Veritas™ Operations Manager Management Server 6.0 Frequently Asked Questions

November 2013

Symantec™

Veritas™ Operations Manager Management Server 6.0 Frequently Asked Questions

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: 6.0

Documentation version: 6.0 Rev 0

Legal Notice

Copyright © 2013 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, Veritas, Veritas Storage Foundation, CommandCentral, NetBackup, Enterprise Vault, and LiveUpdate are trademarks or registered trademarks of Symantec Corporation 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 Symantec Corporation 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. SYMANTEC 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, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations, whether delivered by Symantec 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.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers 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 Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/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.symantec.com/business/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 Symantec
  - Recent software configuration changes and network changes

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec's enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

http://www.symantec.com/connect/storage-management

Documentation

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com

For information regarding the latest HOWTO articles, documentation updates, or to ask a question regarding product documentation, visit the Storage and Clustering Documentation forum on Symantec Connect.

https://www-secure.symantec.com/connect/storage-management/forums/storage-and-clustering-documentation

Contents

Chapter 1

General

This chapter includes the following topics:

Overview

What is Veritas Operations Manager?

Veritas Operations Manager is a comprehensive management platform, for Symantec 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 Operations Manager?

The following documentation resources are available for Veritas Operations Manager:

- Online Help - The online Help for the product is available on the Web or as an add-on that can be installed with the product.
- Guides – The Veritas Operations Manager user documentation is available on https://sort.symantec.com/documents

Does Veritas Operations Manager need anything that is installed on the managed host (MH) to work with Veritas Storage Foundation High availability 5.x?

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

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

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

Does Veritas 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 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 Operations Manager discovers information about.

Family	Frequency in minutes	Discovered information
Host	1440	The operating system, packages, and networking for the host. Typically, most of the information that is related to this family does not change frequently.
SF	30	Volume Manager, File Systems, and the related storage network.
VCS	60	Symantec Cluster Server and the related information.
DB	60	Oracle, DB2, MSSQL, and Sybase databases and their storage dependencies.
LDR	1440	The licenses that are installed on the hosts.

Family	Frequency in minutes	Discovered information
NR	5	Configuration status and external faults.
Native	360	Third-party volume management information.
Zones	120	Oracle Solaris zones and their storage dependencies.
LDoms	120	Oracle Solaris LDoms, and related CPU and memory information.
KVM	120	KVMs, and their correlation with the host.
Hyper-V	120	Virtual machines and storage discovery.
LPAR	360	Hosts, guests, and storage information.
VMware	360	ESX servers, virtual machines, and their storage dependencies. **Note:** This information is discovered only when Control Host Add-on is installed on a managed host that is designated as the control host.
Agentless	360	The following information on the hosts that are configured on the control host for agentless: ■ The IP addresses, operating system, and the usage of the CPU and memory. ■ The host bus adapters (HBAs) on the host. ■ The disks on the hosts and their correlation with the array LUNs and multipathing. ■ The volumes and the volume groups on the native Volume Manager. ■ The mount points of the file systems and the correlation of the file systems with the disks. ■ In a VMware guest environment, the correlation of the ESX server with the virtual machine and the correlation of the storage exported from the ESX server with the storage in the virtual machine **Note:** This information is discovered only when Control Host Add-on is installed on a managed host that is designated as the control host.

Additionally, Symantec Storage Foundation and Symantec Cluster Server 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 Veritas Operations Manager 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. Please refer to the *Veritas Operations Manager Management server User Guide* for more information on Veritas Operations Manager MH discovery.

Does Veritas Operations Manager display localized (i.e. Japanese or Chinese) File System mount points?

Yes. The default encoding Veritas 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 Operations Manager support other non-Symantec Volume Managers and File Systems?

Yes. Veritas Operations Manager discovers Logical Volume Manager (LVM) information on Linux, HP-UX, and AIX managed hosts, as well as ZFS information on Solaris. Veritas 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 Operations Manager Hardware and Software Compatibility List (HSCL)*.

Does Veritas Operations Manager support other non-Symantec Multi-pathing Solutions?

