

Veritas™ Operations Manager Management Server 6.0 Installation and Configuration Guide

Veritas™ Operations Manager Management Server Installation and Configuration Guide

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

Product version: 6.0

Documentation version: 6.0 Rev 3

Legal Notice

Copyright © 2014 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

Technical Support	4
Section 1 Installing and configuring Veritas Operations Manager	17
Chapter 1 Planning your Veritas Operations Manager installation	18
About Veritas Operations Manager	18
Downloading Veritas Operations Manager 6.0	19
Downloading Management Server files	19
Downloading managed host files	20
Using the product documentation	21
Host considerations for installing Veritas Operations Manager	23
Typical Veritas Operations Manager deployment configuration	23
Centralized management of Symantec Storage Foundation High Availability hosts	24
Veritas Operations Manager 6.0 installation overview	24
Choosing a Management Server host	24
Choosing the managed hosts	25
Chapter 2 System requirements	27
Operating system requirements	27
Third-party required libraries	27
32-bit SNIA Common HBA API required on Windows hosts	27
System resource requirements	28
About space estimation for data logs	29
About the frequency of managed host, enclosure and switch information discovery	32
Supported hardware	34
Web browser requirements	34
Network and firewall requirements	34
Internet Protocol version requirements	36

Chapter 3	Installing, upgrading, and uninstalling Veritas Operations Manager	38
	Packages included in Veritas Operations Manager	39
	About installing Management Server	39
	Installing Management Server on Linux	39
	Installing Management Server on Windows	41
	Verifying Management Server installation on Linux	42
	Verifying Management Server installation on Windows	42
	Configuring Veritas Operations Manager on Linux and Windows	43
	About installing managed host	44
	Installing host management on UNIX/Linux	45
	Installing host management on Windows	46
	About cloning virtual machines	47
	About migrating virtual machines	47
	Installing managed host through Solaris JumpStart	48
	Verifying managed host installation on UNIX	49
	Verifying host management installation on Windows	49
	About upgrading Management Server	50
	About migrating objects and features after upgrade to Veritas Operations Manager 6.0	50
	Upgrading Management Server on Linux	53
	Upgrading Management Server on Windows	55
	About backing up and restoring Veritas Operations Manager data	57
	Taking regular backups of Veritas Operations Manager data on Linux	58
	Backing up Veritas Operations Manager data on Linux before upgrading to version 6.0	59
	Restoring backed up data on Linux	59
	Taking regular backups of Veritas Operations Manager data on Windows	60
	Backing up Veritas Operations Manager data on Windows before upgrading to version 6.0	61
	Restoring backed up data on Windows	62
	About upgrading managed hosts to Veritas Operations Manager 6.0	63
	Upgrading managed hosts using the console	64
	Upgrading host management on UNIX/Linux using operating system commands	65
	Upgrading host management on Windows using the installer package	66
	Verifying the version of Management Server in the console	67
	Verifying the version of a managed host in the console	67

Uninstalling Management Server on Linux	68
Uninstalling Management Server on Windows	68
Uninstalling managed host on UNIX	69
Uninstalling host management on Windows	70
 Chapter 4 Configuring Veritas Operations Manager in a high availability and disaster recovery environment	 71
Configuring Veritas Operations Manager in high availability environment	71
Configuring a new Veritas Operations Manager installation in high availability environment	72
Configuring an existing Veritas Operations Manager installation in high availability environment	78
Configuring Veritas Operations Manager in disaster recovery environment	80
Prerequisites for configuring a Management Server in DR environment	81
Performing initial configuration of Management Server installation in DR environment	83
Creating the base service groups for DR configuration	83
Enabling DR configuration	85
Configuring Veritas Operations Manager in high availability and disaster recovery environment	86
Prerequisites for configuring a Management Server in HA-DR environment	87
Performing initial configuration of Management Server installation in HA-DR environment	88
Creating the base service groups for HA-DR configuration	89
Enabling HA-DR configuration	91
About upgrading the high availability configurations	92
Upgrading Management Server in high availability environment	92
About upgrading the high availability and disaster recovery configurations	93
Upgrading Management Server in high availability and disaster recovery environment	94
Removing the high availability configuration	94

Chapter 5	Installing and uninstalling Veritas Operations Manager add-ons	96
	About deploying Veritas Operations Manager add-ons	97
	Downloading a Veritas Operations Manager add-on	98
	Uploading a Veritas Operations Manager add-on to the repository	99
	Upload Solutions to Repository panel options	99
	Installing a Veritas Operations Manager add-on	100
	Install - Download Add-on panel options	101
	Install - Select hosts panel options for add-ons	101
	Uninstalling a Veritas Operations Manager add-on	102
	Uninstall panel options	103
	Removing a Veritas Operations Manager add-on from the repository	103
	Remove panel options	104
	Canceling deployment request for a Veritas Operations Manager add-on	104
	Cancel Deployment Request panel options	105
	Installing a Veritas Operations Manager add-on on a specific managed host	105
	Install panel options	106
	Uninstalling a Veritas Operations Manager add-on from a specific managed host	107
	Uninstall panel options	107
	Enabling a Veritas Operations Manager add-on on a specific managed host	108
	Disabling a Veritas Operations Manager add-on from a specific managed host	109
	Refreshing the repository	109
	Restarting the web server	110
Section 2	Setting up the Management Server environment	111
Chapter 6	Basic Veritas Operations Manager tasks	112
	About the communication between the managed hosts and Management Server	112
	Connecting to Veritas Operations Manager Management Server	113
	Stopping and starting the Web application	114
	About the Management Server perspective	115

Chapter 7	Adding and managing hosts	116
	Overview of host discovery	116
	How Veritas Operations Manager discovers hosts	116
	Supported features for host discovery options	120
	Overview of agentless discovery	122
	About agentless discovery using the Control Host	123
	About agentless discovery of remote hosts	123
	Prerequisites for agentless configuration	124
	How agentless discovery of a UNIX or Linux host works	124
	How agentless discovery of a Windows host works	125
	Requirements for agentless discovery of UNIX hosts	126
	Requirements for agentless discovery of Windows hosts	128
	Requirements for deep array discovery for agentless hosts	129
	Commands that require the root access for agentless discovery of UNIX hosts	130
	Using the privilege control software with agentless discovery of UNIX hosts	132
	SSH configuration requirements for agentless discovery	133
	About installing OpenSSH on a UNIX host	135
	Adding the managed hosts to Management Server using an agent configuration	138
	Add agent hosts panel options	139
	Adding the managed hosts to Management Server using an agentless configuration	140
	Add agentless hosts panel options	141
	Adding managed hosts to Management Server using the Auto Configure (gendeploy.pl) script	143
	Editing the agentless host configuration	145
	Edit agentless host panel options	146
	Refreshing the details of the managed host	146
	Removing managed hosts from the Management Server domain	147
Chapter 8	Setting up user access	149
	About managing authentication brokers and authentication domains in the Veritas Operations Manager domain	149
	Configuring Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server	151
	Configure LDAP/AD panel options	151
	Configure LDAP/AD panel options to specify the domain name	154
	Unconfiguring Lightweight Directory Access Protocol or Active Directory configuration from the authentication broker	156

About predefined roles in Veritas Operations Manager	156
About Organizations, objects, and roles in Veritas Operations Manager	157
Assigning permissions to user groups for a perspective	158
Modifying permissions assigned to user groups for a perspective	159
Deleting permissions assigned to user groups on a perspective	160
Restricting users or user groups from accessing the Veritas Operations Manager console	160
Example: Managing user access in Veritas Operations Manager using Organizations and existing user groups	161

Chapter 9

Setting up fault monitoring	166
About alerts and rules	166
Creating rules in the Management Server perspective	168
Create Rule - Select the type of fault conditions to trigger this rule panel options	169
Create Rule - Select one or more fault topics which will trigger this rule panel options	170
Create Rule - Setup notifications panel options	170
Create Rule - Enter name and description panel options	172
Editing rules in the Management Server perspective	172
Edit Rule - Select the type of fault condition to trigger this rule panel options	173
Edit Rule - Select one or more fault topics which will trigger this rule panel options	174
Edit Rule - Setup notifications panel options	174
Edit Rule - Enter name and description panel options	176
Deleting rules in the Management Server perspective	176
Delete Rule panel options	177
Enabling rules in the Management Server perspective	177
Enable Rule panel options	178
Disabling rules in the Management Server perspective	178
Disable Rule panel options	179
About faults and risks	179
Suppressing faults in the Management Server perspective	179
Suppress Faults panel options	180
Restoring a suppressed fault in the Management Server perspective	181
Suppressing a fault definition in the Management Server perspective	182
Suppress the fault definition panel options	182

	Restoring a suppressed fault definition in the Management Server perspective	183
Chapter 10	Setting up virtualization environment discovery	185
	About the virtualization technologies supported	186
	About Control Hosts in Veritas Operations Manager	187
	Requirements for discovering vCenter and ESX servers using Veritas Operations Manager	189
	About near real-time (NRT) update of virtual machine states	189
	Setting-up near real-time (NRT) update of virtual machine states	189
	Configuring the VMware vCenter Server to generate SNMP traps	191
	Requirements for discovering the Solaris zones	193
	Requirements for the zlogin utility on non-Global Zones	193
	Requirements for devices exported to non-Global Zones	194
	Requirements for file systems exported to non-Global Zones	194
	Requirements for discovering Solaris Logical domains	194
	Requirements for discovering logical partitions	194
	Requirements for Microsoft Hyper-V virtualization discovery	195
	Requirements for Kernel-based Virtual Machine (KVM) virtualization discovery	196
	Configuring the virtualization discovery	196
	Configure Virtualization Server panel options	197
	Configure Virtualization Server panel options	199
	Editing a virtualization discovery configuration	199
	Edit Configuration panel options	200
	Edit Configuration panel options for method selection	201
	Refreshing a virtualization discovery configuration	202
	Removing a virtualization discovery configuration	202
	Configuring performance metering for a VMware vCenter server	203
	Disable performance metering for a VMware vCenter server	203
Chapter 11	Deploying hot fixes, packages, and patches	205
	About deploying Veritas Operations Manager hot fixes	205
	About deploying maintenance release packages and patches	206
	About deploying base release packages	207
	Downloading a hot fix, package, or patch	207
	Uploading a Veritas Operations Manager hot fix or package to the repository	208
	Installing a Veritas Operations Manager hot fix, package, or patch	209

	Install - Download hot fix, package, or patch panel options	209
	Install - Select hosts panel options	210
	Uninstalling a Veritas Operations Manager hot fix	211
	Removing a hot fix, package, or patch from the repository	212
	Canceling deployment request for a hot fix, package, or patch	213
	Installing a Veritas Operations Manager hot fix on a specific managed host	214
	Uninstalling a Veritas Operations Manager hot fix from a specific managed host	214
Chapter 12	Configuring Management Server settings	216
	Configuring the Management Server settings	216
	Configuring SMTP settings for email notifications	218
	Configuring SNMP trap settings for alert notifications	219
	Configuring the proxy server settings	220
	Enabling the analytics gathering on Management Server	221
	Setting the period for retaining the alert and the task logs in the database	222
	Configuring Web server settings	222
	Setting the generation time for subscribed reports	223
	Configuring advance authorization settings	224
	Enabling or disabling policy signatures for the data center	224
Chapter 13	Setting up extended attributes	226
	About using extended attributes	226
	Adding an extended attribute	227
	Modifying an extended attribute	228
	Deleting an extended attribute	229
Chapter 14	Downloading price tier information from SORT	230
	About assigning price tiers to hosts	230
	About updating the price tier information on Management Server	231
	Updating the price tier information automatically on Management Server	232
	Updating the price tier information manually on Management Server	232

Chapter 15	Viewing information on the Management Server environment	234
	Viewing the details of an add-on, hot fix, package, or patch on SORT website	235
	Viewing the hosts configured in the Management Server domain	235
	Viewing the details of the authentication broker and the domains associated with the broker	236
	Viewing faults in the Management Server perspective	237
	Viewing the faults definitions	237
	Viewing details of alert logs	238
	Viewing the details of rules	239
	Viewing the details of active users logged in to Management Server	240
	Viewing the Management Server settings	240
	Viewing the list of extended attributes	241
	Viewing audit information for Management Server	241
	Viewing task information for the data center	242
	Viewing or exporting a list of available policy signatures	243
Appendix A	Troubleshooting	244
	Management Server (MS)	244
	Veritas Operations Manager processes running on Management Server for Linux	244
	Commands to start and stop the Veritas Operations Manager processes on Management Server on Windows	244
	Commands to start and stop the Veritas Operations Manager processes on Management Server on Linux	245
	Veritas Operations Manager services running on Management Server for Windows	245
	Management Server log file locations (Linux)	245
	Management Server log file locations (Windows)	245
	Management Server database configuration and upgrade logs	245
	Windows Installer log file	245
	Managed host (MH)	246
	Veritas Operations Manager processes running on managed host on Unix/Linux	246
	Commands to start and stop Veritas Operations Manager processes on managed host on UNIX/Linux	246
	Veritas Operations Manager services running on managed host on Windows	246
	Managed host log files	246

Gathering information for troubleshooting 246

Index 248

Installing and configuring Veritas Operations Manager

- [Chapter 1. Planning your Veritas Operations Manager installation](#)
- [Chapter 2. System requirements](#)
- [Chapter 3. Installing, upgrading, and uninstalling Veritas Operations Manager](#)
- [Chapter 4. Configuring Veritas Operations Manager in a high availability and disaster recovery environment](#)
- [Chapter 5. Installing and uninstalling Veritas Operations Manager add-ons](#)

Planning your Veritas Operations Manager installation

This chapter includes the following topics:

- [About Veritas Operations Manager](#)
- [Downloading Veritas Operations Manager 6.0](#)
- [Using the product documentation](#)
- [Host considerations for installing Veritas Operations Manager](#)
- [Typical Veritas Operations Manager deployment configuration](#)
- [Veritas Operations Manager 6.0 installation overview](#)
- [Choosing a Management Server host](#)
- [Choosing the managed hosts](#)

About Veritas Operations Manager

Veritas Operations Manager by Symantec gives you a single, centralized management console for the Symantec Storage Foundation High Availability products. You can use it to monitor, visualize, and manage storage and cluster resources, and generate reports about these components in the Management Server domain. Veritas Operations Manager helps administrators centrally manage diverse data center environments.

You can also use Veritas Operations Manager to visualize and report about the hosts which do not have Symantec Storage Foundation High Availability products installed on them.

In Veritas Operations Manager, you can establish user credentials such that authorized users can access the product to perform sensitive management tasks. Other users can perform only a basic set of operations, or can only view information.

A typical Veritas Operations Manager deployment consists of the following:

- Management Server
- Managed hosts

A Veritas Operations Manager deployment may also discover the following:

- Virtualization environment
- SAN/NAS or Unified storage
- SAN fabrics

Downloading Veritas Operations Manager 6.0

You can download Veritas Operations Manager 6.0 packages from the following URL:

<http://go.symantec.com/vom>

Note: You can download any latest patches available for the release from the Symantec Operations Readiness Tools (SORT) website at <https://sort.symantec.com/patch/matrix>.

See “[Downloading Management Server files](#)” on page 19.

See “[Downloading managed host files](#)” on page 20.

Downloading Management Server files

To install or upgrade Veritas Operations Manager Management Server, you need to download a `.zip` file. The `.zip` file contains the file that you can run to install Management Server.

Veritas Operations Manager 6.0 provides you two options for installing Management Server. You can either install only Management Server or install Management Server along with all the add-ons, except the VOM Help Addon.

The names of the `.zip` file and the installer file for each platform are as follows:

- **Linux:**
 - **Download file name:**
 - **For Management Server -**
`Veritas_Operations_Manager_Management_Server_6.0.0_Linux.zip`
 - **For Management server along with the add-ons-**
`Veritas_Operations_Manager_Management_Server_6.0.0_Linux_Full.zip`
 - **Installer file name:**
 - **For Management Server -**
`Veritas_Operations_Manager_MS_6.0_Linux.bin`
 - **For Management server along with the add-ons-**
`Veritas_Operations_Manager_MS_6.0_Linux_Full.bin`
- **Windows:**
 - **Download file name:**
 - **For Management Server -**
`Veritas_Operations_Manager_Management_Server_6.0.0_Win.zip`
 - **For Management server along with the add-ons-**
`Veritas_Operations_Manager_Management_Server_6.0.0_Win_Full.zip`
 - **Installer file name:**
 - **For Management Server -**
`Veritas_Operations_Manager_MS_6.0_Win.exe`
 - **For Management server along with the add-ons-**
`Veritas_Operations_Manager_MS_6.0_Win_Full.exe`

See [“About installing Management Server”](#) on page 39.

See [“About upgrading Management Server”](#) on page 50.

Downloading managed host files

To install or upgrade host management, you need to download the `Veritas_Operations_Manager_Managed_Host_Bundle_6.0.0.zip` file that contains the packages for all the supported operating systems for managed hosts. You can unzip the file and install the package on the host for its corresponding operating system.

To upgrade a managed host to Veritas Operations Manager 6.0, you can choose to use the Deployment Management feature.

[Table 1-1](#) provides the information on the file that you use to install the managed host for each operating system.

Table 1-1 Managed host installation and upgrade files

Operating system	Installer file name
AIX	VRTSsfmh_6.0.0.0_AIX.bff.Z
HP-UX	■ For HP-UX 11.23 and HP-UX 11.31: VRTSsfmh_6.0.0.0_HP-UX.tar.gz ■ For HP-UX 11.11 with Storage Foundation 3.5: VRTSsfmh_6.0.0.0_HP-UX_osr_B.11.11.tar.gz
Linux on x86 or x64	VRTSsfmh_6.0.0.0_Linux.rpm
Solaris versions before version 11 on SPARC	VRTSsfmh_6.0.0.0_SunOS_arch_sparc.pkg
Solaris 11 on SPARC	VRTSsfmh_6.0.0.0_SunOS_arch_sparc_osr_5.11.p5p
Solaris 10 on x86	VRTSsfmh_6.0.0.0_SunOS_arch_i386.pkg
Solaris 11 on x86	VRTSsfmh_6.0.0.0_SunOS_arch_i386_osr_5.11.p5p
Windows 32-bit	VRTSsfmh_6.0.0.0_Windows_arch_x86.msi
Windows 64-bit	VRTSsfmh_6.0.0.0_Windows_arch_x64.msi

See [“About installing managed host”](#) on page 44.

Using the product documentation

[Table 1-2](#) lists the Veritas Operations Manager guides and [Table 1-3](#) lists the URLs for Veritas Operations Manager documentation:

Table 1-2 Names of Veritas Operations Manager Guides

Title	Description
<i>Veritas Operations Manager Hardware and Software Compatibility List (HSCL)</i>	Provides the list of hardware and software compatibility.
<i>Veritas Operations Manager Release Notes</i>	Provides release information such as new features, fixed issues, known issues, and limitations.
<i>Veritas Operations Manager Management Server Installation and Configuration Guide</i> <i>Veritas Operations Manager Management Server User Guide</i> <i>Veritas Operations Manager Management Server Add-ons User Guide</i>	Provide information about Veritas Operations Manager.
<i>Veritas Operations Manager Management Server Frequently Asked Questions</i>	Provides a list of frequently asked questions about Veritas Operations Manager.
<i>Veritas Operations Manager Management Server Third-Party License Agreements</i>	Provides information about the third-party software that is used in Veritas Operations Manager.

Table 1-3 URLs for Veritas Operations Manager documentation

URL	Description
https://sort.symantec.com/documents	Latest version of the product documentation.
http://www.symantec.com/connect/videos/vom-videos	List of How-to videos.
http://www.symantec.com/docs/TECH210708	Late breaking news that is related to this release.

Veritas Operations Manager help content is provided in two modes – online and offline.

The online mode is hosted on the web and is accessed when you launch the product help. The offline mode is packaged as an add-on for Veritas Operations Manager, for use if web access is not available.

The help content hosted on the web can be updated independently of product release. For the most up-to-date version of the help content, use the online mode.

Host considerations for installing Veritas Operations Manager

Host considerations for installing and configuring Veritas Operations Manager include the following:

- Before you begin the Veritas Operations Manager installation, ensure that you have the following information:
 - Administrator accounts and passwords for all target hosts
 - A diagram of your storage network (suggested for your reference)
- The managed hosts within a Management Server domain must report synchronized universal time clock time (UC/UTC).
- You must have at least one valid support contract for Symantec Storage Foundation High Availability to be entitled to use Veritas Operations Manager.

See [“About installing Management Server”](#) on page 39.

See [“About installing managed host”](#) on page 44.

Typical Veritas Operations Manager deployment configuration

If you implement centralized management, a typical full installation of Veritas Operations Manager consists of a single Management Server, multiple managed hosts, and a Web console. We recommend this deployment because centralized management offers you the flexibility of performing operations on multiple Symantec Storage Foundation High Availability hosts.

Advantages also include the following:

- Aggregated information for reporting
- Performance management across the data center
- Monitoring storage utilization across the data center
- Administration and analysis of all clusters in an enterprise

See [“Downloading Veritas Operations Manager 6.0”](#) on page 19.

Centralized management of Symantec Storage Foundation High Availability hosts

In this deployment scenario, you can centrally manage the Symantec Storage Foundation High Availability hosts. We recommend this deployment because centralized management offers you the flexibility of performing operations on multiple Symantec Storage Foundation High Availability hosts.

Advantages also include the following:

- Aggregated information for reporting
- Performance management across the data center
- Monitoring storage utilization across the data center
- Administration and analysis of all clusters in an enterprise

See [“Typical Veritas Operations Manager deployment configuration”](#) on page 23.

Veritas Operations Manager 6.0 installation overview

Installing Veritas Operations Manager involves the following:

- Reviewing the Veritas Operations Manager architecture and typical deployment configurations
 See [“Typical Veritas Operations Manager deployment configuration”](#) on page 23.
- Verifying that you have met system requirements
 See [“Supported hardware”](#) on page 34.
 See [“Network and firewall requirements”](#) on page 34.
- Installing and configuring the Veritas Operations Manager Management Server
 See [“About installing Management Server”](#) on page 39.
 See [“Configuring Veritas Operations Manager on Linux and Windows”](#) on page 43.
- Installing Veritas Operations Manager host management on the hosts that will be centrally managed
 See [“About installing managed host”](#) on page 44.

Choosing a Management Server host

Management Server is the central piece of the Veritas Operations Manager architecture. Management Server is responsible for displaying and managing the information that is reported from the managed hosts, storage, SAN fabrics and Virtualization environment.

To identify a host that is appropriate as Management Server, use the following criteria:

- The host should meet or exceed recommended system requirements.
See [“32-bit SNIA Common HBA API required on Windows hosts”](#) on page 27.
See [“Network and firewall requirements”](#) on page 34.
- The host should provide data security and space for a growing database as Management Server discovers new managed hosts and monitors network events. Ideally, the host should have RAID-protected storage and the capacity to grow its file systems.
- Clients that connect to Management Server using the Veritas Operations Manager console (Web browser) must be able to access the host.
For more information on choosing a Management Server host, refer to the *Veritas Operations Manager Hardware and Software Compatibility List (HSCL)*.

See [“Choosing the managed hosts”](#) on page 25.

Choosing the managed hosts

A typical Veritas Operations Manager deployment consists of a Management Server and multiple managed hosts. A managed host is a server that is configured either with or without an agent to become a part of the Veritas Operations Manager infrastructure. A managed host may be configured to discover the information about servers, storage, Storage Area Network (SAN), and virtualization infrastructure. Once a managed host is configured, it collects the information and transmits this information to Management Server.

For the managed hosts that do not have Storage Foundation or Symantec Storage Foundation High Availability, the server information can be discovered in two ways:

- By installing an agent on the managed hosts
- By agentless discovery using SSH (for UNIX/Linux hosts) or WMI (for Windows hosts)

Note: Agentless discovery is not supported on the hosts that have any of the Symantec Storage Foundation High Availability products installed on them.

For more information on agent and agentless hosts, see the *Veritas Operations Manager Management Server User Guide*.

Before you install a managed host, make sure that it meets or exceeds the recommended system requirements.

For more information on choosing a Management Server host, refer to the *Veritas Operations Manager Hardware and Software Compatibility List (HSCL)*.

See [“Operating system requirements”](#) on page 27.

See [“Choosing a Management Server host”](#) on page 24.

System requirements

This chapter includes the following topics:

- [Operating system requirements](#)
- [Third-party required libraries](#)
- [System resource requirements](#)
- [Supported hardware](#)
- [Web browser requirements](#)
- [Network and firewall requirements](#)

Operating system requirements

For information on Operating system requirements for Veritas Operations Manager 6.0, refer to the *Veritas Operations Manager Hardware and Software Compatibility List (HSCL)*.

Third-party required libraries

This section lists third-party libraries required to run Veritas Operations Manager:

- [32-bit SNIA Common HBA API required on Windows hosts](#)

32-bit SNIA Common HBA API required on Windows hosts

For proper discovery of Fibre Channel attached devices—including discovery of HBA and its target ports—Veritas Operations Manager requires installation of the 32-bit SNIA Common HBA API on all Windows managed hosts running HBA controllers.

The Common HBA API is typically available as part of your HBA vendor's driver kit, or you can download it from your HBA vendor's site.

Follow these steps to determine if the SNIA Common HBA API is already present on your Windows host.

To verify that the 32-bit SNIA Common HBA API is installed on a Windows host

- 1 Open the registry editor on the managed host using the `regedit` command.
- 2 Check the following location to get the SNIA library information:

```
HKEY_LOCAL_MACHINE\SOFTWARE\SNIA\HBA\hba_model
```

On 64-bit platforms, Veritas Operations Manager requires 32-bit libraries installed as a pre-requisite. For more information, see your HBA vendor documentation.

System resource requirements

The amount of CPU cores, memory, and disk space that Veritas Operations Manager requires are listed in this section. These requirements are in addition to any resources used by other software applications running on the same server.

For Management Server:

Environment Size	CPU cores	Memory	Disk space
Small (up to 300 managed hosts)	4	4GB	5GB
Medium (up to 1500 managed hosts)	8	16GB	20GB
Large (up to 3500 managed hosts)	16	32GB	40GB

- Add 4GB of memory and 5GB disk space if Management Server is used for the deep discovery of enclosures using Storage Insight Add-on.
- Add 4GB of memory and 5GB disk space if Management Server is used for the discovery of virtualization infrastructure.

Additional considerations for system resource requirements for Veritas Operations Manager:

- It is recommended to have a swap space that is at least twice the size of RAM.
- It is recommended to upgrade the managed hosts to the latest version for the best performance of the product.
- The system resource requirements may vary based on the actual environment in which the product is deployed.

For a managed host:

- CPU cores: 1
- Memory: 1GB
- Disk space: 2GB
- Add 4GB of memory and 5GB disk space if being used as discovery host for the deep discovery of enclosures using Storage Insight Add-on.

For Control Host (host that has Control Host Add-on):

- CPU: Dual processor for agentless discovery of every 1000 managed hosts.
- Memory: 4GB for agentless discovery of every 1000 managed hosts. Add 4GB of memory if Control Host is used for the discovery of virtualization infrastructure.
- Disk space: 15GB of disk space for agentless discovery of every 1000 managed hosts.

Note: If any of the above is running on a virtual environment, it is recommended to have resources such as CPU cores and memory dedicated to the virtual machine for the best performance of the product.

Read the Late Breaking News tech note for the latest information on updates, patches, and software issues regarding this release.

About space estimation for data logs

In Veritas Operations Manager, historical performance data of various resources is collected in a fixed-size binary file. The older data is overwritten as new data arrives in a circular round robin array. The number of metrics, frequency of data insertion, number of objects, and the roll-up databases affect the size of binary file. The higher resolution data is compressed to a lower resolution data.

