs to be installed on the Management Server/Control Host, which adds the required discovery support for ApplicationHA on IBM logical partitioning (LPAR).

### Which ApplicationHA versions are supported by Veritas InfoScale Operations Manager?

ApplicationHA 6.0, and later.

For more information, refer to the *Veritas InfoScale Operations Manager Hardware and Software Compatibility List (HSCL)*.

## Which are the virtualization technologies supported by Veritas InfoScale Operations Manager?

The following virtualization technologies are supported by Veritas InfoScale Operations Manager:

- VMware ESX/ESXi

- Linux Kernel Virtual Machine (KVM)

- IBM Logical Partitions (LPAR)

- Oracle Solaris Zones

- Microsoft Hyper-V

- Oracle VM Server (OVM) for SPARC (Solaris LDOM)

Oracle Solaris Zones are displayed in the Server perspective and all other virtualization technologies are displayed in the Virtualization perspective.

## Can I deploy ApplicationHA on the virtual machine from Veritas InfoScale Operations Manager using Deployment Manager?

No. ApplicationHA needs to be manually installed on the virtual machine.

## What type of ApplicationHA management operations can I perform using the Management Server console?

Broadly, you can do two types of management operations:

- Configure application monitoring on the virtual machines.

- Administer the configured applications on virtual machines. For example, start an application, stop an application, enable application heartbeat, and disable application heartbeat.

## I am able to click on Configure Application Monitoring to launch the wizard and I can see input fields, but I am unable to configure the application. What might be the reason?

Check whether you have the privileges to perform the operation. You need admin privileges on the cluster to perform the Configure Application Monitoring operation.

## Can I configure Cluster Server (VCS) support for ApplicationHA from Veritas InfoScale Operations Manager?

Yes, you can. You can use the Enable/Disable ApplicationHA Infrastructure operation available on VCS nodes/clusters. Note that this operation is not valid for VMware, since VMware has its own HA solution to manage ApplicationHA virtual machines.

### What are the pre-requisites to perform the enable/disable ApplicationHA infrastructure operation?

- User should have admin privileges on clusters.

- VCS host should have been added to Veritas InfoScale Operations Manager Management Server domain.

- VCS should be running on the hosts.

- VCS host should be one of KVM servers, LDOM server, or LPAR.

- VRTSsfmh version should be 4.1, or later.

- VCS version should be 6.0, or later.

- Hardware Management Console (HMC) should be pre configured in Veritas InfoScale Operations Manager for LPAR hosts.

### How do I know the configuration status of VCS support for ApplicationHA on a node?

The configuration status of VCS support for ApplicationHA (ApplicationHA Infrastructure Status) is only displayed in the properties of the Infrastructure host (VCS host).

# Cluster Server (VCS) fire drill

### How is High Availability (HA) fire drill executed?

HA fire drill is executed by invoking the action entry points (.VFD) on the cluster nodes where the service group is offline. These are bundled and shipped with VCS. HA fire drill can be executed for a service group.

### How is Disaster Recovery (DR) fire drill executed?

DR fire drill is executed by bringing the fire drill (FD) service group online on the Global Cluster Option (GCO) clusters. An option is provided to take the FD service group offline after successfully bringing it online. To be able to run DR fire drills, a single Veritas InfoScale Operations Manager instance must manage all the GCO clusters.

### Can I configure fire drill service group through Veritas InfoScale Operations Manager?

No. Currently, Veritas InfoScale Operations Manager does not support configuring a fire drill service group.

## What platforms are supported for HA and DR fire drills?

HA fire drill is supported only on UNIX/Linux platforms as the action entry points (.VFDs) are not available on Windows. DR fire drill is supported on all platforms.

## Can I schedule fire drill runs?

Yes, both HA fire drills and DR fire drills can be scheduled. There is no default schedule as in Cluster Server Management Console, and it has to be set up manually. Existing schedules can be viewed and edited by using a cluster > **Service Group** node > **Fire Drill Schedules** tab in the console.

## How do I see the results of fire drill runs?

You can view the results of fire drill runs in the task log and also in the task pane.