Yes. Besides support for Veritas DMP, Veritas 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 Operations Manager Hardware and Software Compatibility List (HSCL)*.

Does Veritas Operations Manager support other Clustering Solutions?

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

For more information, refer to the *Veritas 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 Operations Manager simultaneously and do not explicitly log off, it could cause out-of-memory errors.

When should I create a Business Application (BA)?

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 Operations Manager and Symantec Storage Foundation High Availability releases

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

Veritas 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

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

Veritas Operations Manager release	VRTSsfmh version	SFHA release that it is bundled with
2.1RP1 (SFM)	2.1.229.0	SFHA Linux 5.0MP4 SFHA UNIX 5.1RP1 SFHA Linux and Solaris 5.1RP2
3.0	3.0.357.0	
	3.0.358.0	SFHA Windows 5.1 SP2 ApplicationHA VMware Linux 5.1 ApplicationHA VMware Windows 5.1SP1
3.0 RP1	3.0.402.0	
3.1	3.1.429.0	SFHA Solaris, AIX 5.1SP1 ApplicationHA VMware Linux 5.1SP2
3.1RP1	3.1.830.0	SFHA HP, Linux 5.1SP1 & 5.1SP1RP1 SFHA AIX, Solaris, Linux 5.1SP1RP2 ApplicationHA VMware Windows 5.1SP2
4.0	4.0.1097.0	
4.0RU1	4.0.1598.0	ApplicationHA VMware 6.0
4.1	4.1.119.0	SFHA AIX, Linux, Solaris 6.0 Windows 6.0 ApplicationHA Unix 6.0
5.0	5.0.196.0	SFHA AIX, Linux, Solaris 6.0
6.0	6.0.0.0	N.A.

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 Operations Manager offer?

Veritas Operations Manager offers reports in five different categories, such as Trend/Activity, Storage Utilization, Inventory, True up, and Exception.

Is Veritas Operations Manager able to create comparisons between reports?

Veritas 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 Operations Manager Web services API to get data and create reports for analysis.

Performance statistics

What performance-related data does Veritas Operations Manager track?

Veritas 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 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 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 Operations Manager version 6.0 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 Operations Manager Management Server User Guide*.

Chapter 2

Infrastructure

This chapter includes the following topics:

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 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 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 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 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 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 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 Operations Manager documentation for more details.

What is xinfo?

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

What is xclusinfo?

xclusinfo interfaces with the Veritas 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 Operations Manager Management Server. These commands are supported on Linux and Windows operating system. For more information on vomadm command, refer to the *Veritas Operations Manager Management Server User Guide*.

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

Yes, using Veritas Operations Manager Web services API, you can access the information. Veritas 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 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 Operations Manager Management Server User's Guide*.

Chapter 3

Settings and configuration

This chapter includes the following topics:

Installation and upgrade

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

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

I am running an older version of Veritas Operations Manager, Storage Foundation Manager, or Veritas Cluster Server Management Console. How can I upgrade to Veritas Operations Manager 6.0?

Upgrade to Veritas Operations Manager 6.0 is only supported from Veritas Operations Manager 4.1, or later versions. Users of Storage Foundation Manager need to upgrade to Veritas Operations Manager 4.1 or later versions, and then upgrade to Veritas Operations Manager 6.0. Users of Symantec Cluster Server Management Console need to start with a fresh installation of Veritas Operations Manager.

How can I upgrade Veritas Operations Manager 5.0 Management Server on Solaris to Veritas Operations Manager 6.0?

Veritas Operations Manager 5.0 is the last major version of Veritas 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 Operations Manager managed host 6.0?

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 6.0 before managing the host using a 6.0 Management Server.

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

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

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

Veritas 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 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 Operations Manager Management Server. Veritas Operations Manager requires a 64-bit operating system for Linux and Windows.

What is Auto Configure and gendeploy.pl?