For more information on performance metering statistics, see the *Veritas Operations Manager Management Server User Guide*.

[Table 2-1](#) describes the space estimation for data logs for the various resources. For estimation purposes, the data in the Number of resources column is according to the standard environment. The metrics collected column represents the number of metrics collected for each resource. For example, in case of DMP paths, the total number of metrics collected is four: bytes read, bytes written, read average, and write average.

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.

Note: If Veritas Operations Manager is configured in high availability environment, storage array port, adapter, and enclosure logs are saved on a shared disk. VMware ESX server and virtual machines logs are also saved on a shared disk.

[Table 2-2](#) lists the space estimation for data logs for host, file system, volume, and disk on Windows platform.

Table 2-1 Space estimation for data logs

Name of resource	Number of resources	Number of metrics collected	Interval of collection	Duration of collection	Size in KB	Size in KB for a single object
Host, VMware ESX server, and Virtual Machine	1	5	5 minutes	1 day	24	24
	1	5	2 hours	1 month	29	29
	1	5	1 day	1 year	30	30
Multipathing paths	1000	4	5 minutes	1 day	18967	19
	1000	4	2 hours	1 month	23477	24
Initiator	4	9	5 minutes	1 day	171	43
	4	18	2 hours	1 month	423	106
	4	18	1 day	1 year	428	107
Enclosure	4	4	5 minutes	1 day	76	19
	4	8	2 hours	1 month	8	2
	4	8	1 day	1 year	190	46
File system	100	3	5 minutes	1 day	1423	14
	100	3	1 day	1 year	1784	18

Table 2-1 Space estimation for data logs (*continued*)

Name of resource	Number of resources	Number of metrics collected	Interval of collection	Duration of collection	Size in KB	Size in KB for a single object
Volume	100	4	1 minute	6 hours	2348	23
	100	4	5 minutes	1 day	1898	19
	100	4	2 hours	1 month	2348	23
	100	4	1 day	1 year	2379	24
Disk	100	4	1 minute	6 hours	2348	23
	100	4	5 minutes	1 day	1898	19
	100	4	2 hours	1 month	2347	23
	100	4	1 day	1 year	2379	23
Storage array - Array port	32	2	30 minutes	1 day	304	9
	32	4	2 hours	1 month	751	23
	32	4	1 day	1 year	761	24
Storage array - Adapter	8	2	30 minutes	1 day	76	9
	8	4	2 hours	1 month	188	23
	8	4	1 day	1 year	190	24
Storage array -Enclosure	1	1	30 minutes	1 day	5	5
	1	2	2 hours	1 month	12	12
	1	2	1 day	1 year	12	12

Table 2-2 Space estimation for data logs for Windows hosts

Name of resource	Number of resources	Metrics collected	Interval of collection	Duration of collection	Size in KB	Size in KB for a single object
Host	1	5	5 mins	1 day	24	24
	1	5	2 hours	1 month	29	29
	1	5	1 day	1 year	30	30
File system	100	4	5 minutes	1 day	1898	19
	100	4	2 hours	1 month	2348	23
	100	4	1 day	1 year	2379	24
Volume	100	4	5 minutes	1 day	1898	19
	100	4	2 hours	1 month	2348	23
	100	4	1 day	1 year	2379	24
Disk	100	4	5 minutes	1 day	1898	19
	100	4	2 hours	1 month	2347	23
	100	4	1 day	1 year	2379	23

About the frequency of managed host, enclosure and switch information discovery

The following table describes the frequency of the managed host information updates in the Management Server database. The discovery on each managed host is divided into families to focus on a particular functional area:

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.

Family	Frequency in minutes	Discovered information
DB	360	Oracle, DB2, MSSQL, and Sybase databases and their storage dependencies.
LDR	1440	The licenses that are installed on the hosts.
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 guest with the virtual machine and the correlation of the storage in the guest with the storage exported from the ESX server. Note: This information is discovered only when Control Host Add-on is installed on a managed host that is designated as the control host.

Family	Frequency in minutes	Discovered information
Enclosures	360	Logical devices, physical devices, host associations, replications, and other enclosure-specific properties. It is enabled through Storage Insight Add-on.
Switches	360	Switches, switch ports, zone, zone members and other vendor-specific properties. It is enabled through Fabric Insight Add-on.

Note: The discovery for the Storage Foundation and Symantec Cluster Server families is event driven and scheduled. This means that the discovery is triggered when configuration changes occur on the managed hosts. As a result, this information is updated in the Veritas Operations Manager database in the following update. If configuration changes are not detected on the managed hosts, the communication between the managed host and Management Server is restricted to the heartbeat communication that occurs every five minutes. You can connect a managed host to multiple Management Servers. The performance of a managed host is not affected in this scenario because the discovery happens only once. Reporting of the state as per the host configuration is done based on the number of Management Servers to which the managed host reports.

Supported hardware

For information on supported hardware for Veritas Operations Manager 6.0, refer to the *Veritas Operations Manager Hardware and Software Compatibility List (HSCL)*.

Web browser requirements

For information on Web browser requirements for Veritas Operations Manager 6.0, refer to the *Veritas Operations Manager Hardware and Software Compatibility List (HSCL)*.

Network and firewall requirements

If you plan to manage hosts within multiple domains, update the network settings to resolve the host from all domains.

You need to ensure that the *localhost* can be resolved from the host.

If *localhost* cannot be resolved from the host, update your network settings to enable it.

For Veritas Operations Manager Management Server in High Availability, you need to configure firewall settings for both the virtual and the physical IP of all cluster nodes.

Veritas Operations Manager uses the default ports as shown in [Table 2-3](#) to transfer information.

Table 2-3 Default ports in a Veritas Operations Manager installation

Port	Protocol	Initiator	Purpose	Effect if blocked
5634	TCP	Management Server	Management Server configuration	Management Server cannot be configured.
5634	TCP		Management Server communications with the managed hosts	Managed host cannot be added to the Management Server domain.
5634	TCP	managed hosts	Managed host to send heartbeats; also used to upload the data from the managed host to Management Server Note: It is recommended that you keep port 5634 open between managed hosts for scalability and performance optimization.	Managed host cannot be added to the Management Server domain.
14161	TCP	Web browser	Run the Management Server console	Users cannot access the Management Server console.

Table 2-3 Default ports in a Veritas Operations Manager installation
(continued)

Port	Protocol	Initiator	Purpose	Effect if blocked
162	UDP	Vmware VCenter server	Receive SNMP traps	Management Server cannot receive Virtual Machine state change SNMP traps from VMWare VCenter. Changes to vmware infrastructure can not be discovered near real time (NRT).
21	FTP	Management Server	Management Server connectivity with SORT	Management Server can not download patches from SORT.
80	HTTP	Management Server	Management Server connectivity with SORT	Management Server can not download patches from SORT.
443	HTTPS	Management Server	Management Server connectivity with SORT	Management Server can not download patches from SORT.

Internet Protocol version requirements

Various components of Veritas Operations Manager are supported on IPV6, IPV4, or mixed mode.

[Table 2-4](#) describes the Veritas Operations Manager support for IPV4 and IPV6:

Table 2-4 IPV4 and IPV6 support

Components	IPV6	IPV4	Mixed Mode ((IPv4 and IPv6))
Management Server	Not supported	Supported	Supported Note: For Management Server that runs in the mixed mode, use only the IPV4 address during the Management Server configuration.
Managed Host	Supported	Supported	Supported
Control Host	Supported	Supported	Supported

See [“Network and firewall requirements”](#) on page 34.

Installing, upgrading, and uninstalling Veritas Operations Manager

This chapter includes the following topics:

- [Packages included in Veritas Operations Manager](#)
- [About installing Management Server](#)
- [Verifying Management Server installation on Linux](#)
- [Verifying Management Server installation on Windows](#)
- [Configuring Veritas Operations Manager on Linux and Windows](#)
- [About installing managed host](#)
- [Installing managed host through Solaris JumpStart](#)
- [Verifying managed host installation on UNIX](#)
- [Verifying host management installation on Windows](#)
- [About upgrading Management Server](#)
- [About backing up and restoring Veritas Operations Manager data](#)
- [About upgrading managed hosts to Veritas Operations Manager 6.0](#)
- [Verifying the version of Management Server in the console](#)
- [Verifying the version of a managed host in the console](#)
- [Uninstalling Management Server on Linux](#)

- [Uninstalling Management Server on Windows](#)
- [Uninstalling managed host on UNIX](#)
- [Uninstalling host management on Windows](#)

Packages included in Veritas Operations Manager

[Table 3-1](#) lists the software packages that are included in Veritas Operations Manager.

Table 3-1 Software packages

Package name	Description
VRTSsfmcs	Veritas Operations Manager package that is required on Management Server.
VRTSsfmh	Veritas Operations Manager package that is required on the managed host. VRTSsfmh package is also installed on Management Server as part of the Management Server installation.

See [“Downloading Veritas Operations Manager 6.0”](#) on page 19.

About installing Management Server

You can install Management Server on any one of the following hosts:

- A Linux host
- A Windows host

After you install Management Server, you have to configure Veritas Operations Manager before you can use it.

See [“Installing Management Server on Linux”](#) on page 39.

See [“Installing Management Server on Windows”](#) on page 41.

See [“Verifying Management Server installation on Windows”](#) on page 42 on page 42.

Installing Management Server on Linux

You can install the Veritas Operations Manager Management Server on a Linux host using one of the following files:

- For Management server:

```
Veritas_Operations_Manager_MS_6.0_Linux.bin
```

- For Management server along with the add-ons:

```
Veritas_Operations_Manager_MS_6.0_Linux_Full.bin
```

The `.bin` file installs the `VRTSsfmcs` and the `VRTSsfmh` packages on the target host.

To install Veritas Operations Manager Management Server on Linux

- 1 Make sure that the host where you plan to install Management Server meets or exceeds system and operating system requirements.

See [“Choosing a Management Server host”](#) on page 24.

- 2 Download and unzip the installation file.

See [“Downloading Management Server files”](#) on page 19.

- 3 Open an operating system console.

- 4 On the host where you plan to install Management Server, log on as root.

- 5 Change directory to the location where you unzipped the `.bin` file.

- 6 At the command prompt, enter one of the following:

- `./Veritas_Operations_Manager_MS_6.0_Linux.bin`

- `./Veritas_Operations_Manager_MS_6.0_Linux_Full.bin`

If you see the error `Permission Denied`, change the permissions for the `.bin` file. To change the permission, run the appropriate command:

- `chmod +x Veritas_Operations_Manager_MS_6.0_Linux.bin`

- `chmod +x Veritas_Operations_Manager_MS_6.0_Linux_Full.bin`

- 7 To accept the End User License Agreement and proceed with installation, type `y`.

The installation is complete when you see messages similar to the following:

```
Installation is complete. You will need to configure Veritas  
Operations Manager Management Server.
```

Please open your browser and type the following URL to configure:

```
https://myhost.example.com:5634/
```

Please skip this step if you intend to use this host as a standby node for Veritas Operations Manager Management Server HA.

- 8 Verify that the packages are installed and the processes are started.
See [“Verifying Management Server installation on Linux”](#) on page 42.
- 9 Configure Veritas Operations Manager.
See [“Configuring Veritas Operations Manager on Linux and Windows”](#) on page 43.

Installing Management Server on Windows

You can install the Veritas Operations Manager Management Server on a Windows host using one of the following files:

- For Management server: `Veritas_Operations_Manager_MS_6.0_Win.exe`
- For Management server along with the add-ons:
`Veritas_Operations_Manager_MS_6.0_Win_Full.exe`

To install Veritas Operations Manager Management Server on Windows

- 1 Make sure that the host where you plan to install Management Server meets or exceeds system and operating system requirements.
See [“Choosing a Management Server host”](#) on page 24.
- 2 On the host where you plan to install Management Server, log on as a user with administrator privileges.
- 3 Download and unzip the installation file.
See [“Downloading Veritas Operations Manager 6.0”](#) on page 19.
- 4 Turn off the Windows firewall, or, open ports 5634 and 14161 for TCP/IP communication.
- 5 Ensure that there is no pending restart from Windows Update. If there is, restart the host before launching the installer.
- 6 To launch the installer, run the `Veritas_Operations_Manager_MS_6.0_Win.exe` or `Veritas_Operations_Manager_MS_6.0_Win_Full.exe` file.
- 7 To proceed with the Management Server installation, accept the End User License Agreement.
- 8 Click **Next** and follow through the installation process.
- 9 After the installation is complete, select **Launch Veritas Operations Manager configuration** to configure Veritas Operations Manager.
You can choose to configure Veritas Operations Manager later using the **`https://hostname:5634/`** URL.
- 10 Click **Finish**.

- 11 Configure Veritas Operations Manager.
See [“Configuring Veritas Operations Manager on Linux and Windows”](#) on page 43.
- 12 Verify that Management Server is installed and the required services are started.
See [“Verifying Management Server installation on Windows”](#) on page 42.

Verifying Management Server installation on Linux

You can verify the Management Server installation by making sure that the packages are installed and the required processes are started.

To verify Management Server installation on Linux

- 1 On the host where you installed Management Server, check whether the `VRTSsfmcs` package is installed. Run the following command:

```
rpm -q VRTSsfmcs
```
- 2 Check whether the `VRTSsfmh` package is installed. Run the following command:

```
rpm -q VRTSsfmh
```
- 3 Check whether the `xprtld` process is started. Run the following command:

```
ps -ef | grep xprtld
```

Verifying Management Server installation on Windows

You can verify the Management Server installation by making sure that the **Veritas Operations Manager for Windows** program is installed, and the Veritas Storage Foundation Messaging Service is started.

To verify Management Server installation on Windows

- 1 On the host where you installed host management, on the Windows Control Panel, click **Add or Remove Programs**.
- 2 Check whether **Veritas Operations Manager for Windows** appears in the list of installed programs.
- 3 On the Windows Services panel, check whether the **Veritas Storage Foundation Messaging Service** has started.

See [“Verifying the version of Management Server in the console”](#) on page 67.

See [“Verifying Management Server installation on Windows”](#) on page 42 on page 42.

Configuring Veritas Operations Manager on Linux and Windows

After you successfully install Management Server, a message is displayed with the URL that you can use to configure Veritas Operations Manager. On Windows, if you chose to launch the configuration, the Web browser is automatically launched with the URL.

For Internet Explorer 7.0, or later, on Windows Server 2008, or Firefox 3.0, or later, if the webpage does not get displayed, you have to set up the Web browser.

Note: You may configure the networking on Management Server in either the IPv4 mode, or in the mixed mode (IPv4 and IPv6). For Management Server that runs in the mixed mode, use only the IPv4 address during the installation and configuration process and not the IPv6 address.

For Management Server configuration with IPv6 address, the localhost, 127.0.0.1, ::1 should be bound to a network interface that is up and running. For example, lo0 on Linux.

To configure Veritas Operations Manager on Linux and Windows

- 1 Launch the Web browser. On Windows, if you chose to launch the configuration after installation, the Web browser is automatically launched.
 - On a host that has a network connection to the Management Server host, open a Web browser.
 - Launch the following URL:
https://hostname:5634/
Where, *hostname* is the Management Server's host name or fully-qualified host name. For a IPv4 configuration, you can alternatively specify the IP address instead of the host name.
For the dual-mode configuration of Management Server, the IPv6 address and the host name entries of the managed hosts should be present in the `/etc/hosts` file on Management Server. Also, all the managed hosts should have an entry of the IPv6 address and the host name of Management Server in their respective `/etc/hosts` file.
- 2 In the **Authentication Required** dialog, enter Management Server host's root or administrator user name and password.
- 3 In the **Server Setting** panel, check and modify the **Server Name**, if required.
- 4 Check and modify the **Server Address**, if required.

- 5 In the **Database Setting** panel, you can accept the default location or specify your own location. To modify the default location, clear **Use Default** and specify another location. On Windows, if you modify the default, you must have **Full control** permission on the drive that you specify.

The default database directory is `/var/opt/VRTSsfmcs/db` on Linux and `%ALLUSERSPROFILE%\Symantec\VRTSsfmcs\db` on Windows.

- 6 Click **Next**.
- 7 In the **Analytics Setting** panel, select **Enable Analytics Gathering** to allow Symantec to gather data on your Veritas Operations Manager usage.
- 8 Do one of the following:
 - To change settings, click **Back**,
 - To start the configuration, click **Finish**.

At the end of the Veritas Operations Manager configuration, messages similar to the following are displayed:

```
Configuration successful.
```

```
Click the Launch Web Console button to login.
```

- 9 Click **Launch Web Console** to log on to Veritas Operations Manager on the configured Management Server host.

See [“Installing Management Server on Linux”](#) on page 39.

See [“Installing Management Server on Windows”](#) on page 41.

See [“Verifying Management Server installation on Windows”](#) on page 42.

About installing managed host

You must install the `VRTSsfmh` package on a host so you can manage it using Veritas Operations Manager Management Server. By default, a compatible version of `VRTSsfmh` package is packaged with Symantec Storage Foundation High Availability 5.1, or later versions. It is recommended that you upgrade the `VRTSsfmh` package to the same version as the Management Server. Some of the new features added in Veritas Operations Manager may not be available with older versions of `VRTSsfmh` package.

After you install the `VRTSsfmh` package on the host, you need to add the host to the Management Server domain. You can add the host using the Management Server console, or the `gendeploy.pl` script.

For more information on adding hosts to a Management Server domain, see the *Veritas Operations Manager Management Server User Guide*.

See [“Adding the managed hosts to Management Server using an agent configuration”](#) on page 138.

See [“Adding the managed hosts to Management Server using an agentless configuration”](#) on page 140.

See [“Adding managed hosts to Management Server using the Auto Configure \(gendeploy.pl\) script”](#) on page 143.

See [“Operating system requirements”](#) on page 27.

See [“Choosing the managed hosts”](#) on page 25.

See [“About cloning virtual machines”](#) on page 47.

See [“About migrating virtual machines”](#) on page 47.

Installing host management on UNIX/Linux

You can install Veritas Operations Manager host management on a UNIX/Linux host by installing the `VRTSsfmh` package on it.

Note: By default, the `VRTSsfmh` package is installed in the `/opt` directory. You cannot specify a different location to install the package.

To install Veritas Operations Manager host management on a UNIX/Linux host

- 1 Make sure that the host where you plan to install host management meets or exceeds system and operating system requirements.
See [“Operating system requirements”](#) on page 27.
- 2 Download the managed host installation files bundle, and unzip it.
See [“Downloading managed host files”](#) on page 20.
- 3 Open an operating system console.
- 4 On the host where you plan to install host management, log on as root.
- 5 Change directory to the location where you unzipped the installation files bundle.
On AIX or HP-UX hosts, decompress the downloaded file.
- 6 At the command prompt, enter one of the following commands to install the package:
 - For AIX, enter the following:

```
installp -ac -d VRTSsfmh_6.0.0.0_AIX.bff VRTSsfmh
```
 - For HP-UX, enter the following:

```
swinstall -s $PWD VRTSsfmh
```

- For Linux on x86 or Xeon, enter the following:
`rpm -ivh VRTSsfmh_6.0.0.0_Linux.rpm`
 - For Solaris versions before version 11 on SPARC, enter the following:
`pkgadd -d VRTSsfmh_6.0.0.0_SunOS_arch_sparc.pkg`
 - For Solaris 10 on x86, enter the following:
`pkgadd -d VRTSsfmh_6.0.0.0_SunOS_arch_i386.pkg`
 - For Solaris 11 on SPARC, enter the following:
`pkg install --accept -g
VRTSsfmh_6.0.0.0_SunOS_arch_sparc_osr_5.11.p5p VRTSsfmh`
 - For Solaris 11 on x86, enter the following:
`pkg install --accept -g
VRTSsfmh_6.0.0.0_SunOS_arch_i386_osr_5.11.p5p VRTSsfmh`
- 7 Verify that the `VRTSsfmh` package is installed and the required processes have started.
- See [“Verifying managed host installation on UNIX”](#) on page 49.
- See [“About installing managed host”](#) on page 44.

Installing host management on Windows

You can install Veritas Operations Manager host management on a Windows host by running a `.msi` file on it.

To install Veritas Operations Manager host management on a Windows host

- 1 Log on to the target host as a user with administrator privileges.
- 2 Make sure that the host where you plan to install host management meets or exceeds system and operating system requirements.

See [“Operating system requirements”](#) on page 27.
See [“Choosing the managed hosts”](#) on page 25.
- 3 Download the managed host installation files bundle, and unzip it.

See [“Downloading managed host files”](#) on page 20.
- 4 From the directory to which you unzipped the installation files bundle, do one of the following:
 - On a 32-bit host, run `VRTSsfmh_6.0.0.0_Windows_arch_x86.msi`
 - On a 64-bit host, run `VRTSsfmh_6.0.0.0_Windows_arch_x64.msi`
- 5 On the Welcome screen of the InstallShield Wizard, click **Next**.

- 6 On the Ready to Install the Program screen, click **Install** to start the installation.
- 7 Click **Finish** to exit the InstallShield Wizard.
- 8 Verify that the host management program is installed and the required service has started.

See [“Verifying host management installation on Windows”](#) on page 49.

See [“About installing managed host”](#) on page 44.

About cloning virtual machines

`VRTSsfmh` package generates a globally unique identifier for the host using parameters such as host id and MAC address of the host. Veritas Operations Manager Management Server identifies a managed host using this identifier.

Some virtualization technologies such as VMware create a new BIOS UUID for a Virtual Machine when it is cloned. The Veritas Operations Manager Agent (`VRTSsfmh` package) uses this UUID to know if the host has been cloned.

On other virtualization technologies, you need to reset the host id of the clone is reset. If host id is not reset, both the clone and the cloned hosts are recognized as the same, which can cause data corruption in the Veritas Operations Manager database. After you reset the host id of the clone, Veritas Operations Manager removes any managed host-related configuration from the clone that gets copied over from the cloned host. The clone is treated as a new host and has to be added as a managed host to the Management Server domain.

See [“About installing managed host”](#) on page 44.

About migrating virtual machines

When the `VRTSsfmh` package is installed on a host, it generates a globally unique identifier for the host. Veritas Operations Manager Management Server identifies a managed host using this identifier. Veritas Operations Manager generates this unique identifier using parameters such as host id and Media Access Control (MAC) address of the host.

Veritas Operations Manager tries to maintain the same identifier for the host in case the host is migrated.

On some virtualization technologies such as LPAR or LDOM, the MAC address of the host changes when it is migrated. You need to ensure that Veritas Operations Manager uses the same identifier for a managed host even when it is migrated. For this purpose, you need to ensure that the host id of the virtual machine does not change after migration. In most of the virtualization technologies, host id of the virtual machine remains the same after migration.

Exception to this is LDOM, where, if host id is not explicitly set for an LDOM guest (using the command `ldm set-domain`), then the host id changes after migration of the Virtual Machine. It causes VRTSsfmh package to regenerate the unique host identifier and the current configuration of the managed host is lost. In such cases, the managed host can no longer actively report data to the Veritas Operations Manager Management Server.

See [“About installing managed host”](#) on page 44.

Installing managed host through Solaris JumpStart

You can add the managed host to the domain through Solaris JumpStart installation without any user interaction. You can use the `gendeploy.pl` script to create a script that adds the host to the Management Server domain. You can also download the script from the Management Server console under **Settings > Host** and click **AutoConfigure**. The script that is generated by `gendeploy.pl` can be included in the final stages of the Solaris JumpStart installation process.

The following are the highlights of installing Veritas Operations Manager managed host as a part of the Solaris JumpStart installation:

- A script which will install `SRTSsfmh` pkg needs to be included at the time of installing operating system using jumpstart.
- Use the `gendeploy.pl` script to create a script that adds the host to the Management Server domain.
- In the finalized stages of the Solaris JumpStart installation, run the script that is created through `gendeploy.pl`.

To create the script to be used for adding the hosts in Solaris JumpStart installation

- 1 Log on as root on Management Server.
- 2 Run `gendeploy.pl` to create the script file:

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

where, *scriptfilename* is the name of the script file that has to be copied to the managed host, and then run to add the host to the Management Server domain.

See [“Adding the managed hosts to Management Server using an agent configuration”](#) on page 138.

See [“Adding the managed hosts to Management Server using an agentless configuration”](#) on page 140.

See [“Adding managed hosts to Management Server using the Auto Configure \(gendeploy.pl\) script”](#) on page 143.

Verifying managed host installation on UNIX

You can verify host management installation on UNIX by making sure that the `VRTSsfmh` package is installed, and the required processes have started.

To verify the managed host installation on UNIX

- ◆ On the host where you installed managed host package, enter one of the following at the command prompt to verify that the package is installed:
 - On AIX, enter the following:
`lsllpp -l VRTSsfmh`
 - On HP-UX, enter the following:
`swlist VRTSsfmh`
 - On Linux, enter the following:
`rpm -q VRTSsfmh`
 - On Solaris, enter the following:
`pkginfo -l VRTSsfmh`

See [“Verifying the version of a managed host in the console”](#) on page 67.

See [“Installing host management on UNIX/Linux”](#) on page 45.

Verifying host management installation on Windows

You can verify host management installation on Windows by making sure that the Veritas Operations Manager (Host Component) program is installed, and the Storage Foundation Messaging Service is started.

To verify host management installation on Windows

- 1 On the host where you installed host management, launch the Windows Control Panel, and click **Add or Remove Programs**.
- 2 Check whether **Veritas Operations Manager (Host Component)** appears in the list of installed programs.
- 3 On the Windows Services panel, check whether the **Veritas Storage Foundation Messaging Service** has started.

See [“Verifying the version of a managed host in the console”](#) on page 67.

See [“Installing host management on Windows”](#) on page 46.

About upgrading Management Server

To upgrade your existing Management Server installation to Veritas Operations Manager 6.0, you have to download and install the required packages. You can upgrade to Veritas Operations Manager 6.0 from version 4.1, or from version 5.0.

Note: To upgrade to Veritas Operations Manager 6.0 from versions before 4.1, you first need to upgrade to version 4.1, or version 5.0. Then, you can upgrade to version 6.0.

You can upgrade Management Server on Linux and Windows hosts.

Veritas Operations Manager 6.0 does not support Solaris as a platform for Management Server. Before you upgrade your Management Server on Solaris to 6.0, do one of the following:

- For Solaris Management Server 5.0, you need to migrate 5.0 Management Server to Linux or Windows.
- For Solaris Management Server versions before 5.0, you need to first upgrade to Solaris Management Server 5.0 and then migrate to Linux or Windows Management Server 5.0.

For more information on migrating Management Server, see *Veritas Operations Manager Management Server Migration Add-on 5.0 User Guide*.

After migrating a 5.0 Management Server to Linux or Windows, you can upgrade the Management server to 6.0.

See [“Downloading Veritas Operations Manager 6.0”](#) on page 19.

See [“Upgrading Management Server on Linux”](#) on page 53.

See [“Upgrading Management Server on Windows”](#) on page 55.

See [“Backing up Veritas Operations Manager data on Linux before upgrading to version 6.0”](#) on page 59.

See [“Backing up Veritas Operations Manager data on Windows before upgrading to version 6.0”](#) on page 61.

About migrating objects and features after upgrade to Veritas Operations Manager 6.0

After you upgrade your Veritas Operations Manager Management Server installation to 6.0, the objects and features from previous version are moved to the appropriate perspectives in Veritas Operations Manager 6.0. Some of the objects and features are not migrated to 6.0 after the upgrade.

[Table 3-2](#) lists the objects and features that are not migrated to 6.0.

[Table 3-3](#) lists the objects and features that are migrated to 6.0 with their corresponding perspectives.