# Virtual Business Services

## How are the Virtual Business Services back-end components deployed?

The VRTSvbs package contains the Virtual Business Services back-end components. This package is available by default with SFHA 6.0, SFWHA 6.0, and ApplicationHA 6.0 (UNIX) versions and later. For earlier releases of SFHA and ApplicationHA, do the following:

- Download the VRTSvbs packages for all required platforms from the Veritas website to a temporary directory on a local computer.

- Log in to the Management Server console from that computer. Upload all the packages for the relevant cluster platforms using the Deployment Manager.

- Select all the applicable hosts and install the packages using the Management Server console.

## Is Veritas InfoScale Operations Manager Management Server in the critical path and a single point of failure?

Veritas InfoScale Operations Manager Management Server is critical from the point of view of Virtual Business Services configuration, but not for its operation. A virtual business service cannot be created or edited without Veritas InfoScale Operations Manager. After a virtual business service is created, it continues to operate even if the Management Server is down. The Virtual Business Services back-end CLIs can be used for performing the operations and finding status. Veritas InfoScale Operations Manager also has its own high availability and disaster recovery provision to handle its failure.

## How often does the configurator run?

The configurator runs under two circumstances:

- Scheduled: Once every 5 minutes. This scheduled run pushes out any changes that have not yet been sent to one or more virtual business services that have fault management configured.

- Unscheduled: Any configuration changes made in the Management Server console to an existing virtual business service has fault management enabled by default.

## How can I know if all the nodes have been properly configured for Virtual Business Services to work?

There are several ways:

- You can view the "Fault Management Status" in the Management Server console for any virtual business service. This tab has an entry for each host in the virtual business service, and the configuration status on it. You can right-click on the a virtual business service in the tree panel and click on Properties from the menu to see the "Fault Management Status". For each host, there is a "Configured status" column that shows whether fault management is enabled on that host. Also, there is a "VBS package version" column that shows the version of the Virtual Business Services package installed on that host.

- You can create a policy check using the new signature added for a virtual business service. Run it for the selected a virtual business services and see if there are any violations reported. If any violation is reported, the virtual business service may not work properly and it should be fixed.

- You can use the new fault that has been added for the Virtual Business Services. The topic ID is event.alert.vom.vcs. vbs.package.notinstalled, which stands for "VRTSvbs package is not installed". Create a rule that acts on this alert. Choose the notification type that you want. This rule helps in reducing one of the factors that can affect the proper functioning of Virtual Business Services.

It is recommended that you use a combination of all of the above.

## If the Virtual Business Services configuration goes out of synch, how does one correct it?

Run the following command on VOM Management Server:`<sfmh_bin_dir>/xprtlc -l https://localhost:5634/admin/cgi-bin/vbs_configurator.pl -d rescan=all`

For example:

UNIX systems:

```
# /opt/VRTSsfmh/bin/xprtlc -l
https://localhost:5634/admin/cgi-bin/vbs_configurator.pl -d
rescan=cred
```

Windows systems:

```
"C:\Program Files\Veritas\VRTSsfmh\bin\xprtlc.exe" -l
https://localhost:5634/admin/cgi-bin/vbs_configurator.pl -d
rescan=cred
```

### What happens to the Virtual Business Services definitions if Veritas InfoScale Operations Manager Management Server is reinstalled?

All the Virtual Business Services definitions are lost and you have to re-create them. It is recommended that you back up the Veritas InfoScale Operations Manager database before uninstalling Veritas InfoScale Operations Manager, and restore it after reinstall to retain the old Virtual Business Services definitions.

### How is data passed from Veritas InfoScale Operations Manager Management Server to the cluster nodes?

Veritas InfoScale Operations Manager uses XDist to push the data from Management Server to the cluster nodes. XDist has an in-built retry mechanism that sends the data even if the target host is down, and comes back up later.

### Where are the various log files stored for this feature?

The log files can be found at the following locations:

- `<sfmcs_var_dir>/logs/vbs_configurator.log` (on Management Server)
- `<sfmh_var_dir>/logs/` (on managed host)
- `<vbs_var_dir>/log/` (on managed host)

### Which virtualization technologies are supported for starting or stopping virtual machines?

Currently, Veritas InfoScale Operations Manager supports only VMware ESX for starting or stopping virtual machines. For this, Virtual Center/vSphere must be configured in Veritas InfoScale Operations Manager. The virtual machine start and stop operation from the command line is supported only for ApplicationHA or single node VCS clusters.