The Auto Configure option lets you add a managed host to the Veritas 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 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 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 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 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
  ```

- Windows:

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

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

Networking

What protocol is used for Veritas Operations Manager?

Veritas 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 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 Operations Manager?

SNMP trap support is limited in Veritas Operations Manager. Veritas 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 Operations Manager Management Server Installation and Configuration Guide*.

Add-ons

What is a Veritas Operations Manager add-on?

Veritas Operations Manager add-ons allow the extension of the base functionality that is included in Veritas Operations Manager. Refer to http://go.symantec.com/vom 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 Operations Manager Management Server and managed host versions are compatible with an add-on?

For information on Veritas Operations Manager 6.0 add-on compatibility matrix, refer to *Veritas 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 Operations Manager. Veritas 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 Operations Manager allows native OS authentication for end users.

Hot fixes, patches, and packages

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

Veritas Operations Manager integrates with Symantec Operations Readiness Tool (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 Operations Manager to show it.

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

Veritas 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 Operations Manager to show it.

My network does not allow for direct Internet access. Can I still access the Symantec Operational Readiness Tool (SORT) functionality?

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

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

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

Organization and permissions

Can I add secondary authentication broker to Veritas Operations Manager?

No, in Veritas Operations Manager 6.0 you cannot add secondary authentication broker.

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

Veritas 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 Operations Manager supports Lightweight Directory Access Protocol (LDAP) and Active Directory (AD). You can view the following authentication domain types on the Veritas Operations Manager log in page:

- Unixpwd
- Network (NT) Domain
- LDAP
- AD

What are the predefined roles in Veritas Operations Manager?

Veritas 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 Operations Manager?

Veritas 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 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.

Chapter 4

Server

This chapter includes the following topics:

Centralized Storage Foundation administration

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

Table 4-1 Storage Foundation operations

Object	Type of Operation
Disks and disk groups	Creating disk groups
	Recovering disk groups
	Deporting disk groups
	Destroying disk groups
	Importing disk groups
	Adding disks to disk groups
	Resizing disks in disk groups
	Renaming disks in disk groups
	Upgrading disk groups
	Splitting disk groups
	Moving disk groups
	Joining disk groups
	Disconnecting disks
	Initializing disks
	Recovering disks
	Replacing disks
	Removing disks from disk groups
	Bringing disks online
	Taking disks offline
	Evacuating disks
	Setting disk usage
	Running or scheduling Trim
	Rescanning disks

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

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
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 and 6.0
- SFHA on UNIX/Linux: Versions 4.x, 5.x and 6.0

For more information, refer to the *Veritas 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:

- Recovering disk
- Initializing disks
- 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

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
- Monitoring capacity of file systems

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

Mount operation: File systems that are created on Storage Foundation volumes

Unmount operation: Supported for all file systems, except for the root or the ZFS file system.

Chapter 5

Availability

This chapter includes the following topics:

ApplicationHA management

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

- The VRTSsfmh package that is part of Symantec 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 Operations Manager?

ApplicationHA 6.0, and later.

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

Which are the virtualization technologies supported by Veritas Operations Manager?

Following virtualization technologies are supported by Veritas 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 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 Symantec Cluster Server (VCS) support for ApplicationHA from Veritas 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 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 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).

Symantec 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 Operations Manager instance must manage all the GCO clusters.

Can I configure fire drill SG through Veritas Operations Manager?

No. Currently, Veritas 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 Symantec 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-backend 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 Symantec 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 Operations Manager Management Server in the critical path and a single point of failure?

Veritas 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 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 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 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 Operations Manager database before uninstalling Veritas Operations Manager, and restore it after reinstall to retain the old Virtual Business Services definitions.

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

Veritas 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 Start or Stop virtual machine?

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

Chapter 6

Virtualization

This chapter includes the following topics:

Overview

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

Yes. Veritas Operations Manager supports Symantec Storage Foundation running in a VMware virtual machine. Since in most cases VMware does not expose the HBA directly to the guests, Veritas Operations Manager would not be able to discover the array port of any LUNs nor the HBA ports. However, Veritas Operations Manager displays the enclosure information for any raw device mapped LUNs. Non-RDM 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 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 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 Symantec 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 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 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.

Chapter 7

SAN Visibility

This chapter includes the following topics:

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 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 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 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

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

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