Table 3-2 Objects and features that are not migrated

Objects and features in Veritas Operations Manager 4.1 or 5.0	Behavior in Veritas Operations Manager 6.0
Organization Entities	Organization Entities are not migrated after upgrade to 6.0. In Veritas Operations Manager 6.0, you can regroup the objects by creating Organizations in various perspectives. For more information on creating Organizations, refer to the <i>Veritas Operations Manager Management Server User Guide</i>.
Composite Business Entities	Composite Business Entities are not supported in 6.0. These are not migrated after upgrade to Veritas Operations Manager 6.0.
Composite Virtual Business Services	Composite Virtual Business Services are not supported in 6.0. These are not migrated after upgrade to Veritas Operations Manager 6.0.
Security groups that are configured on Organization Entities and Virtual Business Services (VBS)	Security groups that are configured on Organization Entities and VBS, are not migrated after upgrade to Veritas Operations Manager 6.0. In Veritas Operations Manager 6.0, you can implement rule based access control by assigning roles to user groups. There is no longer a concept of security group. See “About predefined roles in Veritas Operations Manager” on page 156.
Scheduled reports	Scheduled reports are not migrated after upgrade to Veritas Operations Manager 6.0.
Archived reports	Archived reports are not supported in Veritas Operations Manager 6.0. These are not migrated after upgrade to Veritas Operations Manager 6.0.

Table 3-2 Objects and features that are not migrated (*continued*)

Objects and features in Veritas Operations Manager 4.1 or 5.0	Behavior in Veritas Operations Manager 6.0
Rules	Rules are not migrated after upgrade to Veritas Operations Manager 6.0.
Policy templates	Policy templates are not migrated after upgrade to Veritas Operations Manager 6.0.
Activity logs	Activity logs are not migrated after upgrade to Veritas Operations Manager 6.0.
Search queries	Search queries are not migrated after upgrade to Veritas Operations Manager 6.0.
Tasks	Tasks are not migrated after upgrade to Veritas Operations Manager 6.0.
Volume migration tasks	Volume migration tasks are not migrated after upgrade to Veritas Operations Manager 6.0 and Storage Provisioning and Enclosure Migration Add-on 6.0.
File system extended attributes	File system extended attributes are not supported in Veritas Operations Manager 6.0. These are not migrated after upgrade to Veritas Operations Manager 6.0.
Dynamic Multipathing (DMP) cases	The DMP cases that are created in Veritas Operations Manager 5.0 are not migrated to Veritas Operations Manager 6.0 after upgrade. It is recommended that you complete all DMP cases before the upgrade.

Table 3-3 Objects and features that are migrated

Objects and features in Veritas Operations Manager 4.1 or 5.0	Behavior in Veritas Operations Manager 6.0
Domain Admin security groups	Admin role in all the perspectives.
Guest security groups	Guest role in all the perspectives except Management Server perspective.
Domain Operator security groups	Operator role in Availability perspective and Guest role in all the other perspectives, except the Management Server perspective.

Table 3-3 Objects and features that are migrated (*continued*)

Objects and features in Veritas Operations Manager 4.1 or 5.0	Behavior in Veritas Operations Manager 6.0
Virtual Business Services (VBS) without fault management	Appear under Business Applications in Server perspective.
Virtual Business Services (VBS) with fault management	Appear under Virtual Business Services in Server and Availability perspectives.
User-defined alerts	Appear under Server perspective.
Fire drill schedules	Appear under Availability perspective.
Extended attributes	All the extended attributes, except file system extended attributes, appear under the perspective to which the attributes are related. For example, the extended attributes that are related to the objects in Availability perspective are displayed in Availability perspective.
LUN extended attributes	Appear as disk extended attribute under Server perspective.
Suppressed faults	Appear under the perspective to which the attributes are related. For example, the faults that are related to objects in Availability perspective are displayed in Availability perspective.
Recovery plans	Appear under Solutions in Availability perspective.
License Deployment Report (LDR) policies	Appear under Deployment policy tab in SFHA Licensing .

See [“Upgrading Management Server on Linux”](#) on page 53.

See [“Upgrading Management Server on Windows”](#) on page 55.

Upgrading Management Server on Linux

You can upgrade an existing Management Server on a Linux host to Veritas Operations Manager 6.0 using `Veritas_Operations_Manager_MS_6.0_Linux.bin` or `Veritas_Operations_Manager_MS_6.0_Linux_Full.bin` file. When you run the `.bin` file, the installer first attempts to upgrade the Veritas Operations Manager database to a temporary location. If the database upgrade is successful, the

remaining steps in the upgrade process are carried out. If the database upgrade fails, the previous version of Veritas Operations Manager is restored.

Before you upgrade Management Server, Symantec recommends that you take a backup of the Management Server data.

See [“Backing up Veritas Operations Manager data on Linux before upgrading to version 6.0”](#) on page 59.

To upgrade Management Server to Veritas Operations Manager 6.0 on Linux

- 1 Make sure that the host where you plan to upgrade Management Server meets or exceeds system and operating system requirements.

See [“Operating system requirements”](#) on page 27.

- 2 Download and unzip the installation file.

See [“Downloading Veritas Operations Manager 6.0”](#) on page 19.

- 3 Open an operating system console.

- 4 On the host where you plan to upgrade Management Server, log on as root.

- 5 Change directory to the location where you unzipped the `.bin` file.

- 6 At the command prompt, run one of the following commands:

- For Management Server -

```
./Veritas_Operations_Manager_MS_6.0_Linux.bin
```

- For Management Server along with the add-ons-

```
./Veritas_Operations_Manager_MS_6.0_Linux_Full.bin
```

If you see the `Permission Denied` error, change the permissions for the `.bin` file. Run one of the following commands:

- For Management Server -

```
chmod +x Veritas_Operations_Manager_MS_6.0_Linux.bin
```

- For Management Server along with the add-ons-

```
chmod +x Veritas_Operations_Manager_MS_6.0_Linux_Full.bin
```

- 7 To accept the End User License Agreement and proceed with the upgrade, type **y**.

- 8 In response to the message that confirms if you want to upgrade to Veritas Operations Manager 6.0, type **y**.

- 9 If you do not have sufficient disk space in your current database directory to create the temporary files, you are prompted to provide the path for a temporary working area having enough disk space. Provide the complete path of a temporary working area.

You can calculate the disk space requirements for the temporary files as follows:

$(2 * DB\ size) + (10\% \text{ of } DB\ size) + 150\ MB$

where *DB size* is the size of your database.

- 10 The upgrade is complete when you see message similar to the following:

```
Veritas Operations Manager upgrade is complete.
```

- 11 To verify the upgrade, run the following command:

```
rpm -q VRTSsfmcs
```

Verify that the version for the `VRTSsfmcs` package is displayed as 6.0.

See [“Verifying Management Server installation on Linux”](#) on page 42.

- 12 After a successful upgrade to Veritas Operations Manager 6.0, you can log on to Management Server using the following link:

`https://HOST_NAME:14161/vom`

where, *HOST_NAME* is the name of the Management Server.

- 13 To check whether the Veritas Operations Manager services are running, run the following command:

```
/opt/VRTSsfmh/bin/vomadm service --status
```

See [“Upgrading host management on UNIX/Linux using operating system commands”](#) on page 65.

Upgrading Management Server on Windows

You can upgrade an existing Management Server on a Windows host to Veritas Operations Manager 6.0 using the `Veritas_Operations_Manager_MS_6.0_Win.exe` or `Veritas_Operations_Manager_MS_6.0_Win_Full.exe` file. When you run the `.exe` file, the installer first attempts to upgrade the Veritas Operations Manager database to a temporary location. If the database upgrade is successful, the remaining steps in the upgrade process are carried out. If the database upgrade fails, the previous version of Veritas Operations Manager is restored.

Before you upgrade Management Server, Symantec recommends that you take a backup of the Management Server data.

See [“Backing up Veritas Operations Manager data on Windows before upgrading to version 6.0”](#) on page 61.

To upgrade Management Server to Veritas Operations Manager 6.0 on Windows

- 1 Make sure that the host where you plan to upgrade Management Server meets or exceeds system and operating system requirements.
 See [“Operating system requirements”](#) on page 27.
- 2 On the host where you plan to upgrade Management Server, log on as a user with administrator privileges.
- 3 Download and unzip the installation file.
 See [“Downloading Veritas Operations Manager 6.0”](#) on page 19.
- 4 Turn off the Windows firewall, or, open ports 5634 and 14161 for TCP/IP communication.
- 5 Ensure that there is no pending restart from Windows Update. If there is, restart the host before launching the installer.
- 6 To launch the installer, run one of the following files:
 - For Management Server-`Veritas_Operations_Manager_MS_6.0_Win.exe`
 - For Management Server along with the add-ons-
`Veritas_Operations_Manager_MS_6.0_Win_Full.exe`
- 7 In the message window that confirms if you wish to upgrade to Veritas Operations Manager 6.0, click **Yes** to continue with the upgrade.
- 8 In the **Veritas Operations Manager 6.0 setup wizard**, click **Next**.
- 9 To accept the End User License Agreement and proceed with the upgrade, select **I accept the terms of the License Agreement**, and click **Next**.
- 10 If the disk space in your current database directory is insufficient for creating the temporary files, provide the path to a temporary work area that has the required disk space.
 You can calculate the disk space requirements for the temporary files as follows:

$$(2 * DB\ size) + (10\% \text{ of } DB\ size) + 150\ MB$$
 where, *DB size* is the size of your database.
- 11 The upgrade is complete when you see message similar to the following:
Completed the Veritas Operations Manager 6.0 Setup
- 12 Click **Finish** to close the installer.
- 13 To verify the upgrade, open the **Programs and features** panel.

- 14 To verify that the version has changed to 6.0, select the **Veritas Operations Manager for Windows** program in the currently installed programs list and check the version that is displayed.

See [“Verifying the version of Management Server in the console”](#) on page 67.
- 15 After a successful upgrade to Veritas Operations Manager 6.0, you can log on to Management Server using the following link:

`https://HOST_NAME:14161/vom`

where, *HOST_NAME* is the name of the Management Server.
- 16 In the Windows Services panel, check whether the **Veritas Storage Foundation Messaging Service** is running.

See [“Upgrading host management on Windows using the installer package”](#) on page 66.

About backing up and restoring Veritas Operations Manager data

You need to back up Veritas Operations Manager data in the following situations:

- As a regular backup task to prevent data loss in the event of a failure
See [“Taking regular backups of Veritas Operations Manager data on Linux”](#) on page 58.
See [“Taking regular backups of Veritas Operations Manager data on Windows”](#) on page 60.
- Before you upgrade Management Server to version 6.0
See [“Backing up Veritas Operations Manager data on Linux before upgrading to version 6.0”](#) on page 59.
See [“Backing up Veritas Operations Manager data on Windows before upgrading to version 6.0”](#) on page 61.

Similarly, you need to restore Veritas Operations Manager data in the following situations:

- To restore the Management Server to the last backed up state, when the Veritas Operations Manager 6.0 application fails.
- To restore the Management Server for the previous version, when the Management Server upgrade to version 6.0 fails.

See [“Restoring backed up data on Linux”](#) on page 59.

See [“Restoring backed up data on Windows”](#) on page 62.

Points to remember when you back up or restore Veritas Operations Manager data:

- You must use the script (`vom_bkup.pl`) of the same version for the backup and restore tasks for that version. For example, use the version 6.0 script to back up data, and use the same script when you need to restore the data.
- You can restore data to a particular version only if the backup was taken for that version. For example, if you back up data for version 4.1, you cannot restore the backup to a version 5.0 Management Server. You can restore a version 4.1 backup only to a version 4.1 Management Server.
- On Linux, you can use the script to back up or restore Management Server data in either the standard configuration, or in the high-availability configuration.
- On Windows, you can use the script to back up Management Server data in either the standard configuration, or in the high-availability configuration. However, you can restore the backup only for a standard configuration. To restore the backed-up data for a high-availability configuration, contact Symantec Technical Support.

Note: Veritas Operations Manager data is also backed up as a part of file system level data backup on the Management Server. In such cases, you need to stop all the Veritas Operations Manager processes before backing up the data.

Taking regular backups of Veritas Operations Manager data on Linux

You can regularly back up the Management Server data to prevent data loss in the event of a failure. Veritas Operations Manager provides the `vom_bkup.pl` script that you can use to back up and restore data.

Before you take the backup, review information on what is supported, and the limitations.

See [“About backing up and restoring Veritas Operations Manager data”](#) on page 57.

To take regular backups of Veritas Operations Manager data on Linux

- 1 On the host where you plan to back up Management Server, log on as a root user.
- 2 Locate the `vom_bkup.pl` perl script at the following location:

```
/opt/VRTSsfmcs/config/adm/
```

- 3 To take the backup, run the script at the command prompt:

```
./vom_bkup.pl --backup dir
```

where, *dir* is the location that you specify for creating the backup. You can specify any location except `/var/opt/VRTSsfmh`, `/opt/VRTSsfmh`, `/var/opt/VRTSsfmcs`, or `/opt/VRTSsfmcs`.

See [“Restoring backed up data on Linux”](#) on page 59.

Backing up Veritas Operations Manager data on Linux before upgrading to version 6.0

We recommend that you back up data before you upgrade Management Server to a newer version. If the upgrade fails, you can reinstall the previous version and restore the backed up data for that version.

To take the backup, use the `vom_bkup.pl` script that is available on the Management Server host.

Before you take the backup, review information on what is supported, and the limitations.

See [“About backing up and restoring Veritas Operations Manager data”](#) on page 57.

To back up Veritas Operations Manager data on Linux before upgrade to version 6.0

- 1 On the host where you plan to back up Management Server, log on as a root user.
- 2 To take the backup, run the script at the command prompt:

```
/opt/VRTSsfmcs/config/adm/vom_bkup.pl --backup dir
```

where, *dir* is the location that you specify for creating the backup. You can specify any location except `/var/opt/VRTSsfmh`, `/opt/VRTSsfmh`, `/var/opt/VRTSsfmcs`, or `/opt/VRTSsfmcs`.

See [“Restoring backed up data on Linux”](#) on page 59.

See [“Upgrading Management Server on Linux”](#) on page 53.

Restoring backed up data on Linux

After you have backed up the Veritas Operations Manager data, you can use the `vom_bkup.pl` backup script to restore the data as and when required.

Note: To restore data after the upgrade to Veritas Operations Manager 6.0 failed, use the same script that you used to take the backup. For more information on restoring the data, refer to the *Veritas Operations Manager Installation and Configuration Guide* of that release.

You can restore the data to the same host on which the data was backed up, or to a different host. To restore the data to a different host, you need to do the following tasks on the new host before you perform the restore operation:

- Change the physical host name and the IP address to match the system on which the backup was taken.
- Install Veritas Operations Manager Management Server. The Veritas Operations Manager version should be the same as the version on the system that was used to back up the data.
- Configure Veritas Operations Manager using the same database directory.
- Restore the data.
- Install all the add-ons that were installed on Management Server at the time of backing up the data.

Before you restore the data, review information on what is supported, and the limitations.

See [“About backing up and restoring Veritas Operations Manager data”](#) on page 57.

To restore the Veritas Operations Manager data on Linux

- 1 Run the following command to restore the data:

```
/opt/VRTSsfmcs/config/adm/vom_bkup.pl --restore dir
```

where, *dir* is the location that you specified for creating the backup.

- 2 Run the following command on Management Server to force the batch rescan of all the managed hosts:

```
/opt/VRTSsfmh/bin/xdistc --run -- mh_ctl.pl --rescan
```

Taking regular backups of Veritas Operations Manager data on Windows

You can regularly back up the Management Server data to prevent data loss in the event of a failure. Veritas Operations Manager provides the `vom_bkup.pl` script that you can use to back up and restore data.

Before you take the backup, review information on what is supported, and the limitations.

See [“About backing up and restoring Veritas Operations Manager data”](#) on page 57.

To take regular backups of Veritas Operations Manager data on Windows

- 1 On the host where you plan to back up Management Server, log on as a user with administrator privileges.

- 2 Locate the `vom_bkup.pl` script at the following location:

```
installdir\VRTSsfmcs\config\adm
```

- 3 To take the backup, run the script at the command prompt:

```
"installdir\VRTSsfmh\bin\perl.exe"
```

```
"installdir\VRTSsfmcs\config\adm\vom_bkup.pl" --backup "dir"
```

where, *installdir* is the installation directory and *dir* is the location that you specify for creating the backup. Make sure that the location that you specify has adequate disk space to store the backup. You can specify any location except the following:

- %ALLUSERPROFILE%\Veritas\VRTSsfmcs
- %ALLUSERPROFILE%\Veritas\VRTSsfmh
- %APPDATA%\Symantec\VRTSsfmcs
- %APPDATA%\Symantec\VRTSsfmh

See [“Restoring backed up data on Windows”](#) on page 62.

Backing up Veritas Operations Manager data on Windows before upgrading to version 6.0

We recommend that you back up data before you upgrade Management Server to a newer version. If the upgrade fails, you can reinstall the previous version and restore the backed up data for that version.

To take the backup, use the `vom_bkup.pl` script that is available on the Management Server host.

Before you take the backup, review information on what is supported, and the limitations.

See [“About backing up and restoring Veritas Operations Manager data”](#) on page 57.

To back up Veritas Operations Manager data on Windows before upgrade to version 6.0

- 1 On the host where you plan to back up Management Server, log on as a user with administrator privileges.
- 2 To take the backup, run the following command at the command prompt:

```
"installldir\VRTSsfmh\bin\perl.exe"  
"installldir\VRTSsfmcs\config\adm\vom_bkup.pl" --backup "dir"
```

where, *installldir* is the installation directory and *dir* is the location that you specify for creating the backup. Make sure that the location that you specify has adequate disk space to store the backup. You can specify any location except the following:

- C:\Program Files\Veritas\VRTSsfmcs
- C:\Program Files\Veritas\VRTSsfmh
- C:\Documents and Settings\All Users\Application Data\Symantec\VRTSsfmcs
- C:\Documents and Settings\All Users\Application Data\Symantec\VRTSsfmh

See [“Restoring backed up data on Windows”](#) on page 62.

Restoring backed up data on Windows

After you have backed up the Veritas Operations Manager data, you can use the `vom_bkup.pl` backup script to restore the data as and when required.

Note: To restore data because the upgrade to Veritas Operations Manager 6.0 failed, use the same script that you used to take the backup. For more information on restoring the data, refer to the *Veritas Operations Manager Installation and Configuration Guide* for that release.

You can restore the data to the same host on which the data was backed up, or to a different host. To restore the data to a different host, you need to do the following tasks on the new host before you perform the restore operation:

- Change the physical host name and the IP address to match that of the system that you backed up the data on.
- Install Veritas Operations Manager Management Server. The Veritas Operations Manager version should be the same as the version on the system that was used to back up the data.
- Configure Veritas Operations Manager using the same database directory.
- Restore the data.
- Install all the add-ons, that were installed on Management Server at the time of backing up the data.

Before you restore the data, review information on what is supported, and the limitations.

See [“About backing up and restoring Veritas Operations Manager data”](#) on page 57.

To restore the Veritas Operations Manager data on Windows

- 1 Run the following command to restore the data:

```
"installldir\VRTSsfmh\bin\perl.exe"  
"installldir\VRTSsfmcs\config\adm\vom_bkup.pl" --restore dir
```

where, *installldir* is the installation directory and *dir* is the location that you specified for creating the backup.

- 2 Run the following command on Management Server to force the batch rescan of all the managed hosts:

```
"installldir\VRTSsfmh\bin\perl.exe" "installldir\VRTSsfmh\bin\xdistc  
--run -- mh_ctl.pl --rescan
```

See [“Taking regular backups of Veritas Operations Manager data on Windows”](#) on page 60.

About upgrading managed hosts to Veritas Operations Manager 6.0

You can upgrade managed hosts in your Management Server domain to Veritas Operations Manager 6.0 to make them compatible with the 6.0 Management Server. You can upgrade both the UNIX-based and the Windows-based managed hosts. You can upgrade to Veritas Operations Manager 6.0 from the following:

- SF Manager 2.x managed host
- Veritas Operations Manager 3.x managed host
- Veritas Operations Manager 4.x managed host
- Veritas Operations Manager 5.x managed host

Note: You must upgrade Management Server to 6.0 before you upgrade the managed hosts in its domain to 6.0.

You can choose one of the following methods to upgrade a managed host to Veritas Operations Manager 6.0:

- Upgrade the managed host using **Settings > Deployment** in the Veritas Operations Manager console.

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

- Upgrade the managed host using operating system commands.
See [“Upgrading host management on UNIX/Linux using operating system commands”](#) on page 65.
See [“Upgrading host management on Windows using the installer package”](#) on page 66.

Upgrading managed hosts using the console

You can upgrade multiple managed hosts using the Management Server console. This method is an efficient method to upgrade the `VRTSsfmh` package remotely on the managed hosts, instead of upgrading it individually. To upgrade the managed hosts, ensure that the `VRTSsfmh` package is uploaded to the repository. You need not remove any hot fix that is installed on the host for the `VRTSsfmh` package before the upgrade.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective. The root user can also perform this task.

To upgrade managed hosts using the Veritas Operations Manager console

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Select **Deployment**, and then select **Base Releases**.
- 3 Right-click the `vom-6.0.0.0-mh` package, and select **Install**.
- 4 In the **Install Download** wizard panel, select a download option, and click **Next**.

See [“Install - Download hot fix, package, or patch panel options”](#) on page 209.

- 5 In the **Install Select hosts** panel, click **Hosts** option, and select the desired managed hosts. To upgrade all the managed hosts that use a specific platform, use the **Platforms** option. Click **Finish**.

See [“Install - Select hosts panel options”](#) on page 210.

- 6 In the **Result** panel, click **Close**.

See [“Adding the managed hosts to Management Server using an agent configuration”](#) on page 138.

See [“Adding the managed hosts to Management Server using an agentless configuration”](#) on page 140.

Upgrading host management on UNIX/Linux using operating system commands

You can upgrade an existing managed host on UNIX to Veritas Operations Manager 6.0 by upgrading the `VRTSsfmh` package on it.

To upgrade managed host to Veritas Operations Manager 6.0 on UNIX

- 1 Make sure that the host where you plan to upgrade host management meets or exceeds system and operating system requirements.

See [“Operating system requirements”](#) on page 27.

- 2 Download the managed host installation files bundle, and unzip it.

See [“Downloading Veritas Operations Manager 6.0”](#) on page 19.

- 3 Open an operating system console.

- 4 On the host where you plan to upgrade host management, log on as root.

- 5 Change directory to the location where you unzipped the installation files bundle.

If the host is an AIX or an HP-UX host, decompress the downloaded file.

See [“Downloading managed host files”](#) on page 20.

- 6 If you are upgrading a Solaris 11 host, run the following commands to stop the services:

- `/opt/VRTSsfmh/adm/xprtldctrl stop`
- `/opt/VRTSsfmh/adm/vxvmdiscovery-ctrl.sh stop`

- 7 At the command prompt, enter one of the following commands to upgrade the package:

- For AIX, enter the following:
`installp -ad VRTSsfmh_6.0.xxx.0_AIX.bff VRTSsfmh`
 where, `xxx` is the build number for the release.
- For HP-UX, enter the following:
`swinstall -s $PWD VRTSsfmh`
- For Linux on x86 or Xeon, enter the following:
`rpm -U VRTSsfmh_6.0.xxx.0_Linux.rpm`
 where, `xxx` is the build number for the release.
- For Linux on PowerPC, enter the following:
`rpm -U VRTSsfmh_6.0.xxx.0_Linux_arch_ppc64.rpm`
 where, `xxx` is the build number for the release.
- For Solaris on SPARC versions before version 11, enter the following:

```
pkgadd -d VRTSsfmh_6.0.xxx.0_SunOS_arch_sparc.pkg -a
/opt/VRTSsfmh/etc/VRTSsfmhadmin VRTSsfmh
```

where, *xxx* is the build number for the release.

- For Solaris on x86 versions before version 11, enter the following:

```
pkgadd -d VRTSsfmh_6.0.xxx.0_SunOS_arch_i386.pkg -a
/opt/VRTSsfmh/etc/VRTSsfmhadmin VRTSsfmh
```

where, *xxx* is the build number for the release.

- For Solaris 11 on SPARC, enter the following:

```
pkg update --accept -g
VRTSsfmh_6.0.xxx.0_SunOS_arch_sparc_osr_5.11.p5p package_path
VRTSsfmh
```

- For Solaris 11 on x86, enter the following:

```
pkg update --accept -g
VRTSsfmh_6.0.xxx.0_SunOS_arch_i386_osr_5.11.p5p package_path
VRTSsfmh
```

- 8 To verify that the package has been upgraded and the version has changed to 6.0, enter one of the following at the command prompt:

- On AIX, enter the following:

```
lsllpp -l VRTSsfmh
```

- On HP-UX, enter the following:

```
swlist VRTSsfmh
```

- On Linux, enter the following:

```
rpm -q VRTSsfmh
```

- On Solaris, enter the following:

```
pkginfo -l VRTSsfmh
```

See [“Verifying the version of a managed host in the console”](#) on page 67.

Upgrading host management on Windows using the installer package

You can upgrade an existing managed host on Windows to Veritas Operations Manager 6.0 by upgrading the .msi package on it.

To upgrade managed host to Veritas Operations Manager 6.0 on Windows

- 1 Log on to the target host as a user with administrator privileges.
- 2 Download the managed host installation files bundle, and unzip it.

See [“Downloading Veritas Operations Manager 6.0”](#) on page 19.

- 3 From the directory to which you unzipped the installation files bundle, do one of the following:
 - On a 32-bit host, run `VRTSsfmh_6.00.xxx_Windows_arch_x86.msi`
 - On a 64-bit host, run `VRTSsfmh_6.00.xxx_Windows_arch_x64.msi`where, `xxx` is the build number for the release.
See [“Downloading managed host files”](#) on page 20.
 - 4 On the Welcome screen of the InstallShield Wizard, click **Next**.
 - 5 On the Ready to Install the Program screen, click **Install** to start the upgrade.
 - 6 Click **Finish** to exit the InstallShield Wizard.
 - 7 To verify the upgrade, open the **Add or Remove Programs** panel.
 - 8 To verify that the version has changed to 6.0, click the support information link under the **Veritas Operations Manager for Windows (Host Component)** program in the currently installed programs list.
- See [“Verifying the version of a managed host in the console”](#) on page 67.

Verifying the version of Management Server in the console

After you have installed or upgraded Management Server, you can verify its version in the Management Server console.

To verify the version of Management Server in the console

- 1 In the Home page of the Management Server console, click **Help > About**.
The Management Server version is displayed.

- 2 To close the window, click **OK**.

See [“Verifying Management Server installation on Linux”](#) on page 42.

See [“Verifying Management Server installation on Windows”](#) on page 42.

Verifying the version of a managed host in the console

After you have installed or upgraded a managed host, you can verify its version in the Management Server console.

To verify the version of a managed host in the console

- 1 In the Management Server console, go to the **Server** perspective and select **Manage** in the left pane.
- 2 Select **Data Center** in the navigation tree.
- 3 Select the **Hosts** tab.
- 4 In the hosts list that is displayed, verify the managed host version under **MH Version**.

See [“Verifying managed host installation on UNIX”](#) on page 49.

See [“Verifying host management installation on Windows”](#) on page 49.

Uninstalling Management Server on Linux

You can uninstall Veritas Operations Manager Management Server by removing the `VRTSsfmcs` and `VRTSsfmh` packages from the Management Server host. When you uninstall Management Server, all data on managed hosts is also removed. If you reinstall Management Server on the host, you have to add the hosts again to the Management Server domain.

Note: You must remove the `VRTSsfmcs` package before you remove the `VRTSsfmh` package.

To uninstall Veritas Operations Manager Management Server on Linux

- 1 Open an operating system console.
- 2 On the Management Server host, log on as root.
- 3 To remove the `VRTSsfmcs` package, run the following command:
- 4 To remove the `VRTSsfmh` package, run the following command:

```
rpm -e VRTSsfmcs
```

```
rpm -e VRTSsfmh
```

See [“About installing Management Server”](#) on page 39.