### What is the port used by the Virtual Business Services daemon?

2410

### How is the Virtual Business Services daemon made HA?

The Virtual Business Services daemon is configured as a resource (vbsapp) in the ClusterService group on all the participating clusters in the virtual business Service.

# Multi-Site Management

### What is the minimum SFHA version required for Multi-Site Management?

The minimum version of Storage Foundation High Availability required for the Multi-Site Management feature is as follows:

For UNIX or Linux: SFHA 6.1 or later

For Windows: SFW 6.0 or later

### How can I make an already configured disk group site consistent which has disks from different enclosures?

When you tag the enclosure and hosts using the Configure Stretch Site wizard, Veritas InfoScale Operations Manager automatically tags the disks and makes the disk group site consistent.

# VCS failover reporting and alerting

### Why are all my failovers not listed in the VCS Failover Duration report?

This can occur for the following reasons:

- All the hosts that are part of the cluster may not be reporting to Management Server.

- Hosts may not be running managed host version 6.1 or later.

- The failover may not be automatic unplanned.

### Why is the alert for the failover not shown on the service group or cluster?

Verify the following:

- Verify if the failover was of the type automatic unplanned.

- Make sure the threshold was set at the service group or cluster level.

- Verify that all nodes of the cluster are reporting to Management Server.

- Go to **Settings > Alert & Rules** on the Management Server console and check if the threshold alert is visible.

# Virtualization

This chapter includes the following topics:

-

-

-

## Virtualization overview

### Can Veritas InfoScale Operations Manager manage Storage Foundation that is running in a VMware virtual machine?

Yes. Veritas InfoScale Operations Manager supports Storage Foundation running in a VMware virtual machine. Since in most cases VMware does not expose the HBA directly to the guests, Veritas InfoScale Operations Manager would not be able to discover the array port of any LUNs nor the HBA ports. However, Veritas InfoScale Operations Manager displays the enclosure information for any raw device mapped LUNs. The virtual disks are plain old SCSI disks since they are abstracted from the guest.

### What do I need to deploy to see end-to-end storage correlation for the supported virtualization technologies?

For VMware:

- Configure VMware vCenter Server in Veritas InfoScale Operations Manager from a control host.

- Configure deep discovery of storage arrays using Storage Insight Add-on.

- Configure guest virtual machines via agent or agentless method.

For LPARs:

- Configure Hardware Management Console (HMC) in Veritas InfoScale Operations Manager from a control host.

- Configure deep discovery of storage arrays using Storage Insight Add-on.

- Configure LPAR guest virtual machines via agent.

- Configure VIO servers via agent (only if they are running Dynamic Multi-Pathing)

For Microsoft Hyper-V:

- Configure Hyper-V server via agent.

- Configure Hyper-V guest virtual machines via agent or agentless method.

For Kernel-based Virtual Machine (KVM):

- Configure KVM server via agent.

- Configure KVM guests via agent.

For Zones:

- Configure global zone via agent.

For LDOMs

- Configure LDOM control domain via agent.

- Configure LDOM guests via agent.

### Can I perform virtualization discovery through VMware vCenter using a non-default port?

The default vCenter port is 443 which is used by Veritas InfoScale Operations Manager for the virtualization discovery. However if VMware vCenter is configured on a non-default port, you can specify the port number after VMware vCenter IP / host name so that Veritas InfoScale Operations Manager will use the same for the discovery. For example, MyvCenter.example.com:65535.

# Near real-time (NRT) update of virtual machine states

### How can I change the default listening port (port 162) for `xtrapd`?

To change the default listening port for `xtrapd`, run the commands as described below:

On Linux Management Server:

- `/opt/VRTSsfmcs/bin/xtrapdctrl stop`

- `/opt/VRTSsfmcs/bin/xtrapdctrl start` *new port no*

---

**Note:** If `xtrapd` is restarted, it will again fall back to the default listening port 162.

---

On Windows Management Server:

On Windows operating system, `xtrapd` runs as a service. To change the listening port in Windows, the `xtrapd` service must be re-registered for the new port.