Uninstalling Management Server on Windows

You can uninstall Veritas Operations Manager Management Server from a Windows host. When you uninstall Management Server, all data on managed hosts is also

removed. If you reinstall Management Server on the host, you have to add the hosts again to the Management Server domain.

To uninstall Veritas Operations Manager Management Server on Windows

- 1 Log on to the target host as a user with administrator privileges.
- 2 In the Windows Control Panel, click **Program and Features**.
- 3 From the list of installed programs, select **Veritas Operations Manager for Windows**.
- 4 Click **Uninstall/Change**.
- 5 In the dialog box, do one of the following:
 - To confirm that you want to uninstall Management Server, click **Yes**.
 - To exit without uninstalling Management Server, click **No** and skip step 6.
- 6 On the message window that indicates that the uninstall was successful, click **OK**.

See [“About installing Management Server”](#) on page 39.

Uninstalling managed host on UNIX

You can use an operating system command to remove the `VRTSsfmh` package from a UNIX managed host. When you remove the package, Veritas Operations Manager managed host is uninstalled from the managed host.

Note: Before you uninstall the host, remove it from the Management Server domain.

To uninstall Veritas Operations Manager managed host on UNIX/Linux

- 1 Open an operating system console.
- 2 On the managed host where you plan to uninstall managed host, log on as root.
- 3 At the command prompt, enter one of the following commands to uninstall the package:
 - On AIX, enter the following:
`installp -u VRTSsfmh`
 - On HP-UX, enter the following:
`swremove VRTSsfmh`
 - On Linux, enter the following:

```
rpm -e VRTSsfmh
```

- On Solaris 10, enter the following:

```
pkgrm VRTSsfmh
```

- On Solaris 11, enter the following:

```
pkg uninstall VRTSsfmh
```

See [“About installing managed host”](#) on page 44.

Uninstalling host management on Windows

You can uninstall Veritas Operations Manager host management on a Windows managed host.

Note: Before you uninstall the host, remove it from the Management Server domain.

To uninstall Veritas Operations Manager host management on Windows

- 1 Log on to the target host as a user with administrator privileges.
- 2 Go to the Windows control panel and do one of the following:
 - On Windows Server 2003, click **Add or Remove Programs**.
 - On Windows Server 2008 and Windows Server 2012, click **Programs and Features**.
- 3 From the list of installed programs, select **Veritas Operations Manager (Host Component)**.
- 4 Do one of the following:
 - On Windows Server 2003, select **Remove**.
 - On Windows Server 2008 and Windows Server 2012, select **Uninstall**.
- 5 In the dialog box, do one of the following:
 - To confirm that you want to uninstall host management, click **Yes**.
 - To exit without uninstalling host management, click **No**.

See [“About installing managed host”](#) on page 44.

Configuring Veritas Operations Manager in a high availability and disaster recovery environment

This chapter includes the following topics:

- [Configuring Veritas Operations Manager in high availability environment](#)
- [Configuring Veritas Operations Manager in disaster recovery environment](#)
- [Configuring Veritas Operations Manager in high availability and disaster recovery environment](#)
- [About upgrading the high availability configurations](#)
- [About upgrading the high availability and disaster recovery configurations](#)
- [Removing the high availability configuration](#)

Configuring Veritas Operations Manager in high availability environment

You can configure the high availability (HA) feature on a Veritas Operations Manager Linux-based or Windows-based Management Server. Configuring Veritas Operations Manager in high availability environment enhances the availability of Management

Server. Also, this configuration improves the availability of the applications and the services that Veritas Operations Manager provides.

Following is an overview of the process of configuring Veritas Operations Manager in high availability environment:

- Install Management Server on both the nodes (Node1 and Node2).
- Configure Management Server on Node1 only.
- Add Node2 as a managed host to the Management server that is configured on Node1.
- Symantec Cluster Server (VCS) uses two components, Low Latency Transport (LLT) and Group Atomic Broadcast (GAB), to share data between the two nodes.
- In case of a failover, Node1 fails over to Node2 that is configured for HA.

To perform this task, you must have a root user account or your user group must be assigned the Admin role on the Management Server perspective.

You can configure the high availability (HA) feature on a new Management server that is being configured as well as on an existing Management Server.

See [“Configuring a new Veritas Operations Manager installation in high availability environment”](#) on page 72.

See [“Configuring an existing Veritas Operations Manager installation in high availability environment”](#) on page 78.

Configuring a new Veritas Operations Manager installation in high availability environment

You can configure Veritas Operations Manager in high availability environment immediately after the initial configuration of Management Server. In this method, you do not have to change the host name and the IP address of the host.

Note: To avoid losing the data, do not use this method to configure high availability environment on an existing Management Server. Follow the process of configuring an existing Veritas Operations Manager installation in high availability environment.

Configuring a new Veritas Operations Manager installation in high availability environment involves the following steps:

Table 4-1 Configuring a new Veritas Operations Manager installation in high availability environment

Step	Action	Description
1	Ensure the prerequisites for configuring a new Management Server installation in high availability environment.	See “Prerequisites for configuring a new Management Server in high availability environment” on page 73.
2	Perform initial configuration of Management Server installation in high availability environment.	See “Performing initial configuration of Management Server installation in HA environment” on page 74.
3	Create the base service groups in VCS.	See “Creating the base service groups for HA configuration” on page 75.
4	Complete the configuration of a Management Server installation in high availability environment.	See “Completing the configuration of a Management Server installation in HA environment” on page 78.

See [“Configuring an existing Veritas Operations Manager installation in high availability environment”](#) on page 78.

See [“Configuring Veritas Operations Manager in high availability and disaster recovery environment”](#) on page 86.

Prerequisites for configuring a new Management Server in high availability environment

Before you configure a new Management Server in the high availability environment, ensure the following:

- A virtual IP and a virtual host name are available for installing and using Veritas Operations Manager in high availability environment. This IP is used and configured in VCS and should not be shared with other applications.
- Storage Foundation HA 5.x, or later is installed on Node1 and Node2 as part of preparing Management Server for high availability configuration. Both Node1 and Node2 should be in the same cluster.
- A Storage Foundation disk group, volume and a file system for the data is created. Use VxVM and VxFS to create the disk group, volume and a file system. The disk group, volume and a file system are used to configure the Veritas Operations Manager database in high availability environment.
For more information on creating disk groups and volume, see *Veritas Storage Foundation Administrator's Guide*.

See “[Configuring a new Veritas Operations Manager installation in high availability environment](#)” on page 72.

Performing initial configuration of Management Server installation in HA environment

You need to install Management Server on Node1 and Node2 and configure Management Server on Node1 only. Add Node2 as a managed host to the Management server that is configured on Node1.

To configure Management Server on Node1

- 1 You need to configure Node1 as Management Server in standalone mode.
 To configure a new Management Server, click the following URL that displays after you install the Management Server on Node1:
`https://My_host_1:5634`
 Where, *My_host_1* is the host name of Node1. Alternatively, you can use the IP address of Node1.
 You must ensure that you have appropriate privileges to log on to this host.
- 2 In the Server Setting page, do the following:
 - In the **Server Name** field, enter the *virtual host name* of Node1.
 - In the **Server Address** field, enter the *virtual IP address* of Node1.
- 3 In the Database Setting page, specify the *database location*.
 This field displays the default database path. If required, you can modify it. If you specify a database path other than the default path, ensure the availability of sufficient disk space.
 If you specify the location other than the default database location, you must make sure that it is not part of the shared file system that is used for failover. Later, the Veritas Operations Manager HA script moves the database to the shared file system.
- 4 In the Analytics Setting page, select **Enable Analytics Gathering** to allow Symantec to gather data on your Veritas Operations Manager usage. Click **Finish**.
- 5 In the next panel, view the status of the tasks that are performed. Click **Launch Web Console** to log on to Management Server on Node1.

To add Node2 as a managed host to the configured Management Server

- ◆ Use the Veritas Operations Manager Web console to add Node2 as a managed host to the Management Server that is configured on Node1.

- See “Configuring a new Veritas Operations Manager installation in high availability environment” on page 72.
- See “Configuring an existing Veritas Operations Manager installation in high availability environment” on page 78.
- See “Configuring Veritas Operations Manager in disaster recovery environment” on page 80.
- See “Configuring Veritas Operations Manager in high availability and disaster recovery environment” on page 86.

Creating the base service groups for HA configuration

For HA configuration, you need to create some base service groups and resources, and add some dependencies between resources.

To perform this task, your user group must be assigned the Admin role on the cluster or the Availability perspective. The permission on the cluster may be explicitly assigned or inherited from a parent Organization.

You need to create following service groups with their respective resources:

Table 4-2

Service group	Resource
SFM_SStore	■ SFM_SStore_DG
SFM_Services	■ SFM_Services_IP ■ SFM_Services_NIC ■ SFM_Services_Mount

Note: For HA configuration, you need to use the service group names and resource names as suggested. Failure to do so will result in configuration failure.

- For the resources that you can create on the SFM_SStore service group for Windows cluster, refer to the following table:

Resource name	Resource type	Attributes
SFM_SStore_DG	VMDg	Diskgroup: Disk group that is specified for the failover. Note: You must create a clustered disk group.

- For the resources that you can create on the SFM_SStore service group for Linux cluster, refer to the following table:

Resource name	Resource type	Attributes
SFM_SStore_DG	Disk group	Diskgroup: Disk group that is specified for the failover.

- For the resources that you can create on the SFM_Services service group for a Windows cluster, refer to the following table:

Resource name	Resource type	Attributes
SFM_Services_IP	IP	■ Address: Virtual IP address. ■ MACAddress: Physical address of NIC, to which virtual IP address is assigned. This address is always local and different for each system. ■ SubNetMask: Subnet mask that is associated with the IP address.
SFM_Services_NIC	NIC	■ MACAddress: Physical address of NIC, to which virtual IP address is assigned. This address is always local and unique for each system.
SFM_Services_Mount	Mountv	■ MountPath: The drive letter that is assigned to the volume being mounted. ■ VMDGResName: Name of the disk group resource (SFM_SStore_DG). ■ Volume Name: Name of the volume to be mounted.

- For the resources that you can create on the SFM_Services service group for a Linux cluster, refer to the following table:

Resource name	Resource type	Attributes
SFM_Services_IP	IP	■ Address: Virtual IP address, which you have configured along with the virtual host name. ■ Device: Name of the NIC where virtual IP is plumbed. ■ NetMask: Subnet mask that is associated with the virtual IP address.

Resource name	Resource type	Attributes
SFM_Services_NIC	NIC	Device: Name of the NIC where virtual IP is plumbed.
SFM_Services_Mount	Mount	■ MountPoint: Mount point name of the file system that is specified for failover. ■ Block Device: Complete path of the storage device that is specified for failover. For example, <code>/dev/vx/dsk/disk_group/volume_name</code>. ■ FSType: Type of the file system (VxFS). ■ FsckOpt: File check option (fsckpt = -n or -y).

For more information on configuring resources, refer to the *Veritas Cluster Server Bundled Agents Reference Guide*.

After creating the base service groups and resources, you need to link those base service groups and resources as following:

SFM_Services	Parent Group
SFM_SStore	Child Group
Relationship	Online Local
Dependency Type	Hard

For **SFM_Services** service group, link the **SFM_Services_IP** resource as parent and **SFM_Services_NIC** as child resource.

Note: You need to setup the autostart list for **SFM_Store** and **SFM_Services** service groups to make the services start on a particular node in case of reboot of both the nodes at the same time.

See [“Configuring a new Veritas Operations Manager installation in high availability environment”](#) on page 72.

See [“Configuring an existing Veritas Operations Manager installation in high availability environment”](#) on page 78.

Completing the configuration of a Management Server installation in HA environment

After you create the base service groups and resources and add dependencies between resources, you need to perform certain steps to complete the configuration in high availability environment.

To complete the configuration of a new Veritas Operations Manager installation in high availability environment

- 1 Open a Web browser, and launch the following URL:
https://My_virtual-host:5634
where, My_virtual-host is the virtual host name of Node1.
You must ensure that you have appropriate privileges to log on to this host.
- 2 In the panel that displays the message **Click Next to configure MS as a Cluster Node**, click **Next**.
- 3 In the next panel, which displays the steps that you must do to configure Management Server as a cluster node, click **Start**.
- 4 In the panel, that displays the steps that you must do to configure Management Server in high availability environment, click **Next**.
- 5 In the panel, that displays the details of the service group for the HA configuration for your review, click **Next**.
- 6 View the status of the tasks that are performed as part of Veritas Operations Manager HA configuration and do one of the following:
 - Click the link that is displayed on the panel to log on to Veritas Operations Manager that is configured in high availability environment.
 - Click **Quit** to quit the configuration dialog.

See [“Configuring a new Veritas Operations Manager installation in high availability environment”](#) on page 72.

See [“Configuring an existing Veritas Operations Manager installation in high availability environment”](#) on page 78.

Configuring an existing Veritas Operations Manager installation in high availability environment

Configuring an existing Veritas Operations Manager installation in high availability environment involves the following steps:

- If you have used a virtual host name and a virtual IP address for configuring the Management Server, follow the process of configuring a new Veritas Operations

Manager installation in high availability environment, see [Configuring a new Veritas Operations Manager installation in high availability environment](#)

- If you have not used a virtual host name and a virtual IP address for initially configuring the Management Server, see [Table 4-3](#)

Table 4-3 Configuring an existing Veritas Operations Manager installation in high availability environment, if virtual host name and virtual IP address has not been used for initially configuring the Management Server

Step	Action	Description
Step 1	Ensure the prerequisites for configuring an existing Management Server installation in high availability environment.	See “Prerequisites for configuring an existing Management Server in high availability environment” on page 79.
Step 2	Modify the default host name and virtual IP address of the Management Server.	See “Modifying the default IP address and host name of the existing Management Server for high availability configuration” on page 80.
Step 3	Create the base service groups in VCS to ensure failover.	See “Creating the base service groups for HA configuration” on page 75.
Step 4	Complete the configuration of a Management Server installation in high availability environment.	See “Completing the configuration of a Management Server installation in HA environment” on page 78.

See [“Configuring a new Veritas Operations Manager installation in high availability environment”](#) on page 72.

See [“Configuring Veritas Operations Manager in disaster recovery environment”](#) on page 80.

See [“Configuring Veritas Operations Manager in high availability and disaster recovery environment”](#) on page 86.

Prerequisites for configuring an existing Management Server in high availability environment

Before you configure an existing Management Server in the high availability environment, ensure the following:

- Storage Foundation HA 5.x, or later is installed on Node1 and Node2 as part of preparing Management Server for high availability configuration. Both Node1 and Node2 should be in the same cluster.

- A Storage Foundation disk group, volume and a file system for the data is created with identical names on all the nodes. Use VxVM and VxFS to create the disk group, volume and a file system. The disk group, volume and a file system are used to configure the Veritas Operations Manager database in high availability environment.
For more information on creating disk groups and volume, see *Veritas Storage Foundation Administrator's Guide*.
- Node2 is added as a managed host to the Management Server that is configured on Node1.

See [“Configuring an existing Veritas Operations Manager installation in high availability environment”](#) on page 78.

Modifying the default IP address and host name of the existing Management Server for high availability configuration

Based on the operating system of Management Server, you need to follow the recommended methods to change the default IP address and host name to a new IP address and a new host name. The old default IP address and host name will be used as a virtual IP and virtual host name for the Management Server, and will be used in the HA configuration.

See [“Configuring an existing Veritas Operations Manager installation in high availability environment”](#) on page 78.

Configuring Veritas Operations Manager in disaster recovery environment

You can configure the disaster recovery (DR) feature only on a Veritas Operations Manager Linux-based Management Server. Disaster recovery feature enhances the failover support and the availability of Management Server in your globally distributed data center.

Following is an overview of the process of configuring Veritas Operations Manager for disaster recovery:

- Install Management Server on the local cluster (Node1) and the remote cluster (Node2).
- Configure Management Server on Node1 only.
- Add Node2 as a managed host to the Management server that is configured on Node1. Node1 at the local cluster acts like the primary site while Node2 at the remote cluster acts like the secondary site.

- Replicate the Veritas Operations Manager database and the domain-wide information that is stored in the shared storage to the secondary node. You can use Symantec volume replicator (VVR) to replicate the data on the secondary node.
- In case of a failover, the primary node fails over to the secondary node.

To perform this task, you must have a root user account or your user group must be assigned the Admin role on the Management Server perspective.

Configuring a Veritas Operations Manager installation in disaster recovery environment involves the following steps:

Table 4-4 Configuring a Veritas Operations Manager 6.0 installation in disaster recovery environment

Step	Action	Description
1	Ensure the prerequisites for configuring a Management Server installation in disaster recovery environment.	See “Prerequisites for configuring a Management Server in DR environment” on page 81.
2	Perform initial configuration of Management Server installation in disaster recovery environment.	See “Performing initial configuration of Management Server installation in DR environment” on page 83.
3	Create the base service groups in VCS for DR configuration.	See “Creating the base service groups for DR configuration” on page 83.
4	Enable Veritas Operations Manager DR configuration.	See “Enabling DR configuration” on page 85.

See [“Configuring a new Veritas Operations Manager installation in high availability environment”](#) on page 72.

See [“Configuring an existing Veritas Operations Manager installation in high availability environment”](#) on page 78.

Prerequisites for configuring a Management Server in DR environment

Before you configure Veritas Operations Manager in the high availability and disaster recovery environment, ensure the following:

- A Storage Foundation disk group, volume and a file system for the data is created. Use VxVM and VxFS to create the disk group, volume and a file system.

The disk group, volume and a file system are used to configure the Veritas Operations Manager database in high availability environment.

- A virtual IP and a virtual host name are available for installing and using Veritas Operations Manager in disaster recovery environment. This IP is later used for configuring SFM_Services_IP resource and it should not be shared with other applications.
- Storage Foundation HA 5.x, or later, and VCS cluster are installed on the hosts that you want to designate as Node1 in local site (Site A) and Node2 in remote site (Site B).
- Global Cluster Option (GCO) is enabled in VCS in Site A and Site B. For more information on enabling GCO, see *Symantec Cluster Server Administrator's Guide*.
- Symantec Replicator Option (VVR) should be configured in Site A and Site B at VxVM level. For more information on configuring VVR, see *Veritas Volume Replicator Administrator's Guide*.
- Both the nodes on which you want to configure Veritas Operations Manager in the disaster recovery environment must report synchronized Universal Time Clock (UTC/UC) time.
- You must specify the database location. You can either use the default database location `/var/opt/VRTSsfmcs/db` or specify another location. If you specify the location other than the default database location, you must make sure that it is not part of the shared file system that is used for failover. Later, the Veritas Operations Manager DR script moves the database to the shared file system.
- If you do not use DNS Agent, you must add the host names to the `/etc/hosts` file.
- The SFM_Services and the SFM_SStore base service groups that are created on Site A and Site B should have similar attributes and values.
- Use different virtual IP addresses for GCO IP, SFM_Services_IP, and for the VVR rlinks.
- The virtual host name corresponding to the virtual IP configured in SFM_Services_IP must be the same in Site A and Site B.
- The SFM_Services base service group must be configured as Global Service group between the two clusters.
- SFM_SStore service is online on any of the nodes before you execute the disaster recovery script.
- For more information on creating disk groups and volume, see *Veritas Storage Foundation Administrator's Guide*.

See [“Configuring Veritas Operations Manager in disaster recovery environment”](#) on page 80.

Performing initial configuration of Management Server installation in DR environment

Before you configure a Linux-based Management Server in disaster recovery environment, you need to perform the following steps:

To perform initial configuration of Management Server installation in disaster recovery environment

- 1 Install Management Server on Node1 in Site A and Node2 in Site B.
- 2 Configure Node1 as Management Server in high availability environment using the virtual host and virtual IP. Follow the steps only for configuring Management server on Node1, described in the procedure.

See [“Performing initial configuration of Management Server installation in HA environment”](#) on page 74.

- 3 Use VCS DNS resource to update the host name and IP mapping. If you do not use DNS Agent, you must add the host names to the /etc/hosts file.

See [“Configuring Veritas Operations Manager in disaster recovery environment”](#) on page 80.

Creating the base service groups for DR configuration

You need to create the base service groups in Symantec Cluster Server and link those base service groups and resource types for DR configuration.

You need to create at least the following service groups with their respective resources on Node1 and Node2:

Service group	Resource
SFM_SStore	■ SFM_SStore_DG ■ SFM_SStore_RVG
SFM_Services	■ SFM_Services_IP ■ SFM_Services_NIC ■ SFM_Services_Mount ■ SFM_Services_RVGPrimary

Note: For DR configuration, you need to use the service group names and resource names as suggested. Failure to do so may result in configuration failure.

It is recommended to set up the VVR rlinks under Symantec Cluster Server control. No naming convention is required for the VVR rlink resources. For more information, refer to the *Veritas Cluster Server Bundled Agents Reference Guide* and *Veritas Cluster Server Agents for Veritas Volume Replicator Configuration Guide* depending on the version of the Symantec Cluster Server.

- For the resources that you need to create on the SFM_SStore service group, refer to the following table:

Resource name	Resource type	Attributes
SFM_SStore_DG	Disk group	Diskgroup: Disk group that is specified for the failover. Note: You must create a clustered disk group.
SFM_SStore_RVG	RVG	RVG: Replicated volume group (RVG) that is configured for replication of volumes Diskgroup: Disk group that is used for creating RVG.

- For HA-DR configuration, you need to create the resources that are created for HA configuration as well as some additional resources.
See [“Creating the base service groups for HA configuration”](#) on page 75.
For the resources that you need to create apart from the resources already created, refer to the following table:

Resource name	Resource type	Attributes
SFM_Services_RVGPrimary	RVG Primary	Contains the RVG resource name that is to be used for replication.

For more information on configuring resources, refer to the *Veritas Cluster Server Bundled Agents Reference Guide*.

After creating the required service groups and resources, you need to link the base service groups. For selecting the options while linking the service groups, refer to the following table:

Selection	Option
SFM_Services	Parent Group
SFM_SStore	Child Group
Relationship	Online Local
Dependency Type	Hard

You need to link the resources. For selecting parent and child dependencies, refer to the following table:

Parent Dependency	Child Dependency
SFM_SStore_RVG	SFM_SStore_DG
SFM_Services_IP	SFM_Services_NIC
SFM_Services_Mount	SFM_Services_RVGPrimary
SFM_Services_RVGPrimary	SFM_Services_IP

After creating the SFM_Services and SFM_SStore service groups on Site A and linking them, repeat the same procedure for site B. On Site B, ensure that the SFM_Services_NIC, SFM_SStore_RVG, and SFM_SStore_DG are online and rest of the resources are offline. Also, you must configure SFM_Services service group as Global on site A and add Site B in the cluster.

See [“Configuring Veritas Operations Manager in disaster recovery environment”](#) on page 80.

Enabling DR configuration

To enable Veritas Operations Manager DR configuration

- ◆ Run the following script on Site A to configure Site B as part of the Veritas Operations Manager DR configuration:

```
/opt/VRTSsfmh/bin/xprtlc
-u vxss://virtual_hostname:14545/sfm_admin/sfm_domain/vx
-d debug=1
-d setup=1
-d mh=Node_2
-l https://virtual_hostname:5634/admin/cgi-bin/cs_hadr_config.pl
```

where, *virtual_hostname* is the virtual host name of Site A and *Node_2* is the name of Node at Site B.

See [“Configuring Veritas Operations Manager in disaster recovery environment”](#) on page 80.

Configuring Veritas Operations Manager in high availability and disaster recovery environment

You can configure the high availability and disaster recovery feature only on a Veritas Operations Manager Linux-based Management Server that is configured in high availability environment. In your globally distributed data center, the Veritas Operations Manager HADR setup that is enabled with disaster recovery enhances the failover support.

Following is an overview of the process of configuring Veritas Operations Manager in high availability and disaster recovery environment:

- Configure a Veritas Operations Manager HA setup in a local cluster (Node1 and Node2) along with another Veritas Operations Manager HA setup in a remote cluster (Node3 and Node 4). The HA setup at the local cluster acts like the primary site while the HA setup at the remote cluster acts like the secondary site.
- Replicate the Veritas Operations Manager database and the domain-wide information that is stored in the shared storage to the secondary node. You can use Symantec volume replicator (VVR) to replicate the data on the secondary node.
- In case of a failover, at first, Node1 of primary site attempts to fail over locally to Node2. If this attempt to failover locally fails, then Node1 fails over to Node3 that is located at the secondary site. In case the attempt to fail over to Node3 also fails, node1 attempts to fail over to Node4.

To perform this task, you must have a root user account or your user group must be assigned the Admin role on the Management Server perspective.

Configuring an existing Veritas Operations Manager installation in high availability and disaster recovery environment involves the following steps:

Table 4-5

Configuring a Veritas Operations Manager 5.0 installation in high availability and disaster recovery environment

Step	Action	Description
1	Ensure the prerequisites for configuring a Management Server installation in high availability and disaster recovery environment.	See “Prerequisites for configuring a Management Server in HA-DR environment” on page 87.

Table 4-5 Configuring a Veritas Operations Manager 5.0 installation in high availability and disaster recovery environment (*continued*)

Step	Action	Description
2	Perform initial configuration of Management Server installation in high availability and disaster recovery environment.	See “Performing initial configuration of Management Server installation in HA-DR environment” on page 88.
3	Create the base service groups in VCS for HA-DR configuration.	See “Creating the base service groups for HA-DR configuration” on page 89.
4	Enable Veritas Operations Manager HA-DR configuration.	See “Enabling HA-DR configuration” on page 91.

See [“Configuring a new Veritas Operations Manager installation in high availability environment”](#) on page 72.

See [“Configuring an existing Veritas Operations Manager installation in high availability environment”](#) on page 78.

Prerequisites for configuring a Management Server in HA-DR environment

Before you configure Veritas Operations Manager in the high availability and disaster recovery environment, ensure the following:

- A virtual IP and a virtual host name are available for installing and using Veritas Operations Manager in high availability and disaster recovery environment. This IP is used and configured in VCS for SFM_Services_IP and should not be shared with other applications.
- Storage Foundation HA 5.x, or later, and VCS cluster are installed on the hosts that you want to designate as Node1 and Node2 in local site (Site A) and Node3 and Node4 in remote site (Site B). Also, Node1 in Site A and Node3 in Site B are considered as primary nodes.
- Global Cluster Option (GCO) is enabled in VCS in Site A and Site B. For more information on enabling GCO, see *Symantec Cluster Server Administrator's Guide*.
- Symantec Replicator Option (VVR) is configured in Site A and Site B at VxVM level. For more information on configuring VVR, refer to the *Veritas Volume Replicator Administrator's Guide*.

- All the nodes on which you want to configure Veritas Operations Manager in the high availability environment must report synchronized Universal Time Clock (UTC/UC) time.
- You must specify the database location. You can either use the default database location `/var/opt/VTRSsfmcs/db` or specify another location. If you specify the location other than the default database location, you must make sure that it is not part of the shared file system that is used for failover. Later, the Veritas Operations Manager DR script moves the database to the shared file system.
- If you do not use DNS Agent, you must add the host names to the `/etc/hosts` file.
- The SFM_Services and the SFM_SStore base service groups that are created on Site A and Site B should have similar attributes and values, except for SFM_SStore_IP.
- Use different virtual IP addresses for GCO IP and SFM_Services_IP.
- The virtual host name that is used on all domains in Site A and Site B are the same.
- The SFM_Services base service group must be configured as Global Service group between the two clusters.
- SFM_SStore service is online on any of the nodes before you execute the disaster recovery script.
- You need to create a Storage Foundation disk group, file system, and a volume for the data with identical names on all the nodes. Use VxVM and VxFS to create the file system and volume. The disk group, file system, and volume are used to configure the Veritas Operations Manager database in high availability environment.

For more information on creating disk groups and volume, see *Veritas Storage Foundation Administrator's Guide*.

See [“Configuring Veritas Operations Manager in high availability and disaster recovery environment”](#) on page 86.

Performing initial configuration of Management Server installation in HA-DR environment

Before you configure a Linux-based Management Server in high availability and disaster recovery environment, you need to perform the following steps:

To perform initial configuration of Management Server installation in high availability and disaster recovery environment

- 1
- Install Management Server on Node1 and Node2 in Site A and Node3 and Node4 in Site B.
- 2
- Configure Node1 as Management Server in high availability environment using the virtual host and virtual IP. Follow the steps only for configuring Management server on Node1, described in the procedure.
- 3
- Add Node3 and Node4 as managed hosts to the Management Server that is configured on Node1.
- 4
- Use VCS DNS resource to update the host name and IP mapping. If you do not use DNS Agent, you must add the host names to the /etc/hosts file.

See “Performing initial configuration of Management Server installation in HA environment” on page 74.

See “Configuring Veritas Operations Manager in high availability and disaster recovery environment” on page 86.

Creating the base service groups for HA-DR configuration

You need to create the base service groups in Symantec Cluster Server and link those base service groups and resource types for HA-DR configuration.

You need to create at least the following service groups with their respective resources on the cluster that contains Node1 and Node2 on site A:

Service group	Resource
SFM_SStore	■ SFM_SStore_DG
	■ SFM_SStore_RVG
SFM_Services	■ SFM_Services_IP
	■ SFM_Services_NIC
	■ SFM_Services_Mount
	■ SFM_Services_RVGPrimary

Note: For HA-DR configuration, you need to use the service group names and resource names as suggested above. Failure to do so may result in configuration failure.

It is recommended to set up the VVR rlinks under Symantec Cluster Server control. No naming convention is required for the VVR rlink resources. For more information, refer to the *Veritas Cluster Server Bundled Agents Reference Guide* and *Veritas*

Cluster Server Agents for Veritas Volume Replicator Configuration Guide depending on the version of the Symantec Cluster Server.

- For the resources that you need to create on the SFM_SStore service group, refer to the following table:

Resource name	Resource type	Attributes
SFM_SStore_DG	Disk group	Diskgroup: Disk group that is specified for the failover. Note: You must create a clustered disk group.
SFM_SStore_RVG	RVG	RVG: Replicated volume group (RVG) that is configured for replication of volumes Diskgroup: Disk group that is used for creating RVG.

- For HA-DR configuration, you need to create the resources that are created for HA configuration as well as some additional resources.
See [“Creating the base service groups for HA configuration”](#) on page 75.
For the resources that you need to create apart from the resources already created, refer to the following table:

Resource name	Resource type	Attributes
SFM_Services_RVGPrimary	RVG Primary	Contains the RVG resource name that is to be used for replication.

For more information on configuring resources, refer to the *Veritas Cluster Server Bundled Agents Reference Guide*.

After creating the required service groups and resources, you need to link the base service groups. For selecting the options while linking the service groups, refer to the following table:

Selection	Option
SFM_Services	Parent Group
SFM_SStore	Child Group
Relationship	Online Local
Dependency Type	Hard

You need to link the resources. For selecting parent and child dependencies, refer to the following table:

Parent Dependency	Child Dependency
SFM_Services_IP	SFM_Services_NIC
SFM_SStore_RVG	SFM_SStore_DG
SFM_Services_Mount	SFM_Services_RVGPRI
SFM_Services_RVGPRI	SFM_Services_IP

After creating the above-mentioned service groups on Site A and linking them, repeat the same procedure for site B that contains Node3 and Node4. On Site B, ensure that the SFM_Services_NIC, SFM_SStore_DG, SFM_SStore_RVG are online and rest of the resources are offline. Also, you must configure SFM_Services service group as Global on site A and add Site B in the cluster.

See [“Configuring Veritas Operations Manager in disaster recovery environment”](#) on page 80.

See [“Configuring Veritas Operations Manager in high availability and disaster recovery environment”](#) on page 86.

Enabling HA-DR configuration

To enable Veritas Operations Manager HA-DR configuration

- ◆ Run the following script on Node1 at Site A to configure Site B as part of the Veritas Operations Manager HA-DR configuration:

```
/opt/VRTSsfmh/bin/xprtlc
-u vxss://virtual_hostname:14545/sfm_admin/sfm_domain/vx
-d debug=1
-d setup=1
-d mh=Node_3,Node_4
-l https://virtual_hostname:5634/admin/cgi-bin/cs_hadr_config.pl
```

where, *virtual_hostname* is the virtual hostname that resolves to SFM_Services_IP and *Node_3* , and *Node_4* are the names of Node3 and Node4 in SiteB.

See [“Configuring Veritas Operations Manager in disaster recovery environment”](#) on page 80.

See [“Configuring Veritas Operations Manager in high availability and disaster recovery environment”](#) on page 86.

About upgrading the high availability configurations

You can upgrade Veritas Operations Manager 4.1 or later versions, Linux-based, or Windows-based Management Server that is configured in the high availability (HA) environment to version 6.0. To upgrade, you can download and use the installer for Management Server.

See [“Downloading Veritas Operations Manager 6.0”](#) on page 19.

After the upgrade, you can use the HA environment on the upgraded Veritas Operations Manager 6.0 Management Server.

Note: In the HA configuration for the Windows environment, it is mandatory to use Symantec Cluster Server (VCS) private NT domain to log on to Veritas Operations Manager.

See [“Upgrading Management Server in high availability environment”](#) on page 92.

Upgrading Management Server in high availability environment

Before you upgrade Veritas Operations Manager in the high availability environment, keep in mind the following:

- The SFM_Services, the SFM_SStore, and the SFM_XprtId service groups should be online on one of the nodes of Veritas Operations Manager in the high availability environment, which is the active node.
- Symantec recommends that you take a backup of the Management Server data.
See [“Backing up Veritas Operations Manager data on Linux before upgrading to version 6.0”](#) on page 59.
See [“Backing up Veritas Operations Manager data on Windows before upgrading to version 6.0”](#) on page 61.

Note: You must upgrade the active node before you upgrade the slave nodes.

To upgrade Management Server in high availability environment to 6.0

- 1 Follow the steps to upgrade Management Server on the active node, and then, on the slave nodes.

See [“Upgrading Management Server on Linux”](#) on page 53.

See [“Upgrading Management Server on Windows”](#) on page 55.

After the upgrade on the active node, the SFM_Services service group, and the SFM_SStore service group, are in a frozen state.

You must upgrade all the slave nodes before you unfreeze the service groups on the active node to prevent issues during failover.

- 2 To unfreeze the service groups on the active node, run the following command:

- On a UNIX host:

```
/opt/VRTSsfmcs/config/vcs/sfmha start
```

- On a Windows host:

```
"installldir\VRTSsfmh\bin\perl.exe"
```

```
"installldir\VRTSsfmcs\config\vcs\sfmha" start
```

where, *installldir* is the installation directory of Management Server.

- 3 In the console, verify that the SFM_Services, the SFM_SStore, and the SFM_Xprtld service groups are online on the active node.

See [“About upgrading the high availability configurations”](#) on page 92.

See [“Upgrading Management Server in high availability and disaster recovery environment”](#) on page 94.

About upgrading the high availability and disaster recovery configurations

You can upgrade Veritas Operations Manager 4.1, or later versions, UNIX-based Management Server that is configured in the high availability and disaster recovery (HA-DR) environment to version 6.0. To upgrade, you can download and use the installer for Management Server.

See [“Downloading Veritas Operations Manager 6.0”](#) on page 19.

After the upgrade, you can use the HA-DR environments on the upgraded Veritas Operations Manager 6.0 Management Server.

See [“Upgrading Management Server in high availability and disaster recovery environment”](#) on page 94.

Upgrading Management Server in high availability and disaster recovery environment

Before you upgrade Veritas Operations Manager in the high availability and disaster recovery environment, keep in mind the following:

- The SFM_Services, the SFM_SStore, and the SFM_Xprtld service groups should be online on one of the nodes of Veritas Operations Manager in the high availability environment, which is the active node.

Note: You must upgrade the active node before you upgrade the slave nodes.

To upgrade Management Server in high availability environment to 6.0

- 1 Follow the steps to upgrade Management Server on the active node, and then, on the slave nodes.

See [“Upgrading Management Server on Linux”](#) on page 53.

After the upgrade on the active node, the SFM_Services service group, and the SFM_SStore service group, are in a frozen state.

You must upgrade all the slave nodes before you unfreeze the service groups on the active node to prevent issues during failover.

- 2 To unfreeze the service groups on the active node, run the following command:

```
/opt/VRTSsfmcs/config/vcs/sfmha start
```

where, *installdir* is the installation directory.

- 3 You must upgrade all the slave nodes before you unfreeze the service groups on the active node to prevent issues during failover.
- 4 In the console, verify that the SFM_Services, the SFM_SStore, and the SFM_Xprtld service groups are online on the active node.

See [“About upgrading the high availability and disaster recovery configurations”](#) on page 93.

See [“Upgrading Management Server in high availability environment”](#) on page 92.

Removing the high availability configuration

You can remove the high availability configuration only from a Veritas Operations Manager Linux-based Management Server. To remove the high availability configuration from Veritas Operations Manager, you need to launch the **https://hostname:5634** URL.

Note: In Veritas Operations Manager 6.0, you cannot remove the Veritas Operations Manager HA-DR environment that is configured in the remote site.

The procedure uses the following host names:

Name of the Management Server host that is configured in My_virtual-host_1
a high availability environment

To remove the high availability configuration from Veritas Operations Manager

- 1 Launch the following URL from a Web browser:

`https://My_Virtual-host_1:5634`

where, My_Virtual-host_1 is the virtual host name of the Management Server host that is configured in a high availability environment.

- 2 In the configuration dialog, select **Reconfigure as a NON HA CMS** and click **Next**.

- 3 In the panel that lists the tasks that are to be performed to remove the Veritas Operations Manager HA configuration, click **Rollover**.

You must perform the rollover task on Node1 when you remove the high availability configuration from Veritas Operations Manager.

After the rollover task, you remove the high availability configuration from Veritas Operations Manager and move back to standalone mode. After you perform the rollover task, you do the following:

- On Node1 and Node2, remove the `sfm_ha` directory from the mount location of the file system.
 - On both the nodes, check for the `VRTSsfmcs.pre_clus` file on the location `var/opt/VRTSsfmcs.pre_clus/`. If the `VRTSsfmcs.pre_clus` file exist on any of the nodes, remove the file.
- 4 In the next panel, view the status of the tasks that are performed as part of removing the Veritas Operations Manager HA configuration and do the following:
 - Click the link that is displayed on the panel to log on to Management Server from which the HA configuration is removed.
 - Click **Quit** to quit the configuration dialog.

Installing and uninstalling Veritas Operations Manager add-ons

This chapter includes the following topics:

- [About deploying Veritas Operations Manager add-ons](#)
- [Downloading a Veritas Operations Manager add-on](#)
- [Uploading a Veritas Operations Manager add-on to the repository](#)
- [Installing a Veritas Operations Manager add-on](#)
- [Uninstalling a Veritas Operations Manager add-on](#)
- [Removing a Veritas Operations Manager add-on from the repository](#)
- [Canceling deployment request for a Veritas Operations Manager add-on](#)
- [Installing a Veritas Operations Manager add-on on a specific managed host](#)
- [Uninstalling a Veritas Operations Manager add-on from a specific managed host](#)
- [Enabling a Veritas Operations Manager add-on on a specific managed host](#)
- [Disabling a Veritas Operations Manager add-on from a specific managed host](#)
- [Refreshing the repository](#)
- [Restarting the web server](#)

About deploying Veritas Operations Manager add-ons

Veritas Operations Manager add-ons are independent optional feature packs that you can deploy on managed hosts. Add-ons are independent of each other, and they can be installed or uninstalled based on your business requirements.

Using the Management Server console, you can view the details of those Veritas Operations Manager add-ons for which there is at least one applicable host in the domain.

You can download and install the add-ons in one of the following ways:

- Download from Symantec Operations Readiness Tools (SORT) website. In the Management Server console, upload the add-on to the repository using **Upload Solutions**, and then install.
- Use the Management Server console to download and install the add-on.

Note: If you have installed the Management Server package with the add-ons, then you can view the add-ons in the Repository view and directly install them.

The Help add-on is not a part of the package. You need to separately download and install it.

For more information on the Veritas Operations Manager add-ons and their supported versions, refer to the *Veritas Operations Manager Hardware and Software Compatibility List (HSCL)*.

Add-on are of the following types:

- Install on Management Server only.
- Install on managed host only.
- Install on Management Server and managed host.

Note: When you install the add-on in high availability and high availability-disaster recovery (HA-DR) environment, you need to install the add-ons manually on all the nodes of high availability and high availability-disaster recovery cluster before using them for the configuration. Avoiding this step might result into configuration loss when the Management Server failovers to other nodes in the high availability and high availability-disaster recovery cluster.

If you have upgraded to Veritas Operations Manager Management Server 6.0 from a previous version of Veritas Operations Manager, you may need to upgrade the add-ons. The previous version of the add-on may not be supported with Veritas Operations Manager 6.0.

When you upgrade an add-on which is installed on Management Server, the new version overwrites the old version. When you upgrade an add-on which is installed on the managed host, the old version is retained.

See [“About deploying Veritas Operations Manager hot fixes”](#) on page 205.

See [“About deploying maintenance release packages and patches”](#) on page 206.

See [“Downloading a Veritas Operations Manager add-on”](#) on page 98.

See [“Uploading a Veritas Operations Manager add-on to the repository”](#) on page 99.

See [“Downloading Management Server files”](#) on page 19.

Downloading a Veritas Operations Manager add-on

Using the Management Server console, you can do one of the following:

- Download individual Veritas Operations Manager add-ons using the Management Server console.
- Download the compress file which contains all the Veritas Operations Manager add-ons from SORT website.

The `Veritas_Operations_Manager_Addons_Bundle_5.0.0.zip` contains all the add-ons applicable for version 5.0, whereas the `Veritas_Operations_Manager_Addons_Bundle_6.0.0.zip` contains all the add-ons applicable for version 6.0.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To download a Veritas Operations Manager add-on

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**.
- 3 Expand **Add-ons** to locate the add-on which you want to download.
- 4 Right-click the add-on and select **Download** to download on your local computer.

See [“Uploading a Veritas Operations Manager add-on to the repository”](#) on page 99.

See [“Installing a Veritas Operations Manager add-on”](#) on page 100.

Uploading a Veritas Operations Manager add-on to the repository

You need to download the

`Veritas_Operations_Manager_Addons_Bundle_5.0.0.zip` or 6.0.0 zip file for the add-ons from SORT website. You can also download individual add-ons using the Management Server console.

After you download the add-ons, you can upload them to the Management Server individually or as a zip file.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To upload a Veritas Operations Manager add-on to the repository

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Do one of the following:
 - Click **Upload Solutions**.
 - Click **Deployment**, and then click **Upload Solutions**.
- 3 In the **Upload Solutions to Repository** wizard panel, click **Browse** to select the add-on that you want to upload.

See [“Upload Solutions to Repository panel options”](#) on page 99.
- 4 Click **Upload** to upload the add-on to the repository.
- 5 Click **Close**.

See [“Installing a Veritas Operations Manager add-on”](#) on page 100.

See [“Removing a Veritas Operations Manager add-on from the repository”](#) on page 103.

See [“About deploying Veritas Operations Manager add-ons”](#) on page 97.

Upload Solutions to Repository panel options

Use this wizard panel to select the Veritas Operations Manager add-on, hot fix, or package, and upload the same to the repository.

Symantec Storage Foundation High Availability hot fixes cannot be uploaded to the repository.

To upload Symantec Storage Foundation High Availability hot fixes to the repository, you need to install the Patch Installer Add-on.

For more information on Patch Installer Add-on add-on, refer to the *Veritas Operations Manager Management Server Add-ons User Guide*.

See [“Uploading a Veritas Operations Manager add-on to the repository”](#) on page 99.

See [“Uploading a Veritas Operations Manager hot fix or package to the repository”](#) on page 208.

Installing a Veritas Operations Manager add-on

Before you install an add-on, you need to download it either from SORT website or using the Management Server console. Add-ons are of the following types:

- Install on Management Server only.
- Install on managed host only.
- Install on Management Server and managed host.

If you select to install an add-on that is applicable to Management Server and managed hosts, then the add-on first installs on Management Server and then on the managed hosts.

Depending on the add-on that you install, you may need to restart the web server.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To install a Veritas Operations Manager add-on

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**.
- 3 Expand **Add-ons** to select the add-on.
- 4 In the **Add-ons** tab, right-click the add-on, and select **Install**.
- 5 In the **Install -Download Add-on** wizard panel, select a download option, and click **Next**.

See [“Install - Download Add-on panel options”](#) on page 101.

- 6 In the **Install - Selects hosts** wizard panel, select the hosts, and click **Finish**.

See [“Install - Select hosts panel options for add-ons”](#) on page 101.

- 7 In the **Result** panel, click **Close**

- 8 Those add-ons which require web server restart, click **Restart Web server**.

See [“Restarting the web server”](#) on page 110.

See [“Uninstalling a Veritas Operations Manager add-on”](#) on page 102.

See [“Removing a Veritas Operations Manager add-on from the repository”](#) on page 103.

See [“Canceling deployment request for a Veritas Operations Manager add-on”](#) on page 104.

See [“Viewing the details of an add-on, hot fix, package, or patch on SORT website”](#) on page 235.

Install - Download Add-on panel options

Use this wizard panel to select the download method for downloading a Veritas Operations Manager add-on.

Table 5-1 Select the download method

Field	Description
Download from SORT	Select to download the add-on from SORT website. The add-on is uploaded to the repository.
Upload local copy	Select if you have already downloaded the add-on from SORT website.

See [“Installing a Veritas Operations Manager add-on”](#) on page 100.

Install - Select hosts panel options for add-ons

Use this wizard panel to select the managed hosts or Management Server on which you want to install the Veritas Operations Manager add-on.

If you select to install an add-on which is applicable only for managed hosts, you see **Hosts** and **Platform** options.

If you select to install an add-on which is applicable only for Management Server, these options are not available.

For the add-ons that can be installed on managed hosts, you can do one of the following:

- Select the hosts explicitly and install the add-on on the selected hosts.
- Select the platform.

If you select a specific platform, the add-on is installed on all the managed hosts using that platform. Also the add-on will be installed on all the new managed hosts that are added to the domain in the future.

For example, if you select Windows the add-on is installed on all the hosts that use Windows platform. Also when a new Windows host is added to the domain, the add-on is installed on the host.

Table 5-2 Select hosts panel options

Field	Description
Hosts	Select to view the list of all managed hosts where the add-on is not installed. Select Show all applicable hosts (Overwrites existing installation) to list all the managed hosts on which you can install the add-on. It includes: ■ Managed hosts on which the add-on is not installed currently. ■ Managed hosts on which the add-on is installed currently. In this case, Veritas Operations Manager overwrites the existing add-on installation.
Platform	Select to install the add-on on all managed hosts using the specific platform. This option is useful to install the add-on whenever a new managed host using the specific platform is added to Management Server. Select Force install (Overwrites existing installation) to overwrite existing add-on installation on the managed hosts.

See [“Installing a Veritas Operations Manager add-on”](#) on page 100.

Uninstalling a Veritas Operations Manager add-on

You can uninstall a Veritas Operations Manager add-on from the Management Server and managed host. If the add-on is applicable to the Management Server, you need to restart the web server depending on the add-on after you uninstall the add-on successfully.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To uninstall a Veritas Operations Manager add-on

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**.
- 3 Expand **Add-ons** to locate the add-on.
- 4 In the **Add-ons** tab, right-click the add-on that you want to uninstall, select **Uninstall**.
- 5 In the **Uninstall** panel, review the information, and click **Yes**.
See [“Uninstall panel options”](#) on page 103.
- 6 Those add-ons which require web server restart, click **Restart Web server**.
See [“Restarting the web server”](#) on page 110.
See [“Installing a Veritas Operations Manager add-on”](#) on page 100.
See [“Removing a Veritas Operations Manager add-on from the repository”](#) on page 103.

Uninstall panel options

Use this wizard panel to uninstall the Veritas Operations Manager add-on or hot fix.

Use this wizard panel to confirm the action of uninstalling the add-on or hot fix from all the hosts.

Select **Ignore checks (if any) before uninstalling** to ignore the checks before uninstalling.

Veritas Operations Manager packages and patches cannot be uninstalled.

See [“Uninstalling a Veritas Operations Manager add-on”](#) on page 102.

See [“Uninstalling a Veritas Operations Manager hot fix”](#) on page 211.

Removing a Veritas Operations Manager add-on from the repository

You can remove a Veritas Operations Manager add-on from the repository and Management Server. Detailed information of the add-on will not be displayed in the **Repository** view within **Deployment**.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To remove a Veritas Operations Manager add-on from the repository

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**.
- 3 Expand **Add-ons** to locate the add-on.
- 4 In **Add-ons** tab, right-click the add-on that you want to remove, select **Remove**.
- 5 In the **Remove** panel, click **Yes**.

See [“Remove panel options”](#) on page 104.

See [“Refreshing the repository”](#) on page 109.

See [“Installing a Veritas Operations Manager add-on”](#) on page 100.

See [“Installing a Veritas Operations Manager hot fix, package, or patch”](#) on page 209.

See [“Uninstalling a Veritas Operations Manager add-on”](#) on page 102.

Remove panel options

Use this wizard panel to confirm the action of removing the add-on, hot fix, package, or patch for Veritas Operations Manager or Symantec Storage Foundation High Availability from the repository.

See [“Removing a Veritas Operations Manager add-on from the repository”](#) on page 103.

See [“Removing a hot fix, package, or patch from the repository”](#) on page 212.

Canceling deployment request for a Veritas Operations Manager add-on

Using the Management Server console, you can cancel the deployment request for a Veritas Operations Manager add-on.

Deployment requests are of two types, **Deploy by host** and **Deploy by platform**. **Deploy by host** type lets you select the hosts on which you want to deploy the add-on. If you select **Deploy by platform**, then the add-on is deployed on all the hosts having the selected platform.

Request of the type **Deploy by host** cannot be canceled.

If you initiate an install request of **Deploy by platform** type, then the request is applicable for all the existing hosts as well as the new hosts that are added to the Management Server domain on a later date. In case of **Deploy by platform** request, if you cancel the deployment request, the add-on installation on all the existing

hosts is completed. But the add-on is not installed on the hosts that are added to the domain after cancellation of the deployment request.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To cancel deployment request for a Veritas Operations Manager add-on

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**.
- 3 Expand **Add-ons** to locate the add-on whose deployment request you want to cancel.
- 4 Select the **Requests** tab.
- 5 Right-click the request and select **Cancel Request**.
- 6 In the **Cancel Deployment Request** wizard panel, click **OK**.

See [“Cancel Deployment Request panel options”](#) on page 105.

See [“Installing a Veritas Operations Manager add-on”](#) on page 100.

See [“Installing a Veritas Operations Manager hot fix, package, or patch”](#) on page 209.

See [“Uninstalling a Veritas Operations Manager add-on”](#) on page 102.

Cancel Deployment Request panel options

Use this wizard panel to cancel deployment request for add-on, hot fix, package, or patch for Veritas Operations Manager or Symantec Storage Foundation High Availability.

See [“Canceling deployment request for a Veritas Operations Manager add-on”](#) on page 104.

See [“Canceling deployment request for a hot fix, package, or patch”](#) on page 213.

Installing a Veritas Operations Manager add-on on a specific managed host

Using the Management Server console, you can install the Veritas Operations Manager add-on on the selected managed host. If the add-on is already installed on the selected host, then Veritas Operations Manager overwrites the existing installation. It is referred to as a force installation.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To install a Veritas Operations Manager add-on on a specific managed host

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**.
- 3 Expand **Add-ons** to select an add-on.
- 4 In the **Applicable Hosts** tab, right-click the host, and select **Install**.
- 5 In the **Install** wizard panel, review the information, and click **OK**.
See [“Install panel options”](#) on page 106.
- 6 In the **Install - Result** panel, click **OK**. If the add-on requires web server restart, click the **Restart Web Server** button on the toolbar.
See [“Restarting the web server”](#) on page 110.
See [“About deploying Veritas Operations Manager add-ons”](#) on page 97.
See [“About deploying Veritas Operations Manager hot fixes”](#) on page 205.

Install panel options

Use this wizard panel to install the Veritas Operations Manager add-on or hot fix on a selected host.

[Table 5-3](#) lists the options for Veritas Operations Manager add-on and hot fixes.

Table 5-3 Install panel options for installing an add-on or hot fix on a selected host

Field	Description
Name	Displays the name of the selected host.
Status	Displays the status of the selected add-on or hot fix on the selected host.
Ignore checks (if any) before installing	Select to ignore checks before installing.

See [“Installing a Veritas Operations Manager add-on on a specific managed host”](#) on page 105.

See [“Installing a Veritas Operations Manager hot fix on a specific managed host”](#) on page 214.

Uninstalling a Veritas Operations Manager add-on from a specific managed host

Using the Management Server console, you can uninstall the Veritas Operations Manager add-on from the selected managed host. You can uninstall the add-on irrespective of its state (enabled or disabled).

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To uninstall a Veritas Operations Manager add-on from a specific managed host

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**.
- 3 Expand **Add-ons** to select an add-on.
- 4 In the **Applicable Hosts** tab, right-click the host, and select **Uninstall**.
- 5 In the **Uninstall** wizard panel, review the information, and click **OK**.
See [“Uninstall panel options”](#) on page 107.
- 6 In the **Uninstall - Result** panel, click **OK**.
- 7 Those add-ons which require web server restart, click **Restart Web server**.
See [“Restarting the web server”](#) on page 110.
See [“About deploying Veritas Operations Manager add-ons”](#) on page 97.
See [“About deploying Veritas Operations Manager hot fixes”](#) on page 205.

Uninstall panel options

Use this wizard panel to uninstall the Veritas Operations Manager add-on or hot fix from the selected host.

[Table 5-4](#) lists the uninstall options for Veritas Operations Manager add-on and hot fixes.

Table 5-4 Uninstall panel options for uninstalling an add-on or hot fix from a selected host

Field	Description
Name	Displays the name of the selected host.
Status	Displays the status of the selected add-on or hot fix on the selected host.

Table 5-4
Uninstall panel options for uninstalling an add-on or hot fix from a selected host (*continued*)

Field	Description
Ignore checks (if any) before installing	Select to ignore checks before installing.

See [“Uninstalling a Veritas Operations Manager add-on from a specific managed host”](#) on page 107.

See [“Uninstalling a Veritas Operations Manager hot fix from a specific managed host”](#) on page 214.

Enabling a Veritas Operations Manager add-on on a specific managed host

Using the Management Server console, you can enable a Veritas Operations Manager add-on on a selected managed host. Depending on the add-on, you may need to restart the web server.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To enable a Veritas Operations Manager add-on on a specific managed host

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**.
- 3 Expand **Add-ons** to select the add-on.
- 4 In the **Applicable Hosts** tab, right-click the host, and select **Enable**.
- 5 In the **Enable** wizard panel, review the information, and click **OK**.
- 6 In the **Enable - Result** panel, click **OK**.
- 7 Those add-ons which require web server restart, click **Restart Web server**.

See [“Restarting the web server”](#) on page 110.

See [“Installing a Veritas Operations Manager add-on on a specific managed host”](#) on page 105.

See [“Uninstalling a Veritas Operations Manager add-on from a specific managed host”](#) on page 107.

See [“Disabling a Veritas Operations Manager add-on from a specific managed host”](#) on page 109.