- `C:\Program Files\Veritas\VRTSsfmcs\bin>vomsc --stop xtrapd`

- `C:\Program Files\Veritas\VRTSsfmcs\bin>xtrapd.exe -unregister`

- `C:\Program Files\Veritas\VRTSsfmcs\bin>xtrapd.exe -register -c "`*Path in* `%ALLUSERSPROFILE%\Symantec\VRTSsfmh\shared\xtrapd\xtrapd.conf" `*new port no*

- `C:\Program Files\Veritas\VRTSsfmcs\bin>vomsc --start xtrapd`

---

**Note:** No SNMP traps will be processed while the ports are being updated.

---

# Veritas HA Plug-in for vSphere Web Client

### What versions of ApplicationHA and Cluster Server (VCS) are supported by Veritas HA Plug-in for vSphere Web Client?

ApplicationHA 5.1 SP2 and later

VCS for VMware 6.0.1, 6.0.2, and 6.1

### If I am using ApplicationHA 5.1SP2 or 6.0, can I monitor and manage my applications with Veritas HA Plug-in for vSphere Web Client?

Yes, But you need to upgrade VRTSfsmh to version 5.0 or later on the guest VMs on which ApplicationHA is installed.

### If I am using VCS for VMware 6.0.1, 6.0.2, or 6.1 can I monitor and manage my applications with Veritas HA Plug-in for vSphere Web Client?

Yes, But you need to upgrade VRTSfsmh to version 6.1 or later on the guest VMs on which VCS for VMware is installed.

## Can I use Veritas HA Plug-in for vSphere Web Client in a Veritas InfoScale Operations Manager HA environment?

There are two scenarios for using Veritas HA Plug-in for vSphere Web Client in a Veritas InfoScale Operations Manager high availability (HA) environment. They depend on whether Veritas InfoScale Operations Manager Management Server is already configured for HA:

■ If Management Server is already configured for HA, you need to install Veritas HA Plug-in for vSphere Web Client on both the primary and secondary nodes. This behavior is similar to other Veritas InfoScale Operations Manager add-ons.

■ If Management Server is not yet configured for HA, do the following steps:
  If Veritas HA Plug-in for vSphere Web Client is already configured on the standalone Management Server, then before configuring Management Server for HA, unregister all the registered vCenters with Symantec High Availability Console in the VMware vSphere Web Client. Then uninstall Veritas HA Plug-in for vSphere Web Client.
  After Management Server is configured for HA, install Veritas HA Plug-in for vSphere Web Client on both the primary and secondary nodes and register the vCenters with Symantec High Availability Console console.

For more information on Veritas HA Plug-in for vSphere Web Client, see the *Veritas InfoScale Operations Manager Add-ons User Guide*.

# SAN Visibility

This chapter includes the following topics:

- SAN visibility overview

## SAN visibility overview

### What components do I need to start discovering switches and fabrics in my data center?

You need to install Fabric Insight Add-on. You need to install the Fabric Insight Add-on first on the Veritas InfoScale Operations Manager Management Server and then on one or more managed hosts from which you want to perform the discovery of Cisco or Brocade fabrics. It is recommended that you perform the fabric discovery from a managed host and not from the Management Server. The version of Veritas InfoScale Operations Manager on the Management Server, or the managed host should be 6.0 to install the Fabric Insight Add-on.

### What do I need to configure for discovering the switches and fabrics?

For Cisco, you need to configure the credentials for one of the switches in the fabric in Veritas InfoScale Operations Manager. For Brocade, you can either configure the credentials for Brocade Network Advisor (BNA) that manages the fabrics, or the credentials of one of the switches in the fabric. For a successful discovery, ensure that all the switches participating in the fabric are using the same credentials.

### Does Veritas InfoScale Operations Manager support the discovery of fabrics containing switches from different vendors?

Veritas InfoScale Operations Manager does not support the discovery of such fabrics. The fabric should contain switches exclusively from either Brocade or Cisco.