Disabling a Veritas Operations Manager add-on from a specific managed host

Using the Management Server console, you can disable a Veritas Operations Manager add-on from a selected managed host. Depending on the add-on, you may need to restart the web server.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To disable a Veritas Operations Manager add-on from a specific managed host

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**.
- 3 Expand **Add-ons** to select the add-on.
- 4 In the **Applicable Hosts** tab, right-click the host, and select **Disable**.
- 5 In the **Disable** wizard panel, review the information, and click **OK**.
- 6 In the **Disable - Result** panel, click **OK**.
- 7 Those add-ons which require web server restart, click **Restart Web server**.

See [“Restarting the web server”](#) on page 110.

See [“Installing a Veritas Operations Manager add-on on a specific managed host”](#) on page 105.

See [“Uninstalling a Veritas Operations Manager add-on from a specific managed host”](#) on page 107.

See [“Enabling a Veritas Operations Manager add-on on a specific managed host”](#) on page 108.

Refreshing the repository

If you remove an add-on, hot fix, package, or patch from the repository and Management Server, detailed information of the same is not displayed in the **Repository** view within **Deployment**. Using the Management Server console, you can refresh the repository to view the information again.

Latest information about add-ons, hot fixes, packages, and patches that is available on SORT is also synchronized and displayed in the **Repository** view.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To refresh the repository

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**.
- 3 Right-click **Repository** and select **Refresh Repository**.
- 4 In the **Refresh Repository** panel, to include the previously removed updates, select **Include removed updates**.
- 5 Select the updates from the list and click **Yes**.
- 6 In the **Result** panel, click **OK**.

See [“Removing a Veritas Operations Manager add-on from the repository”](#) on page 103.

See [“About deploying Veritas Operations Manager add-ons”](#) on page 97.

See [“About deploying Veritas Operations Manager hot fixes”](#) on page 205.

Restarting the web server

Depending on the Veritas Operations Manager add-on that you install, uninstall, enable, or disable on a host, you may need to restart the web server.

The **Restart Web server** button is displayed only if restart is required. You can also restart using the CLI command: `vomsc --restart web`.

When you restart the web server, all the logged in users are logged out.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To restart the web server

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**, and click **Restart Web Server**.

See [“Installing a Veritas Operations Manager add-on”](#) on page 100.

Setting up the Management Server environment

- [Chapter 6. Basic Veritas Operations Manager tasks](#)
- [Chapter 7. Adding and managing hosts](#)
- [Chapter 8. Setting up user access](#)
- [Chapter 9. Setting up fault monitoring](#)
- [Chapter 10. Setting up virtualization environment discovery](#)
- [Chapter 11. Deploying hot fixes, packages, and patches](#)
- [Chapter 12. Configuring Management Server settings](#)
- [Chapter 13. Setting up extended attributes](#)
- [Chapter 14. Downloading price tier information from SORT](#)
- [Chapter 15. Viewing information on the Management Server environment](#)

Basic Veritas Operations Manager tasks

This chapter includes the following topics:

- [About the communication between the managed hosts and Management Server](#)
- [Connecting to Veritas Operations Manager Management Server](#)
- [Stopping and starting the Web application](#)
- [About the Management Server perspective](#)

About the communication between the managed hosts and Management Server

Veritas Operations Manager provides you a single, centralized management console for the Storage Foundation and High Availability products. You can use it to monitor, visualize, and manage storage resources and generate reports about them. Veritas Operations Manager lets administrators centrally manage diverse data center environments.

A typical Veritas Operations Manager deployment consists of a Management Server and the managed hosts. The managed host can run on any platform that Veritas Operations Manager supports. In a centrally managed deployment, you must configure one host as Management Server. Management Server receives information about all the resources in its domain. When you log on to Management Server, you can gain access to the resources on different hosts within the centrally-managed deployment.

The installer installs the VRTSsfmcs (Management Server) and the VRTSsfmh (managed host) packages on the host that is designated as Management Server.

The VRTSsfmh package contains the XPRTL component that facilitates the communication between the managed hosts and Management Server. The VRTSsfmh package is installed on the managed host and Management Server.

The XPRTL component consists of the following:

- The XPRTLD component, which is a light weight and full-featured Web server.
- The XPRTLC component, which is an HTTP client that is based on command lines. The XPRTLC component can send information to Web servers .

The XPRTLD and the XPRTLC components are integrated with Veritas Authentication Services for secure SSL communication over HTTP.

The communication between the managed host and Management Server occurs through the HTTPS protocol. The XPRTLD Web server running on both the managed host and Management Server supports the Common Gateway Interface (CGI) standards. The managed hosts use XPRTLC and invoke CGI through the XPRTLD on Management Server to perform several actions such as the Veritas Operations Manager database update. Management Server uses XPRTLC and invokes CGI through the XPRTLD on the managed hosts to perform various actions that include Storage Foundation and high availability operations.

See [“Connecting to Veritas Operations Manager Management Server”](#) on page 113.

Connecting to Veritas Operations Manager Management Server

After downloading the installation files, you must install and configure Veritas Operations Manager Management Server.

See [“Installing Management Server on Linux”](#) on page 39.

See [“Installing Management Server on Windows”](#) on page 41.

See [“Verifying Management Server installation on Windows” on page 42](#) on page 42.

You can use any supported Web browser to connect to Management Server.

To connect to Veritas Operations Manager Management Server

- 1 On a client system that has a network connection to the host, open a Web browser.

Your browser must be configured to accept cookies. If you are using pop-up blockers, either disable them or configure them to accept pop-ups from the host.

- 2 In the browser's address field, type the following URL and press Enter:

`https://hostname:14161/`

where *hostname* is the host name, fully-qualified host name, or IP address of Management Server.

Example: `https://myhost.example.com:14161/`

For Internet Explorer 7.0 on Windows Server 2008, or Firefox 3.0, if the Web page does not get displayed, you have to set up the browser.

- 3 In the **username** and **password** fields, type credentials for a valid operating system network domain account.

The Authentication Service automatically recognizes users in the domain—for example, unixpwd or NT—on which the Authentication Broker host is a member.

- 4 Click **Login**.

You can view the Veritas Operations Manager dashboard.

See [“About installing managed host”](#) on page 44.

Stopping and starting the Web application

You can stop and restart Veritas Operations Manager Web UI framework.

To stop and restart Veritas Operations Manager Web UI framework

- 1 Open an operating system console and log on as root to Management Server.
- 2 Depending on the platform of Management Server, use one of the following to restart Veritas Operations Manager Web UI framework:
 - Red Hat Linux: Execute the `/opt/VRTSsfmcs/cweb/sfmw restart` command.
 - Windows: Under Service Control Manager (`services.msc`), restart the `Storage Manager Service` service.

See [“Connecting to Veritas Operations Manager Management Server”](#) on page 113.

About the Management Server perspective

The Veritas Operations Manager administrator uses the Settings page on the Management Server console to set up the Management Server environment.

The Settings page is also known as the Management Server perspective.

To view information or perform operations on the Management Server perspective requires root user access or assignment of the Admin role on the Management Server perspective.

See [“Connecting to Veritas Operations Manager Management Server”](#) on page 113.

Adding and managing hosts

This chapter includes the following topics:

- [Overview of host discovery](#)
- [Overview of agentless discovery](#)
- [Adding the managed hosts to Management Server using an agent configuration](#)
- [Adding the managed hosts to Management Server using an agentless configuration](#)
- [Adding managed hosts to Management Server using the Auto Configure \(gendeploy.pl\) script](#)
- [Editing the agentless host configuration](#)
- [Refreshing the details of the managed host](#)
- [Removing managed hosts from the Management Server domain](#)

Overview of host discovery

For an overview of host discovery, refer to the following topics:

See [“How Veritas Operations Manager discovers hosts”](#) on page 116.

See [“Supported features for host discovery options”](#) on page 120.

How Veritas Operations Manager discovers hosts

Veritas Operations Manager provides several ways to discover the hosts and their associations to storage resources and network devices. To discover the hosts and their connections to storage resources, you can either install an agent or use agentless capabilities.

Agent and agentless capabilities include the following:

Discovery of the hosts using an agent, for the hosts that have Veritas Operations Manager and Storage Foundation installed on them	An agent is a software package that runs on a host. It discovers the storage resources that are associated with a host and relays the information to Management Server.
Discovery of the non-Storage Foundation hosts using an agent, for the hosts that have Veritas Operations Manager installed on them	Agent-based discovery is also used for the non-Storage Foundation hosts that have Veritas Operations Manager installed on them.
Discovery of the non-Storage Foundation hosts using agentless discovery scripts, for the hosts that do not have Veritas Operations Manager installed on them	Veritas Operations Manager can discover a host by remotely accessing the host and then running the scripts that collect data. The agentless discovery scripts access the host using SSH (for UNIX hosts) or WMI (for Windows hosts). Veritas Operations Manager identifies this type of the host as an agentless host.

Note: Agentless discovery is not supported on the hosts that have Symantec Storage Foundation or Veritas Operations Manager installed.

Through each of these host discovery options, Management Server is the central point to which all of the discovered data flows. [Figure 7-1](#) depicts the flow of data with each of the host discovery options. [Figure 7-2](#) depicts how Veritas Operations Manager discovers virtualization servers and virtual machines.

Figure 7-1 Veritas Operations Manager components and discovery (basic)

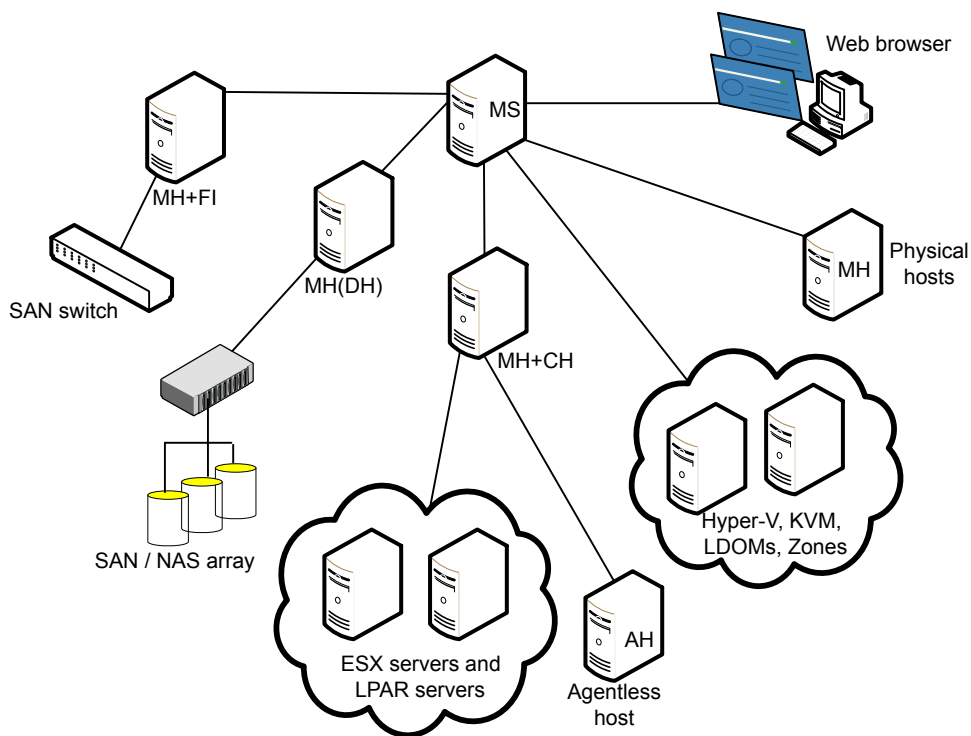
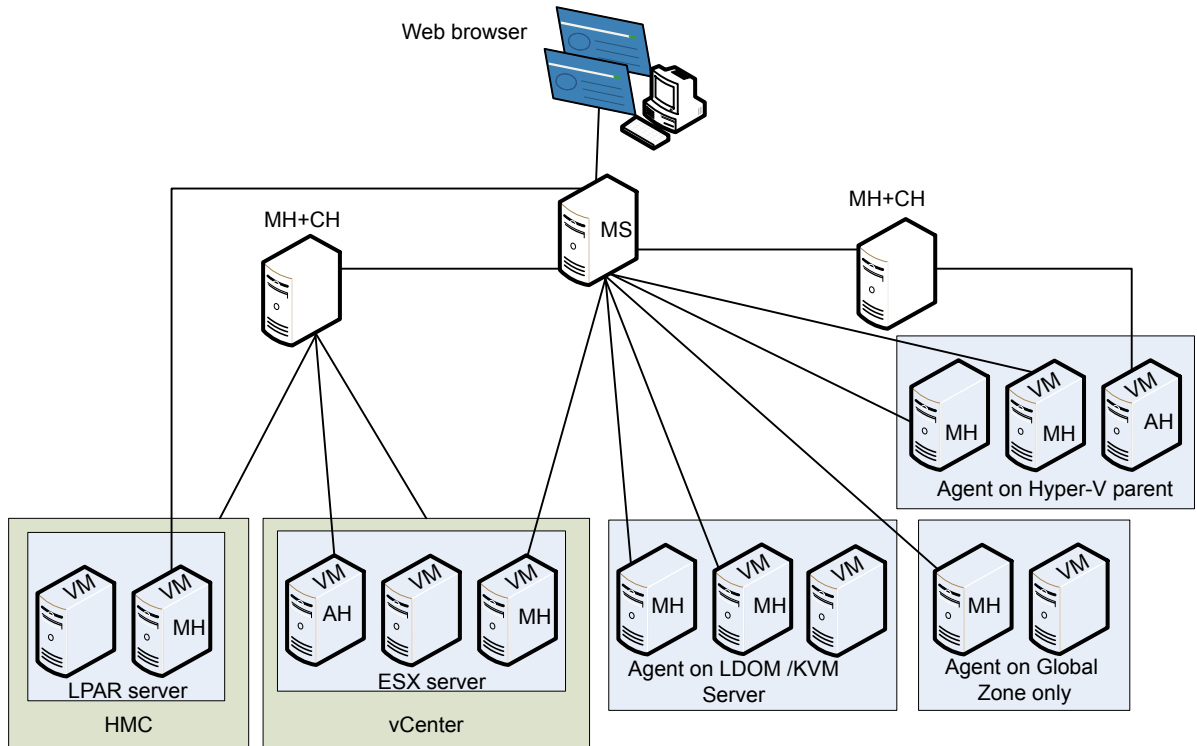


Figure 7-2 Veritas Operations Manager components and discovery (virtualization servers and virtual machines)



Managed host (MH(DH)) is the discovery host for SAN and NAS arrays. Managed host (MH+FI) discovers SAN switches if Fabric Insight Add-on is installed. Control Host (MH+CH) discovers agentless hosts (AH), VMware and LPAR servers and virtual machines. Management Server (MS) discovers managed hosts (physical hosts), Hyper-V virtualization servers, KVM, LDOMs, and Solaris Zones.

For more information on Fabric Insight Add-on, refer to the *Veritas Operations Manager Management Server Add-ons User Guide*.

See [“About Control Hosts in Veritas Operations Manager”](#) on page 187.

See [“Requirements for discovering vCenter and ESX servers using Veritas Operations Manager”](#) on page 189.

See [“Requirements for discovering the Solaris zones”](#) on page 193.

See [“Requirements for discovering Solaris Logical domains”](#) on page 194.

Supported features for host discovery options

Veritas Operations Manager provides several ways to discover hosts and their associations to storage resources and network devices.

See [“How Veritas Operations Manager discovers hosts”](#) on page 116.

Table 7-1 identifies the use cases that each host discovery option provides.

Table 7-1 Use cases for discovery options at the host level

Category	Use case	Agentless host	Agent Host
Inventory and environment reporting	Inventory report for various resources at License and product usage reporting host, enclosure, and cluster level	X* * Does not include Veritas Storage Foundation disk groups, volumes, file systems, clusters, and databases. Includes only VMware servers and virtual machines	X
Storage utilization	Storage allocation at host level		X
	File system usage	X* *Does not include Veritas Storage Foundation File Systems	X
	Resource mapping from disks on hosts to LUNs in an enclosure	X	X
	Thin pool usage	X	X
	Enclosure storage allocation to hosts	X	X
Cluster analysis	Cluster activity and trends		X

Table 7-1 Use cases for discovery options at the host level (*continued*)

Category	Use case	Agentless host	Agent Host
Storage reclamation	Reporting underutilized file systems	X* *Does not include Veritas Storage Foundation File Systems	X
	LUNs connected to multiple hosts	X	X
	Underutilized LUNs under Veritas Storage Foundation		X
	LUNs that are not part of a disk group		X

Veritas Operations Manager includes the ability to discover virtualization servers (VMware ESX servers). You can choose from different discovery options to discover virtualization servers. For VMware ESX servers, Management Server and Control Host can perform remote discovery by using VMware Infrastructure (VI SDK). To discover ESX servers, the Control Host Add-on must be installed.

Note: Agentless discovery of non-global zones, LDOMs, and VMware ESX servers is not supported. Agentless discovery of any virtual machines other than VMware guests is not supported. Agentless discovery of a non-global zone or LDOM virtual machine will result in the discovery of a physical host without any storage correlation. Agentless discovery of global zones is supported, however resources allocated from global to non-global zones on the hosts will not be discovered.

Veritas Operations Manager has the ability to discover VMware guest operating systems. The information that Veritas Operations Manager discovers depends on the discovery option that you choose. To discover information from VMware environments, you must configure the ESX server or VirtualCenter discovery, and also configure the guests using agent or agentless discovery.

If you discover the VMware guests using agentless discovery, any RDM disks visible on the guest will not be correlated to array LUNs. Similar to non-RDM disks visible to the guest, the RDM disks will be correlated to the storage exported by the corresponding ESX server. If you configure VMware guests using an agent then you can see the correlation of RDM disks visible to the guest with corresponding array LUNs.

Note: For configuring Linux VMware guests using agentless discovery, the version of the `/usr/sbin/dmidecode` utility must be 2.7 or higher.

The following tables identify the objects that Veritas Operations Manager can discover and report on with each host discovery option.

[Table 7-2](#) compares the storage resources that Veritas Operations Manager can discover with each host discovery option.

Table 7-2 Discovery of storage resources by host discovery option

Discovery area	Agentless host	Agent Host
Host	X	X
HBA	X* * Does not support iSCSI initiators discovery	X
Storage allocation and connectivity	X	X
LUNs and multipathing	X* * Does not support Veritas DMP. Does not support iSCSI LUN correlation to enclosures	X
Volume managers and file systems	X* * Does not support Veritas Storage Foundation Volume Manager and File Systems	X
Databases		X
Clusters		X

Overview of agentless discovery

For an overview of agentless discovery, refer to the following topics:

See [“About agentless discovery using the Control Host”](#) on page 123.

See [“About agentless discovery of remote hosts”](#) on page 123.

See [“How agentless discovery of a UNIX or Linux host works”](#) on page 124.

See [“How agentless discovery of a Windows host works”](#) on page 125.

See [“Prerequisites for agentless configuration”](#) on page 124.

See [“Requirements for agentless discovery of UNIX hosts”](#) on page 126.

See [“Requirements for agentless discovery of Windows hosts”](#) on page 128.

See [“Requirements for deep array discovery for agentless hosts”](#) on page 129.

See [“Commands that require the root access for agentless discovery of UNIX hosts”](#) on page 130.

See [“Using the privilege control software with agentless discovery of UNIX hosts”](#) on page 132.

See [“SSH configuration requirements for agentless discovery”](#) on page 133.

See [“About installing OpenSSH on a UNIX host”](#) on page 135.

About agentless discovery using the Control Host

Veritas Operations Manager uses Control Hosts as a discovery mechanism. A Control Host can be used to perform agentless discovery of a remote host. To perform agentless discovery, you must install the Control Host Add-on on one of the managed hosts. You can install the Control Host Add-on on Management Server, however it is not recommended as it puts extra load on Management Server.

Note: A Linux or Solaris Control Host can only discover UNIX or Linux agentless hosts using SSH. A Windows Control Host can discover Windows agentless hosts using WMI or UNIX/Linux agentless hosts using SSH. Ensure that you install one or more Control Hosts on the appropriate platform depending on the operating system of the remote hosts you want to discover agentlessly.

See [“About Control Hosts in Veritas Operations Manager”](#) on page 187.

About agentless discovery of remote hosts

Agentless discovery lets you discover hosts without installing an agent on the host. The discovery provides end-to-end visibility from the file system to the spindle. Because an agent is not required, agentless discovery eliminates agent deployment and maintenance and minimizes CPU and memory consumption.

To perform agentless discovery, Veritas Operations Manager remotely accesses the host and runs discovery scripts that collect data from a host.

See [“How agentless discovery of a UNIX or Linux host works”](#) on page 124.

See [“How agentless discovery of a Windows host works”](#) on page 125.

Prerequisites for agentless configuration

The following list provides prerequisites required for agentless configuration:

- You must install the Control Host Add-on on one or more managed hosts and/or Management Server.
Veritas Operations Manager lets you discover a host through the Control Host. The Control Host helps you manage discovery data from agentless hosts and can discover HBAs, OSHandles on the host, multipathing, Linux LVM, and file systems (including native options like ZFS). Agentless discovery does not support the discovery of databases and applications.
- A UNIX Control Host cannot be used to agentlessly discover Windows hosts. If you plan to agentlessly discover Windows hosts, you will need to plan your Control Host deployment accordingly.
- You must install Storage Insight Add-on and configure arrays for deep discovery. Storage Insight Add-on must be deployed to enable correlation of OSHandles on the agentless hosts to array LUNs.
If you make any configuration changes, for example creating new LUNs and making them visible to the host, on storage arrays, then the agentless discovery that occurs after a subsequent SI deep array discovery will reflect the changes on the agentless hosts. After making changes to the array, one SI deep discovery needs to occur and only then a subsequent agentless discovery will pick up the changes on the host.

See [“About agentless discovery using the Control Host”](#) on page 123.

How agentless discovery of a UNIX or Linux host works

To perform agentless discovery of a remote UNIX or Linux host, Veritas Operations Manager does the following:

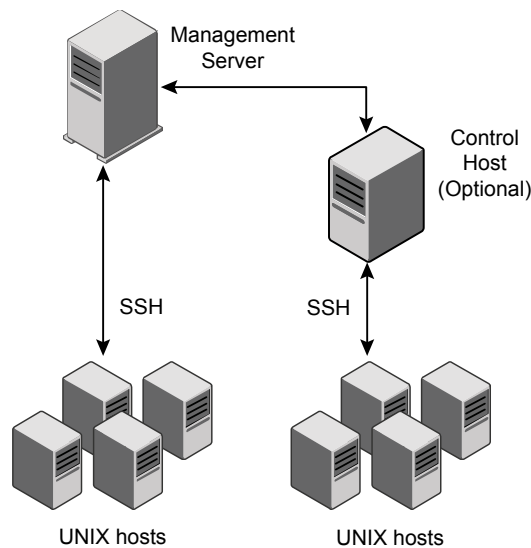
- Uses Secure Shell (SSH) to send the discovery script to the remote host.
- Runs the discovery script on the remote host.
- Saves the output of the script to a data file on the remote host in the `/var/tmp` directory.
- Uses SSH to get the output on to the Control Host.
- Deletes the files from the remote host that it used for discovery.

To perform this discovery process, Veritas Operations Manager requires a non-root user account for the remote host. Privileged access is required to discover some information.

See [“Requirements for agentless discovery of UNIX hosts”](#) on page 126.

[Figure 7-3](#) depicts how Veritas Operations Manager performs agentless discovery of UNIX or Linux hosts.

Figure 7-3 Agentless discovery of UNIX or Linux hosts



See [“About agentless discovery of remote hosts”](#) on page 123.

How agentless discovery of a Windows host works

To perform agentless discovery of a remote Windows host, Veritas Operations Manager runs a script that executes data-gathering commands. The script uses Windows Management Instrumentation (WMI), a Windows management technology that is used to work with remote hosts. The WMI calls use Microsoft's Distributed Component Object Model (DCOM) to obtain the data from the host. Veritas Operations Manager creates a private local user account (vomuser) on Management Server or a Control Host to facilitate its use of DCOM. To communicate between Veritas Operations Manager Control Host and the remote host, WMI uses port 135.

Veritas Operations Manager uses WMI in two ways:

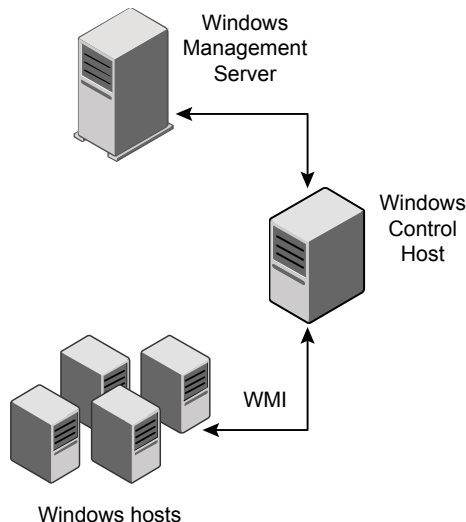
- First, WMI contacts a service that runs on the remote host and invokes the service to perform the actions that collect data about the host. As it collects data, WMI sends the data back to the Control Host.
- Second, WMI invokes command line tools such as nslookup and fcinfo. The output from the command line tools saves to a data file on the remote host in the `%systemroot%\temp` directory. Veritas Operations Manager copies the file from the host's mapped admin\$ filestore, sends it to Veritas Operations Manager Control Host, and deletes the file from the remote host.

To perform this discovery process, Veritas Operations Manager requires a local administrator account for the remote host.

Veritas Operations Manager cannot perform agentless discovery of a Windows host from a Solaris Control Host.

[Figure 7-4](#) depicts how Veritas Operations Manager performs agentless discovery of Windows hosts.

Figure 7-4 Agentless discovery of Windows hosts



See [“About agentless discovery of remote hosts”](#) on page 123.

Requirements for agentless discovery of UNIX hosts

[Table 7-3](#) lists the requirements for agentless discovery of UNIX hosts.

Table 7-3 Requirements for agentless discovery of UNIX hosts

Requirement	Description
A user account	■ The minimum requirement is a non-root user account. ■ Symantec requires privileged access to discover some information. You can use privilege control software to designate privileged access to a specific user for specific commands. See “Commands that require the root access for agentless discovery of UNIX hosts” on page 130. See “Using the privilege control software with agentless discovery of UNIX hosts” on page 132.
Network access between hosts	Ensure there is network access between the host that you want to discover and Veritas Operations Manager Control Host that performs discovery. UNIX agentless discovery requires contacting SSH running on TCP port 22 on the remote host. TCP port 22 should be open in both directions between the Control Host and the remote host.
Persistent binding for Solaris 9 hosts	Enable persistent binding if you want Veritas Operations Manager to discover the storage that is allocated to a Solaris 9 host.
A shell on the remote host	Veritas Operations Manager requires a shell on the remote host (sh, ksh, or bash) that accepts sh file redirection.

Table 7-3 Requirements for agentless discovery of UNIX hosts (*continued*)

Requirement	Description
Secure Shell (SSH) on the remote host	To communicate between the Veritas Operations Manager host and remote UNIX hosts, Veritas Operations Manager uses the non-keyboard interactive, password-based authentication of SSH. Ensure that: ■ SSH is installed. The SSH package is typically installed by default; however, it may not be present if a minimal operating system installation was performed. If the SSH package is not present, use the operating system installer to install SSH, or download and install OpenSSH. See “About installing OpenSSH on a UNIX host” on page 135. ■ SSH is set up properly. See “SSH configuration requirements for agentless discovery” on page 133. ■ SunSSH is version 1.1 (Sun_SSH_1.1) or higher on Solaris 9 hosts. If a Solaris 9 host runs version 1.0 (Sun_SSH_1_0), network communication between Veritas Operations Manager and the Solaris 9 host may terminate during agentless configuration and discovery. ■ OpenSSH is not version 0.9.8e or 0.9.7e on AIX, Linux, and Solaris hosts. These versions have known AES encryption issues, which can cause a warning.

See [“How agentless discovery of a UNIX or Linux host works”](#) on page 124.

Requirements for agentless discovery of Windows hosts

[Table 7-4](#) lists the requirements for agentless discovery of Windows hosts

Table 7-4 Requirements for agentless discovery of Windows hosts

Requirement	Description
A user account	Veritas Operations Manager requires a local administrator account for the remote host.
Network access between hosts	Ensure there is network access between the host that you want to discover and Veritas Operations Manager Control Host that performs discovery.

Table 7-4 Requirements for agentless discovery of Windows hosts (*continued*)

Requirement	Description
Windows Management Instrumentation (WMI)	WMI is installed as part of the Windows operating system. Ensure that the WMI service is enabled on the Veritas Operations Manager host that performs discovery and on the remote host that you want to discover.
Port 135 opened	Open TCP port 135 on the remote host that you want to discover and the host that performs discovery (Control Host). WMI uses port 135 to communicate between the hosts.
A Windows Management Server or Control Host	Veritas Operations Manager cannot perform agentless discovery of a Windows host from a Solaris Management Server or Control Host. Initiate discovery from a Windows Control Host if you want to discover a Windows host and do not have a Windows Management Server.
User Account Control (UAC) turned off on a Windows 2008 host	Disable User Account Control on Veritas Operations Manager Control Host that initiates agentless discovery, if the host runs Windows 2008. For information about how to turn off UAC, see the section titled "Turning off UAC" at the following URL: http://technet.microsoft.com/en-us/library/cc709691(WS.10).aspx
Microsoft's Fibre Channel Information Tool installed on Windows 2003 hosts	Install Microsoft's Fibre Channel Information Tool (fcinfo) on Windows 2003 hosts that you want to discover. This tool is required only if you want Veritas Operations Manager to discover information about the host's Fibre Channel (FC) hardware (HBAs and Fibre Channel LUNs). For example, the tool is not necessary if you want to discover a VMware Windows guest operating system. FC discovery is not possible for VMware guest operating systems. You can download the tool from the following location: www.microsoft.com/downloads/details.aspx?FamilyID=73d7b879-55b2-4629-8734-b0698096d3b1&displaylang=en

See ["How agentless discovery of a Windows host works"](#) on page 125.

Requirements for deep array discovery for agentless hosts

The following list provides requirements for deep array discovery for agentless hosts:

- You must have the Storage Insight Add-on deployed to correlate OSHandles on the agentless host with array LUNs.
- After making masking changes to make new LUNs visible to a host, you must wait for the next scheduled Storage Insight deep array discovery and then either perform a manual refresh or wait for the next scheduled discovery of the agentless host.

For VMware environments, when you make new LUNs visible to the ESX server, you must wait for the next scheduled Storage Insight deep array discovery, either perform a manual refresh or wait for the next scheduled discovery of the agentless host, and then either perform a manual refresh or wait for the next scheduled discovery of vCenter.

These requirements apply to both UNIX and Windows agentless hosts.

See [“About agentless discovery of remote hosts”](#) on page 123.

See [“Prerequisites for agentless configuration”](#) on page 124.

Commands that require the root access for agentless discovery of UNIX hosts

Veritas Operations Manager requires a user account to perform agentless discovery of a remote UNIX host. The minimum requirement is a non-root user account. However, there are a few cases where Veritas Operations Manager requires a root user account.

[Table 7-5](#) identifies the commands that require root access.

Table 7-5 Commands that require root access for agentless discovery

Resource	Operating system	Command	Purpose	Requirement ¹
VMware BIOS UUID	Linux (VMWare Guest OS)	/usr/sbin/dmidecode	Provides the VMware BIOS UUID for the virtual machine.	Mandatory (for VMware guests only)
Disks	HP-UX	/usr/sbin/diskinfo	Provides the device handles for disks.	Mandatory

Table 7-5 Commands that require root access for agentless discovery
(continued)

Resource	Operating system	Command	Purpose	Requirement ¹
EMC PowerPath	AIX, HP-UX, Linux, and Solaris	AIX: /usr/sbin/powermt check_registration HP-UX: /sbin/powermt check_registration Linux: /sbin/powermt check_registration Solaris: /etc/powermt check_registration	Provides the license-related information.	Mandatory
		Linux: /usr/sbin/powermt display dev=all HP-UX: /sbin/powermt display dev=all Linux: /sbin/powermt display dev=all Linux: /etc/powermt display dev=all	Provides the paths and their status details.	Mandatory
HBAs or target ports	Solaris	fcinfo	Provides the Fibre Channel-related details regarding HBA, HBA port WWNs, etc.	Optional
	HP-UX	/opt/fcms/bin/ fcmsutil		Mandatory
Linux LVM	Linux	vgdisplay -v --units b	Provides the volume-related details for all volumes.	Mandatory
		lvdisplay -m --units b	Provides the volume-related details for all volumes.	Mandatory
Linux DM Multipath	Linux	/sbin/multipath	Provides the paths and their status details.	Mandatory (for Linux hosts having DM multipath configuration)

¹ Mandatory indicates that the specified part of feature discovery fails if you do not provide root access for the command. Optional indicates that most of the feature

discovery works even if you do not provide root access for the command. The mandatory commands for a given OS platform need not be enabled in the privilege control software if the host does not have the utilities installed on it

See [“How agentless discovery of a UNIX or Linux host works”](#) on page 124.

See [“Requirements for agentless discovery of UNIX hosts”](#) on page 126.

Using the privilege control software with agentless discovery of UNIX hosts

Veritas Operations Manager requires a user account to perform agentless discovery of a remote UNIX host. The minimum requirement is a non-root user account. However, there are a few instances where Veritas Operations Manager requires a root user account.

See [“Commands that require the root access for agentless discovery of UNIX hosts”](#) on page 130.

To discover that information, you can configure Veritas Operations Manager to use one of the following:

- A root user account.
- A non-root user account and use privilege control software to grant that user the ability to run specific commands.

Veritas Operations Manager supports the following privilege control software with agentless discovery:

- PowerBroker
- Privilege Manager for UNIX
- Sudo

[Table 7-6](#) identifies how you can use privilege control software with agentless discovery.

Table 7-6 Using privilege control software with agentless discovery of UNIX hosts

Step	Action
1	Install the privilege control software on the remote host that you want to discover.

Table 7-6 Using privilege control software with agentless discovery of UNIX hosts (*continued*)

Step	Action
2	Modify the configuration file for the privilege control software as follows: ■ Add the user name that you want to use for agentless discovery. ■ Add the commands that you want to allow the user to run. ■ Ensure that the software does not require a TTY session for commands to succeed. ■ Ensure that the software does not require a password when running a command. ■ Ensure that the user has the privilege to kill the commands that are initiated with the privilege control software. Symantec recommends this privilege because it gives the non-root user the ability to kill any commands that hang when run through the privilege control software.
3	Configure agentless discovery of hosts. See “Adding the managed hosts to Management Server using an agent configuration” on page 138. See “Adding the managed hosts to Management Server using an agentless configuration” on page 140.

See [“Requirements for agentless discovery of UNIX hosts”](#) on page 126.

See [“How agentless discovery of a UNIX or Linux host works”](#) on page 124.

SSH configuration requirements for agentless discovery

Veritas Operations Manager uses SSH to perform agentless discovery of UNIX hosts. The configuration file `sshd_config` defines SSH configuration. The file is located in `/etc/ssh` or in `/opt/etc/ssh`.

[Table 7-7](#) lists the requirements for SSH and the associated parameters that are defined in `sshd_config`.

Table 7-7 Requirements for SSH

Requirement	Parameter(s)	Comments
The SSH port is open for the user account that you use for discovery	Port	The port must be set to 22. Agentless configuration does not support the specification of the SSH port.
SSH allows password-based authentication	PasswordAuthentication	To allow password-based authentication, set the parameter to yes .
SSH allows access for the root user	PermitRootLogin	Root user logon is required only if you use a root account for discovery. To allow logons by the root user, set the <code>PermitRootLogin</code> parameter to yes .
SSH allows access for the user account that you use for discovery	■ <code>AllowUsers</code> If you use this parameter, ensure that it allows the user account that you use for agentless discovery. ■ <code>DenyUsers</code> If you use this parameter, ensure that it does not deny the user account that you use for agentless discovery. ■ <code>AllowGroups</code> If you use this parameter, ensure that it allows the group to which the user account belongs. ■ <code>DenyGroups</code> If you use this parameter, ensure that it does not deny the group to which the user account belongs.	By default, SSH does not restrict user logons. However, you may have setup SSH to restrict access. If you use parameters to restrict access, ensure that they do not block access by the user account that you use for discovery.

For more information about `sshd_config`, refer to your system documentation.

See [“About agentless discovery using the Control Host”](#) on page 123.

See [“About agentless discovery of remote hosts”](#) on page 123.

About installing OpenSSH on a UNIX host

The SSH package may not be present on a UNIX host. If SSH is not present, you can either use the operating system installer to install SSH, or you can download and install OpenSSH. OpenSSH is a free, open-source version of SSH.

See “[Installing OpenSSH on AIX](#)” on page 135.

See “[Installing OpenSSH on Linux](#)” on page 135.

See “[Installing OpenSSH on Solaris](#)” on page 136.

Installing OpenSSH on AIX

AIX includes OpenSSH. You may also download OpenSSH.

To install OpenSSH on AIX

- 1 For AIX 5.2 or earlier, download OpenSSL from the AIX Toolbox page on the IBM Web site:

https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=aixtbx&S_PKG=dlaixww&S_TACT=&S_CMP=

For AIX 5.3 or later, download the OpenSSL install package from the AIX Web Download Pack Programs page on the IBM Web site:

<https://www14.software.ibm.com/webapp/iwm/web/reg/pick.do?source=aixbp>

- 2 Install OpenSSL.
- 3 Download OpenSSH from the following location:
<http://sourceforge.net/projects/openssh-aix/files>

- 4 Install OpenSSH.

See “[About installing OpenSSH on a UNIX host](#)” on page 135.

Installing OpenSSH on Linux

Most Linux distributions include OpenSSH. You may also download OpenSSH. On Linux, the following OpenSSH packages are required:

- openssl-0.9.8b-8.3.e15.i386.rpm
- openssh-4.3p2-16.e15.i386.rpm
- openssh-server-4.3p2-16.e15.i386.rpm

To install OpenSSH on Linux

- 1 For Red Hat, download the OpenSSH packages from the following location:

<http://www.redhat.com>

For other Linux distributions, download the OpenSSH packages from the following location:

<http://rpm.pbone.net>

- 2 Run the following command to install the OpenSSH packages:

```
# rpm -ivh openssh-4.3p2-16.e15.i386.rpm  
openssh-server-4.3p2-16.e15.i386.rpm
```

See “About installing OpenSSH on a UNIX host” on page 135.

Installing OpenSSH on Solaris

On Solaris 10, SSH is installed by default. There is no need to install SSH manually.

On Solaris 9, the easiest way to install OpenSSH is to download and install the precompiled packages from Sunfreeware.com. The following OpenSSH packages are required:

- GNU Compiler
- Zlib
- OpenSSL
- OpenSSH

To install OpenSSH on Solaris 9

- 1 Download the OpenSSH packages from the following locations.

- GNU Compiler
<ftp://ftp.sunfreeware.com/pub/freeware/sparc/9/libgcc-3.4.6-sol9-sparc-local.gz>
- Zlib
<ftp://ftp.sunfreeware.com/pub/freeware/sparc/9/zlib-1.2.3-sol9-sparc-local.gz>
- OpenSSL
<ftp://ftp.sunfreeware.com/pub/freeware/sparc/9/openssl-0.9.8i-sol9-sparc-local.gz>
- OpenSSH

<ftp://ftp.sunfreeware.com/pub/freeware/sparc/9/openssh-5.3p1-sol9-sparc-local.gz>

- 2 Unzip the packages and install the files using the following commands:

For the GNU Compiler:

```
# gunzip libgcc-3.4.6-sol9-sparc-local.gz
# pkgadd -d libgcc-3.4.6-sol9-sparc-local
```

For Zlib:

```
# gunzip zlib-1.2.3-sol9-sparc-local.gz
# pkgadd -d zlib-1.2.3-sol9-sparc-local
```

For OpenSSL:

```
# gunzip openssl-0.9.81-sol9-sparc-local.gz
# pkgadd -d openssl-0.9.81-sol9-sparc-local
```

For OpenSSH:

```
# gunzip openssh-5.3p1-sol9-sparc-local.gz
# pkgadd -d openssh-5.3p1-sol9-sparc-local
```

- 3 Set up the /var/empty directory by running the following commands:

```
# mkdir /var/empty
# chown root:sys /var/empty
# chmod 775 /var/empty
```

- 4 Add the user sshd by running the following command:

```
# useradd -g sshd -c 'sshd Privsep' -d /var/empty -s /bin/false
sshd
```

- 5 Edit the default /user/local/sshd_config file.

Replace these lines:

```
Subsystem sftp /user/libexec/sftp-server
PermitRootLogin no
```

with:

```
Subsystem sftp /user/local/libexec/sftp-server
PermitRootLogin yes
```

- 6 Generate keys for the server by running the following commands:

```
# ssh-keygen -t rsa1 -f /usr/local/etc/ssh_host_key -N ""
# ssh-keygen -t dsa -f /usr/local/etc/ssh_host_dsa_key -N ""
# ssh-keygen -t rsa -f /usr/local/etc/ssh_host_rsa_key -N ""
```

- 7 Start SSHD by running the following command:

```
# nohup /usr/local/sbin/sshd &
```

See [“About installing OpenSSH on a UNIX host”](#) on page 135.

Adding the managed hosts to Management Server using an agent configuration

In the Management Server console, you can add a new managed host to Management Server using an agent configuration.

Note: Veritas Operations Manager does not support adding a managed agent host to Management Server if the version of the managed agent host is newer than the version of Management Server. However, Veritas Operations Manager does not display any error messages when you perform this task.

Before you add a managed agent host to the Management Server, make sure that the managed agent host can communicate with the Management Server. The time difference between the system clocks on the Management Server and managed host should not be more than 90 minutes.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective. The root user can also perform this task.

To add a managed host to Management Server using an agent

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Do one of the following:
 - Click **Add Hosts > Agent**.
 - In the **Settings** tab click **Host**. Click **Add Hosts > Agent**.
- 3 In the **Add agent hosts** wizard panel, enter the host details, and click **Finish**.
See [“Add agent hosts panel options”](#) on page 139.
- 4 In the **Result** panel, verify that the host has been added successfully. Click **OK**.

To add multiple managed hosts to Management Server using the CSV file

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Do one of the following:
 - Click **Add Hosts > Agent**.
 - In the **Settings** tab click **Host**. Click **Add Hosts > Agent**.
- 3 In the **Add agent hosts** wizard panel, under **Advance**, click **Browse** to select the CSV file.
- 4 Click **Import selected file** and click **Finish**.
- 5 In the **Result** panel, verify that the host has been added successfully. Click **OK**.

See [“Adding the managed hosts to Management Server using an agentless configuration”](#) on page 140.

See [“Adding managed hosts to Management Server using the Auto Configure \(gendeploy.pl\) script”](#) on page 143.

See [“Refreshing the details of the managed host”](#) on page 146.

See [“Removing managed hosts from the Management Server domain”](#) on page 147.

Add agent hosts panel options

Use this wizard panel to specify options to add a managed host to Management Server using an agent configuration.

Table 7-8 Add agent hosts panel options for agent configuration

Field	Description
Add entry	Select to manually specify more than one host to add.
Host Name	Enter host name or IP address that you can use to reach the managed host from Management Server.
User Name	Enter the root or administrator user name for the host.
Password	Enter the root or administrator password to log on to the managed host.

Under **Advanced** you can add multiple hosts by importing the information from a comma-separated (.csv) file from a specified location. The CSV file must include

the “.csv” extension. You can use the manual host specification and the CSV file simultaneously to add hosts.

The following is an example of a CSV file that includes user names and passwords for each host:

```
Host,User,Password
host1.abc.com,username1,password1
host2.abc.com,username2,password2
```

The first line in the CSV file must appear as above. You can replace the subsequent lines with your hosts, user names, and passwords.

See [“Adding the managed hosts to Management Server using an agent configuration”](#) on page 138.

Adding the managed hosts to Management Server using an agentless configuration

In the Management Server console, you can add a new managed host to Management Server using an agentless configuration.

Before you add a managed agent host to the Management Server, make sure that the managed agent host can communicate with the Management Server.

You can convert an agentless host to an agent host by installing the Veritas Operations Manager agent on the host and then add the host using the **Add agent host** wizard. You do not need to remove the host from the Management Server domain.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective. The root user can also perform this task.

To add a managed host to Management Server using an agentless configuration

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Do one of the following:
 - Click **Add Hosts > Agentless**.
 - In the **Settings** tab click **Host**. Click **Add Hosts > Agentless**.
- 3 In the **Add agentless hosts** wizard panel, enter the host details, and click **Finish**.

See [“Add agentless hosts panel options”](#) on page 141.
- 4 In the **Result** panel, verify that the host has been added successfully. Click **OK**.

To add multiple managed agentless hosts to Management Server using the CSV file

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Do one of the following:
 - Click **Add Hosts > Agents**.
 - In the **Settings** tab click **Host**. Click **Add Hosts > Agentless**.
- 3 In the **Add agentless host** wizard panel, under **Advance**, click **Browse** to select the .csv file.
- 4 Click **Import selected file** and click **Finish**.
- 5 In the **Result** panel, verify that the host has been added successfully. Click **OK**.

See [“Adding the managed hosts to Management Server using an agent configuration”](#) on page 138.

See [“Adding managed hosts to Management Server using the Auto Configure \(gendeploy.pl\) script”](#) on page 143.

See [“Refreshing the details of the managed host”](#) on page 146.

See [“Removing managed hosts from the Management Server domain”](#) on page 147.

Add agentless hosts panel options

Use this wizard panel to specify options to add a managed host to Management Server using agentless configuration.

The **Advanced** option lets you use privilege control software with the agentless discovery of a host. You must specify the type and location of the software on the remote host. The **Advanced** option is optional and is required when adding agentless host discovery for non-root users.

Table 7-9 Add agentless hosts wizard panel options for agentless configuration

Field	Description
Discovery Mode	Lets you filter the Control Host field by discovery mode. SSH should be used for adding UNIX hosts and WMI should be used for adding Windows hosts.

Table 7-9

Add agentless hosts wizard panel options for agentless configuration
(continued)

Field	Description
Control Host	Control Host through which the agentless host is being discovered. Windows agentless hosts can only be discovered by Windows Control Hosts.
Add entry	Select to manually specify more than one host to add.
Host Name	Enter host name or IP address that you can use to reach the managed host from Management Server.
User Name	Enter user name with administrator rights.
Password	Enter password to log on to the managed host.
Advanced	Lets you specify type and location of privilege control software to use on the agentless hosts.

Under **Advanced** you can add multiple hosts by importing the information from a comma-separated (.csv) file from a specified location. The CSV file must include the “.csv” extension. You can use the manual host specification and the CSV file simultaneously to add hosts.

The following is an example of a CSV file that includes user names and passwords for each host:

```
Host,User>Password
host1.abc.com,username1,password1
host2.abc.com,username2,password2
```

The first line in the CSV file must appear as above. You can replace the subsequent lines with your hosts, user names, and passwords.

For agentless configuration, the CSV file cannot contain both UNIX and Windows hosts.

Note: The discovery mode (SSH or WMI) must be consistent with the types of hosts you specify in the CSV file. You must specify SSH for UNIX hosts and WMI for Windows hosts.

See [“Adding the managed hosts to Management Server using an agentless configuration”](#) on page 140.

Adding managed hosts to Management Server using the Auto Configure (gendeploy.pl) script

You can add an agent host to the Management Server domain with minimal user interaction. The Auto Configure (gendeploy.pl) script available on Management Server can be used to create a script that is run on the host to add the host to the domain. You can create the script either at the command prompt, or in the Veritas Operations Manager Management Server console.

Note: You can only add an agent host using the Auto Configure (gendeploy.pl) script. This feature is not applicable for adding agentless hosts.

You need to copy the script that is created using gendeploy.pl to all the hosts that you want to add to the domain. After you copy the script, you have to run it on each host. A host on which you run the script must have the VRTSsfmh package installed on it.

Adding many hosts to Management Server at the same time using the Auto Configure (gendeploy.pl) script can affect the performance of Management Server. It is recommended that you add no more than 50 agent hosts at a time.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective. The root user can also perform this task.

To add an agent host to Management Server using the Auto Configure (gendeploy.pl) script

- 1 Create the script to add an agent host using either the command prompt, or the console. Do one of the following:
 - In the Home page on the Management Server console, click **Settings**. Click **Auto Configure**. In the **Auto Configure** wizard, click **Download**. In the **File Download** dialog, click **Save** to save the script to the required location.
 - Create the script using command prompt.
 - On Linux Management Server, log on as root.
Run the following command:

```
/opt/VRTSsfmh/bin/gendeploy.pl --out filename [--domain sfm:domainname:port]
```

where, *filename* is the name of the script that you specify. The *domainname* is the Management Server host name.

For example,

```
/opt/VRTSsfmh/bin/gendeploy.pl --out test.pl --domain
sfm://Managementserver.domain.com:5634
```

In this example, the domain name is the Management Server name, or the domain that is hosted by Management Server.

- On Windows Management Server, log on as a user with the administrator privileges.

To change the directory, run the following command at the command prompt:

```
cd "C:\Program Files\Veritas\VRTSsfmh\bin"
```

To create the script to add an agent host, run the following command:

```
perl.exe gendeploy.pl --out <filename> [--domain
<sfm:domainname:port>]
```

where, *filename* is the name of the script that you specify. The *domain name* is the Management Server host name.

For example, `perl.exe gendeploy.pl --out test.pl [--domain sfm://Managementserver.domain.com:5634]`

In this example, the domain name is the Management Server name, or the domain that is hosted by the Management Server.

- 2 Copy the script to the agent host.
- 3 On the agent host, change the directory to the location where you copied the script.
- 4 Do one of the following:

- On UNIX-based hosts, run the following command to make the script executable:

```
chmod +x filename
```

where, *filename* is the name of the script.

Run the script:

```
./filename
```

- On Windows-based hosts, run the following command:

```
"C:\Program Files\Veritas\VRTSsfmh\bin\perl.exe" filename
```

where, *filename* is the name of the script.

For the above script, the optional hostname parameter is the host as seen by the Management Server. The host is discovered by this name or IP address in Veritas Operations Manager.

- 5 In the console, verify that the agent host has been added to the Management Server domain.

See [“Adding the managed hosts to Management Server using an agent configuration”](#) on page 138.

See [“Adding the managed hosts to Management Server using an agentless configuration”](#) on page 140.

See [“Adding managed hosts to Management Server using the Auto Configure \(gendeploy.pl\) script”](#) on page 143.

See [“Refreshing the details of the managed host”](#) on page 146.

See [“Removing managed hosts from the Management Server domain”](#) on page 147.

Editing the agentless host configuration

To edit the details of an agentless host, you can use the **Edit agentless configuration** option.

The **Advanced** option lets you use privilege control software with the agentless discovery of a host. You must specify the type and location of the software. The **Advanced** option is optional and is required while configuring agentless host discovery for non-root users.

The edit operation for agentless hosts is asynchronous. The wizard displays that the operation has triggered the edit, but the discovery operation for the agentless host is actually in progress in the background. You must wait for the actual discovery to complete.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective. The root user can also perform this task.

To edit the details of an agentless host

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Host**.
- 3 Expand **Agentless** to locate the host.
- 4 Right-click in the details list and select **Edit agentless configuration**.

- 5 In the **Edit agentless configuration** wizard panel, edit the host details, and click **Finish**.
 See [“Edit agentless host panel options”](#) on page 146.
- 6 In the **Result** panel, verify that the host has been modified successfully. Click **OK**.
 See [“Using the privilege control software with agentless discovery of UNIX hosts”](#) on page 132.
 See [“Adding the managed hosts to Management Server using an agentless configuration”](#) on page 140.

Edit agentless host panel options

Use this wizard panel to edit the details of configured agentless hosts.

Table 7-10 Edit agentless host wizard panel options for agentless configuration

Field	Options
Host	Displays the host name or IP address that you can use to reach the managed host from Management Server.
User name	Modify the user name. User name must have administrative privileges to log-in to the hosts.
Password	Modify the password to log on to the managed host.
Advanced	Modify the type and location of privilege control software to use on the agentless host.

- See [“Editing the agentless host configuration”](#) on page 145.
- See [“Adding managed hosts to Management Server using the Auto Configure \(gendeploy.pl\) script”](#) on page 143.

Refreshing the details of the managed host

You can use the Management Server console to refresh the discovery of the agent families on both managed agent and agentless hosts. You can also perform this task in the **Hosts** details view in the **Server** perspective.

To refresh more than one managed host, press **Ctrl** as you select hosts from the list.

The refresh operation for agentless hosts is asynchronous. The wizard displays that the operation has triggered the refresh, but the discovery operation for the agentless host is actually in progress in the background. You must wait for the actual discovery to complete. When it is complete, you can view the status reflected in the **State** column if you are in the Server perspective. If you are in the Management Server perspective, click **Host** and view the status in the **Discovery State** column.

To perform this task in the Server perspective, your user group must be assigned the Admin role on the host or the Server perspective. The permission on the host may be explicitly assigned or inherited from a parent Organization.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To refresh the details of a managed host

- 1 In the Home page on the Management Server console, do one of the following:
 - Go to the **Server** perspective and select **Manage** in the left pane. Expand the Organization or **Uncategorized Hosts** to locate the host.
 - Click **Settings**. Click **Host** to locate the host.
- 2 Right-click the managed host and select **Refresh**.
- 3 In the **Refresh Hosts** wizard panel review the managed host and click **Yes**.
- 4 In the **Result** panel click **OK**.

See [“Adding the managed hosts to Management Server using an agent configuration”](#) on page 138.

See [“Adding the managed hosts to Management Server using an agentless configuration”](#) on page 140.

See [“Adding managed hosts to Management Server using the Auto Configure \(gendeploy.pl\) script”](#) on page 143.

See [“Removing managed hosts from the Management Server domain”](#) on page 147.

See [“Verifying the version of a managed host in the console”](#) on page 67.

Removing managed hosts from the Management Server domain

You can dissociate the managed hosts from Management Server and remove the managed hosts from the data center using the Management Server console. To remove more than one managed host, press **Ctrl** as you select hosts from the list.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective. The root user can also perform this task.

To remove managed hosts from the Management Server domain

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Host**.
- 3 Right-click the managed host and select **Remove**.
- 4 In the **Remove Hosts** wizard panel review the managed host and click **Yes**.
- 5 In the **Result** panel click **OK**.

See [“Adding the managed hosts to Management Server using an agent configuration”](#) on page 138.

See [“Adding the managed hosts to Management Server using an agentless configuration”](#) on page 140.

See [“Adding managed hosts to Management Server using the Auto Configure \(gendeploy.pl\) script”](#) on page 143.

See [“Refreshing the details of the managed host”](#) on page 146.

Setting up user access

This chapter includes the following topics:

- [About managing authentication brokers and authentication domains in the Veritas Operations Manager domain](#)
- [Configuring Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server](#)
- [Unconfiguring Lightweight Directory Access Protocol or Active Directory configuration from the authentication broker](#)
- [About predefined roles in Veritas Operations Manager](#)
- [About Organizations, objects, and roles in Veritas Operations Manager](#)
- [Assigning permissions to user groups for a perspective](#)
- [Modifying permissions assigned to user groups for a perspective](#)
- [Deleting permissions assigned to user groups on a perspective](#)
- [Restricting users or user groups from accessing the Veritas Operations Manager console](#)
- [Example: Managing user access in Veritas Operations Manager using Organizations and existing user groups](#)

About managing authentication brokers and authentication domains in the Veritas Operations Manager domain

An authentication broker is an intermediate registration and certification authority that can authenticate clients including users or services.

In Veritas Operations Manager there is a primary authentication broker which is associated with one or more authentication domains that authenticate users. The primary authentication broker is installed on Management Server. The authentication broker is configured automatically during the Management Server configuration. You cannot add more than one authentication broker.

You can also manage the authentication domains that are associated with authentication brokers 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+. In addition to the native operating system authentication, Veritas Operations Manager supports Lightweight Directory Access Protocol (LDAP) and Active Directory (AD).

Veritas Operations Manager authentication has no ability to interact with RSA or other secondary authentication interfaces like proxy, VPN, Kerberos, (where the subscriber must request and receive an encrypted security token that can be used to access a particular service), Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+), DS3, smartcard, or other multifactor authentication methods.

You can view the following authentication domain types on the Veritas Operations Manager log in page:

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

To assign permissions to user groups within perspectives, you need to configure LDAP or AD domain.

If you unconfigure the LDAP or AD domain, the permissions that are assigned to user groups on the perspectives are deleted.

To manage the authentication domains, your user group must be assigned the Admin role on the Management Server perspective.

See [“Configuring Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server”](#) on page 151.

See [“Unconfiguring Lightweight Directory Access Protocol or Active Directory configuration from the authentication broker”](#) on page 156.

See [“Assigning permissions to user groups for a perspective”](#) on page 158.

Configuring Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server

You can configure Lightweight Directory Access Protocol (LDAP) or Active Directory (AD)-based authentication on the primary authentication broker.

By default, the LDAP or AD-based authentication domain that you configure is in the enabled state.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To configure LDAP or AD-based authentication

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Do one of the following:
 - Click **Configure LDAP/AD**.
 - Click **Security**. In the **Brokers & Domains** tab, click **Configure LDAP/AD**.
- 3 In the **Configure LDAP/AD** wizard panel, enter the details, and click **Next**.
See [“Configure LDAP/AD panel options”](#) on page 151.
- 4 In the **Configure LDAP/AD** wizard panel, enter a domain name, specify the search base, and click **Finish**.
See [“Configure LDAP/AD panel options to specify the domain name”](#) on page 154.
- 5 In the **Configure LDAP/AD** panel that confirms that you have configured LDAP or AD-based authentication, click **OK**.

See [“About managing authentication brokers and authentication domains in the Veritas Operations Manager domain”](#) on page 149.

See [“Unconfiguring Lightweight Directory Access Protocol or Active Directory configuration from the authentication broker”](#) on page 156.

Configure LDAP/AD panel options

Use this wizard panel to start configuring LDAP or AD-based authentication on the primary authentication broker.

Table 8-1 LDAP/AD options

Field	Description
Server Information	
Server Name (Mandatory)	Enter the fully-qualified host name or IP address of the LDAP server. If a secure session is configured with the LDAP server using SSL certificates, you must enter the fully-qualified host name that matches with the fully-qualified host name in the LDAP server certificate
Port (Mandatory)	Displays the number of the port on which the LDAP server is configured to run. By default, this field displays the port number as 389. You can edit this port number, if required.
Verify Server	Click to verify the server name and check whether the server requires you to log on or use the SSL certificate.
This server requires me to log on (Optional)	Select this check box if the anonymous operations are disabled on the LDAP server and a bind user ID is required to proceed with configuring the LDAP-based authentication

Table 8-1 LDAP/AD options (*continued*)

Field	Description
Bind User Name/DN	Enter the complete Distinguished Name (DN) of the user that is used to bind to the LDAP server. If the LDAP server being used is Active Directory (AD), you can provide the DN in any of the following formats: ■ <code>username@domainname.com</code> ■ <code>domainname\username</code> For example, You can provide the DN as <code>Administrator@enterprise.domainname.com</code> <code>ENTERPRISE\Administrator</code> For RFC 2307 compliant LDAP servers, specify complete bind DN. For example, cn=Manager,dc=vss,dc=symantec,dc=com The LDAP or the AD administrator can provide you the bind user name that you can use.
Password	Enter the password that is assigned to the bind user name that you use.
Use Secure Sockets Layer	Select this check box to use the Secure Sockets Layer (SSL) certificates to establish a secure channel between the authentication broker and the LDAP server.
Certificate location	Enter the location of the trusted root CA certificate of the vendor that issued the LDAP server certificate.
Query Information	

Table 8-1 LDAP/AD options (*continued*)

Field	Description
User Name (Mandatory)	Enter the user name based on which the system detects the LDAP server-related settings. Note: Ensure that the user name does not contain any special characters. The system determines the search base based on the user name that you specify in this field.
Group Name	Enter the name of the user group based on which the system detects the LDAP server-related settings. Note: Ensure that the group name does not contain any special characters. Veritas Operations Manager displays this field if the user does not belong to any user groups. The system determines the search base based on the group name along with the user name that you have specified.

See [“Configuring Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server”](#) on page 151.

Configure LDAP/AD panel options to specify the domain name

Use this wizard panel to specify the Domain Name and the Search Base to configure Lightweight Directory Access Protocol (LDAP) based authentication on the primary authentication broker.

Table 8-2 LDAP/AD options

Field	Description
Server Name	Displays the fully-qualified host name or IP address of the LDAP server that you have specified in the LDAP/AD wizard panel.

Table 8-2 LDAP/AD options (*continued*)

Field	Description
Domain Name	Enter a unique name to identify the LDAP-based authentication that you configure on the primary authentication broker. You can enter up to 32 characters.
Search Base	
Use Default	Select this option if you want to use the default search base that the system has detected using the information that you have specified on the LDAP/AD wizard panel.
Custom	Select this option to specify the search base other than the default search base. For example, you can customize the search base as follows to authenticate the user (sampleuser) who belongs to the organization (ou=HR), which is an organization unit under ou=user The organization structure is given below: <pre>ou=HR,ou=People,dc=veritas,dc=com -sampleuser ou=Engg,ou=People,dc=veritas,dc=com -Eng1</pre> The default search base is ou=HR,ou=People,dc=veritas,dc=com To authenticate users under ou=HR and ou=Engg, set custom search base to a level up: ou=People,dc=symantec,dc=com

See [“Configuring Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server”](#) on page 151.

Unconfiguring Lightweight Directory Access Protocol or Active Directory configuration from the authentication broker

You can remove or unconfigure Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) configuration from the primary authentication broker using the Management Server console.

The permissions assigned to user groups within perspectives are deleted when you remove LDAP or AD configuration.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To unconfigure LDAP or AD configuration from the primary authentication broker

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Security**.
- 3 In the **Brokers & Domains** tab, right-click the authentication domain that you have configured as LDAP or AD, and select **Unconfigure**.
- 4 In the **Unconfigure** panel review the information, and click **OK**.

See [“About managing authentication brokers and authentication domains in the Veritas Operations Manager domain”](#) on page 149.

See [“Viewing the details of the authentication broker and the domains associated with the broker”](#) on page 236.

See [“Configuring Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server”](#) on page 151.

About predefined roles in Veritas Operations Manager

Veritas Operations Manager has three predefined roles: Admin, Operator, and Guest. Veritas Operations Manager makes use of the existing user groups within the Active Directory or in the native operating system such as Windows or UNIX. A user group is assigned a role on the perspective or an Organization within a perspective.

A user group with Admin role on a perspective can perform tasks such as creating and assigning permissions to an Organization, along with other tasks that are relevant in the perspective. A user group with Guest role can only view the information displayed in the perspective. Only Admin role can be assigned to a user group in the **Management Server** perspective.

Operator role is available only in the **Availability** perspective. A user group with operator role can perform operations such as taking a service group online or offline, freezing or unfreezing service groups, or running the high availability and disaster recovery fire drill.

See [“About Organizations, objects, and roles in Veritas Operations Manager”](#) on page 157.

See [“Assigning permissions to user groups for a perspective”](#) on page 158.

About Organizations, objects, and roles 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. To create an Organization, your user group must have the Admin role on the perspective. The objects within the Organization may or may not represent the physical organization of the objects in the actual data center.

Multiple Organizations can be created in a perspective and user permissions can be assigned to each Organization. For example, a group of users can have Admin role on an Organization having Windows hosts, and Guest role for an Organization having Linux hosts.

You can also create unlimited number of nested Organizations. An Organization defined in one perspective is not available in another perspective.

For more information on creating Organizations, refer to the *Veritas Operations Manager Management Server User Guide*.

[Table 8-3](#) lists the objects in each perspective which can be grouped to form an Organization.

Table 8-3 Objects for creating Organizations

Perspective	Object
Server	Hosts
Availability	Clusters
Storage	Enclosures
Virtualization	Virtualization servers

The objects within an Organization inherit the permissions assigned to the Organization. To assign exclusive user permissions on the objects within the Organization, you need to modify the permissions on the individual object.

For example, an Organization named Windows in the Server perspective has five hosts. By default, the hosts inherit the permissions assigned to the Organization. User permissions can be modified on each of the five hosts.

User permissions can be assigned to the following objects in a perspective:

Table 8-4 Objects within an Organization

Perspective	Object
Server	Hosts
Availability	Clusters and service groups
Storage	Enclosures
Virtualization	Virtualization servers

See [“About predefined roles in Veritas Operations Manager”](#) on page 156.

See [“Assigning permissions to user groups for a perspective”](#) on page 158.

Assigning permissions to user groups for a perspective

Veritas Operations Manager makes use the existing user groups which are present in the Active Directory or in the native operating system such as Windows or UNIX. The root user can assign permissions such as Admin or Guest to the user groups for a perspective.

For the **Availability** perspective, the root user can also assign the Operator role. The user groups having the Operator role can perform operations such as taking a service group online or offline, freezing or unfreezing a service group, or running the high availability and disaster recovery fire drill.

To assign permissions to user groups for a perspective, your user group must have the Admin role assigned on the **Management Server** perspective. The root user can also perform this task.

To assign permissions to user groups for a perspective

- 1 In the Home page on the Management Server console, do one of the following:
 - Click **Settings**. Skip to 2.

- Click on a perspective and expand **Manage** in the left pane. Right-click **Data Center** and select **Properties**. Skip to 4.
 - 2 Click **Security**, and click the **Permissions** tab.
 - 3 Select a perspective from the drop-down list.
 - 4 Under **Add Permission**, click **Select user group**.
 - 5 In the **Select user group** panel, select the domain, and enter the name of the user group.
The user group name is case-sensitive.
 - 6 Click **Verify user group** and click **OK**.
 - 7 Under **Add Permission**, select a role from the drop-down list. Click **Add**.
See [“About predefined roles in Veritas Operations Manager”](#) on page 156.
 - 8 In the **Success** panel click **OK**.
- See [“Modifying permissions assigned to user groups for a perspective”](#) on page 159.
- See [“Deleting permissions assigned to user groups on a perspective”](#) on page 160.

Modifying permissions assigned to user groups for a perspective

Veritas Operations Manager makes use the existing user groups which are present in the Active Directory or in the native operating system such as Windows or UNIX. The root user can modify permissions assigned to the user groups for a perspective. In case of **Availability** perspective, the root user can also assign the Operator role.

To modify permissions assigned to user groups for a perspective, your user group must have the Admin role assigned on the **Management Server** perspective. The root user can also perform this task.

To modify permissions assigned to user groups for a perspective

- 1 In the Home page on the Management Server console, do one of the following:
 - Click **Settings**. Skip to 2.
 - Click on a perspective and expand **Manage** in the left pane. Right-click **Data Center** and select **Properties**. Skip to 3.
- 2 Click **Security** and click the **Permissions** tab.
- 3 Right-click the user group and select **Modify Role**.

- 4 In the **Modify Role** panel, select a role from the drop-down list, and click **OK**.
 - 5 In the **Modify Role** panel click **Close**.
- See [“About predefined roles in Veritas Operations Manager”](#) on page 156.
- See [“Deleting permissions assigned to user groups on a perspective”](#) on page 160.

Deleting permissions assigned to user groups on a perspective

Using the Management Server console, you can delete the permissions assigned to user groups on a perspective.

To delete permissions assigned to user groups on a perspective, your user group must have the Admin role assigned on the **Management Server** perspective. The root user can also perform this task.

To delete permissions assigned to user groups on a perspective

- 1 In the Home page on the Management Server console, do one of the following:
 - Click **Settings**. Skip to [2](#).
 - Click on a perspective and expand **Manage** in the left pane. Right-click **Data Center** and select **Properties**. Skip to [3](#).
- 2 Click **Security**, and click the **Permissions** tab.
- 3 Right-click the user group and select **Delete**.
- 4 In the **Delete** panel click **OK**.
- 5 In the **Delete - Result** panel click **Close**.

See [“About predefined roles in Veritas Operations Manager”](#) on page 156.

See [“Modifying permissions assigned to user groups for a perspective”](#) on page 159.

Restricting users or user groups from accessing the Veritas Operations Manager console

You can restrict a user or a user group from accessing the Management Server console.

Create a file named `.esmwebdeny` and enter the name of the user or the user group whom you want to restrict in the following format.

- For user: `user name@domain name:user`

Example: Managing user access in Veritas Operations Manager using Organizations and existing user groups

- For user group: *user group name@domain name:group*

User and user group names are case-sensitive only for unixpwd domains, for LDAP, AD, and NT domains they are case insensitive.

Web server restart is not required when the file is created or modified. If the user or the user group is already logged in to the Management Server console, the restrictions will be applicable in the subsequent login session.

Following is an example of a `.esmwebdeny` file that includes the names of users and user groups who are restricted from accessing the Management Server console.

```
firstname1_lastname1@symantecdomain.com:user
firstname2_lastname2@symantecdomain.com:user
alpha_usergroup@symantecdomain.com:group
beta_usergroup@symantecdomain.com:group
```

Place the file at the following location:

- For Linux-based Management Server: `/var/opt/VRTSsfmcs/conf/`
- For Windows-based Management Server (2008/2008 R2):
`C:\ProgramData\Symantec\VRTSsfmcs\conf\`

Precede a comment in the `.esmwebdeny` file with "#".

See [“Configuring Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server”](#) on page 151.

See [“Assigning permissions to user groups for a perspective”](#) on page 158.

See [“Deleting permissions assigned to user groups on a perspective”](#) on page 160.

Example: Managing user access in Veritas Operations Manager using Organizations and existing user groups

As an Administrator you may need to restrict user groups from performing certain tasks on specific objects. Using the Management Server console, you can assign roles to existing user groups on a perspective. Alternately you can also create Organizations in a perspective, and assign roles to user groups on these Organizations. Organizations can be created using hosts, clusters, virtualization servers, and enclosures in Server, Availability, Virtualization, and Storage perspective respectively.

You can create an Organization in one of the following ways:

- Create an empty Organization.
- Create an Organization by manually selecting the objects.

Example: Managing user access in Veritas Operations Manager using Organizations and existing user groups

- Create an Organization by selecting objects based on a rule.

This example explains how you can restrict user groups from performing certain tasks on objects.

You can do any one of the following to restrict access:

- Provide access only to the selected perspective.
- Create an Organization in a perspective, and provide access to the same.
- Provide access to an object within the Organization.

For more information on creating Organizations within a perspective and assigning predefined roles, refer to the *Veritas Operations Manager Management Server User Guide*.

In this example, we use the following names:

Domain	alpha.symantecdomain.com
User group 1	UserGroup_A
User group 2	UserGroup_B
User group 3	Operations_team
Organization 1	Windows_cluster
Organization 2	Linux_cluster
Service group	Beta_SG

Provide access to user groups on a perspective

As an Administrator, you can provide access to user groups on a perspective. Veritas Operations Manager makes use of the existing user groups which are present in Lightweight Directory Access Protocol (LDAP) or Active Directory (AD), or the authentication mechanism in the native operating system of Windows and UNIX. Before you assign permissions to user groups, you need to create user groups in LDAP or AD. Create user groups called UserGroup_A, UserGroup_B, and Operations_team. User group names are case-sensitive.

User groups with Admin role on a perspective can perform all the tasks in that perspective. In addition to the Admin role, Operator role is available only in the Availability perspective. User group with Operator role can perform certain tasks such as onlining and offlining service groups, freezing or unfreezing service groups, clearing faults on service groups or, running the disaster recover fire drill.

A user group having the Guest role on any perspective can only view the information and not perform any task.

Example: Managing user access in Veritas Operations Manager using Organizations and existing user groups

Consider the `Operations_team` user group which is responsible for tasks such as freezing or unfreezing service groups, clearing faults on service groups, running the high availability or disaster recover fire drill. These tasks are performed on the services groups in the Availability perspective. A user group having either Admin or Operator role can perform these tasks. As an Administrator, you can assign the Operator role to `Operations_team`, thereby restricting them from performing other tasks which require Admin role.

Using the Management Server console, you can assign the Operator role on the Availability perspective to the `Operations_team` user group.

To assign Operator role to Operations_team on the Availability perspective

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Security**.
- 3 Click the **Permissions** tab.
- 4 Select **Availability** perspective.
- 5 Under **Add Permission**, click **Select user group**.
- 6 In the **Select user group** panel, select `alpha.symantecdomain.com`, and enter `Operations_team`.
- 7 Verify the user group, and click **OK**.
- 8 Under **Add Permission**, select **Operator** role from the list, and click **Add**.

Create an Organization in a perspective, and provide access to the same

Assigning the Admin role to user groups on a perspective, allows the user groups to perform all tasks on all the objects within the perspective. As an Administrator, you may want to restrict the access to certain objects within the perspective. To do this, you need to create an Organization by grouping the objects. You can then provide appropriate roles to user groups on these Organizations.

For example, in the Availability perspective, you can create an Organization called `Windows_cluster` which consists of all Windows cluster nodes and another called `Linux_cluster` having all Linux cluster nodes. You can assign the clusters to the Organization based on a rule.

To create a Windows_cluster Organization

- 1 In the Home page on the Management Server console, go to Availability perspective and select **Manage** in the left pane.
- 2 Right-click **Data Center** and select **Create Organization**.
- 3 In the **Create Organization** wizard panel, enter `Windows_cluster` in the name field.

- 4 Select **Assign Clusters to Organization Based on Rule**, and click **Next**.
- 5 In the **Create Organization - Based on a rule** wizard panel, do the following:
 - In the **Attribute** list, select **Platform**.
 - In the **Condition** list, select **Is One-of**.
 - In the **Values** list, select **Windows**.
- 6 Click **Finish**.

The rule is applied and all the cluster nodes having Windows platform are moved from Uncategorized Clusters into the Organization named Windows_cluster. When a new Windows cluster node is added to the Management Server domain, it is automatically moved into Windows_cluster Organization.

Similarly you can create another Organization called Linux_cluster for all cluster nodes on Linux platform.

You can now restrict access to these Organizations. You can provide Admin role to UserGroup_A on the Windows_cluster Organization, and UserGroup_B on Linux_cluster.

To assign Admin role to UserGroup_A on Windows_cluster

- 1 In the Home page on the Management Server console, go to Availability perspective and select **Manage** in the left pane.
- 2 Right-click **Windows_cluster**, and select **Properties**.
- 3 Under **Add Permission**, click **Select user group**.
- 4 In the **Select user group** panel, select **alpha.symantecdomain.com**, and enter **UserGroup_A**.
- 5 Verify the user group, and click **OK**.
- 6 Under **Add Permission**, select **Admin** role from the list, and click **Add**.

The UserGroup_A is now assigned the Admin role on Windows_cluster. This team can now perform all the tasks on the cluster.

Similarly you can assign Admin role to UserGroup_B on Linux_cluster. If required, you can also assign Guest role to UserGroup_A on Linux_cluster, and Guest role to UserGroup_B on Windows_cluster.

Provide access to an object within the Organization.

Since UserGroup_A is assigned Guest role on Linux_cluster, all the service groups within Linux_cluster inherit the Guest role for UserGroup_A.

Example: Managing user access in Veritas Operations Manager using Organizations and existing user groups

Consider a service group, Beta_SG, which belongs to the Linux_cluster Organization. You want to assign Admin role to UserGroup_A on this service group. To do this you need to modify the role.

To modify role on Beta_SG to Admin for UserGroup_A

- 1 In the Home page on the Management Server console, go to Availability perspective and select **Manage** in the left pane.
- 2 Expand **Linux_cluster**, expand **Service Groups**, and select **Beta_SG**.
- 3 Right-click **Beta_SG**, and select **Properties**.
- 4 Click the **Permissions** tab.
- 5 Right-click **UserGroup_A**, select **Modify Role**.
- 6 Select **Admin** role and click **OK**.

UserGroup_A now has Admin role on Beta_SG, and Guest role on the remaining service groups in the Linux_cluster Organization.

See [“Configuring Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server”](#) on page 151.

See [“About predefined roles in Veritas Operations Manager”](#) on page 156.

See [“About Organizations, objects, and roles in Veritas Operations Manager”](#) on page 157.

See [“Assigning permissions to user groups for a perspective”](#) on page 158.

Setting up fault monitoring

This chapter includes the following topics:

- [About alerts and rules](#)
- [Creating rules in the Management Server perspective](#)
- [Editing rules in the Management Server perspective](#)
- [Deleting rules in the Management Server perspective](#)
- [Enabling rules in the Management Server perspective](#)
- [Disabling rules in the Management Server perspective](#)
- [About faults and risks](#)
- [Suppressing faults in the Management Server perspective](#)
- [Restoring a suppressed fault in the Management Server perspective](#)
- [Suppressing a fault definition in the Management Server perspective](#)
- [Restoring a suppressed fault definition in the Management Server perspective](#)

About alerts and rules

Data center administrators need to manage the condition of the resources in the data center. Administrators typically define the custom rules that specify what conditions generate an alert, what actions should occur if an alert is detected, and which actions generate which type of alert severity. Using the Management Server console, you can create and maintain rules pertaining to alerts.

You can monitor the faulty status and performance information of your data center by reviewing the alert log on the Management Server console.

You can view the following information on alerts in the data center:

- Information about the alert.
- The source of the alert.
- The time when the alert occurred.

The alert severity levels are:

- Critical
- Warning
- Information

You can create alert rules to receive warnings about events and conditions, such as stopped replication or storage capacity, enabled or disabled I/O paths, faulted clusters and so on.

Using the Management Server console, you can specify to initiate one of the following actions when an alert condition is met:

- Send an email message. For some alert conditions, operators may want to send emails notifying key personnel about the condition. You can specify one or more email addresses to which the alert notification is sent.

Note: You must provide the details for the SMTP settings before setting the email notification for an alert.

- Send an SNMP trap notification. Some objects are not polled. When events take place, these objects send traps or unsolicited asynchronous SNMP messages to the Server. Some of the rules that Veritas Operations Manager uses to monitor objects in the environment rely on SNMP trap-based messages.

Note: You must configure SNMP trap settings for receiving alert notifications.

- Run a custom script. You can upload a custom script that runs when the alert conditions that are specified by the rule occur.

See [“Viewing the details of rules”](#) on page 239.

See [“Configuring SMTP settings for email notifications”](#) on page 218.

See [“Configuring SNMP trap settings for alert notifications”](#) on page 219.

Creating rules in the Management Server perspective

In the Management Server console, you can create rules to trigger various actions based on alert conditions. Aside from creating rules from the rules option, you can also create rules from selected faults and alerts.

Rules that are created in the Management Server perspective are applied globally to the entire data center organization, including all sub-organizations that are created.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

Note: If you want to apply a rule only to specific Organizations rather than the entire data center, do not create the rule in the Management Server perspective. Instead create the rule in the perspective that contains the Organizations.

For more information on applying rules to specific Organizations, see *Veritas Operations Manager Management Server User Guide*.

To create a rule in the Management Server perspective

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Alert & Rules**.
- 3 Click **Create Rule**.
- 4 In the **Create Rule** wizard panel, do one of the following:
 - Select **This rule will be triggered for all faults of type:**, click **Next** and skip to 6.
 - Select **Enter the fault topics that will trigger the actions for this rule:**, enter the fault definitions separated by a comma (,) or a semicolon (;), and click **Next**. Skip to 6.
 - Select **Choose from a list of fault topics**, click **Next**, and skip to 5.

See [“Create Rule - Select the type of fault conditions to trigger this rule panel options”](#) on page 169.
- 5 In the **Create Rule - Select one or more fault topics which will trigger this rule** wizard panel, select the fault topics, and click **Next**.

See [“Create Rule - Select one or more fault topics which will trigger this rule panel options”](#) on page 170.
- 6 In the **Create Rule - Setup notifications** wizard panel, enter the required information and click **Next**.

See [“Create Rule - Setup notifications panel options”](#) on page 170.

- 7 In the **Create Rule - Enter name and description** wizard panel, enter the required information and click **Finish**.
 See [“Create Rule - Enter name and description panel options”](#) on page 172.
- 8 In the **Create Rule - Result** panel, verify that the rule has been successfully created, and click **OK**.
 See [“Editing rules in the Management Server perspective”](#) on page 172.
 See [“Deleting rules in the Management Server perspective”](#) on page 176.
 See [“Enabling rules in the Management Server perspective”](#) on page 177.
 See [“Disabling rules in the Management Server perspective”](#) on page 178.

Create Rule - Select the type of fault conditions to trigger this rule panel options

Use this panel to select a type of fault condition to trigger an alert.

[Table 9-1](#) list the options that you can select to create a rule.

Table 9-1 Create Rule - Select the type of fault conditions to trigger this rule options

Field	Description
This rule will be triggered for all faults of type:	Select this option to trigger a rule for any faults of the selected type. You can select the following types of faults: ■ Fault ■ Risk
Enter the fault topics that will trigger the actions for this rule:	Select this option to trigger a rule when the specified fault occurs. You can enter the name of the fault. Use a colon (,) or semicolon (;) to separate multiple entries. Enter event.alert.vom to view the list of fault topics. You can choose a fault topic from the list. You can use a wildcard character (*) to select multiple faults. For example, you can enter event.alert.vom.vm.* to select all the faults on virtual machines.

Table 9-1 Create Rule - Select the type of fault conditions to trigger this rule options (*continued*)

Field	Description
Choose from a list of fault topics	Select this option to choose from a list of existing fault definitions. The fault topics listed are those which are relevant to the perspective in which you are creating the rule. If you are creating a rule in the Management Server perspective (Settings), the list includes all host fault topics and array and switch fault topics.

See [“Creating rules in the Management Server perspective”](#) on page 168.

Create Rule - Select one or more fault topics which will trigger this rule panel options

Use this panel to select the fault topics that will trigger the rule.

The fault topics listed are those which are relevant to the perspective in which you are creating the rule. If you are creating a rule in the Management Server perspective (Settings), the list includes all host fault topics and array and switch fault topics.

See [“Creating rules in the Management Server perspective”](#) on page 168.

Create Rule - Setup notifications panel options

Use this wizard panel to set up notifications for the alert.

[Table 9-2](#) lists the options to set up the notification.

Table 9-2 Create Rule - Set up notifications options

Field	Description
Email	Select to set up an email notification when the fault conditions that are specified by the rule occur.

Table 9-2 Create Rule - Set up notifications options (*continued*)

Field	Description
SNMP Trap	Select to send an SNMP trap when the alert conditions that are specified by the rule occur. This option is disabled if SNMP trap settings are not configured. To configure the SNMP trap settings, See “Configuring SNMP trap settings for alert notifications” on page 219.
Custom script	Select to run a custom script when the alert conditions that are specified by the rule occur. Note: You can run a custom script only if you create a rule in the Management Server perspective.

You must set up at least one type of notification for the rule that you create else the rule will not be enabled.

Table 9-3 Notification options

Field	Description
Email: To	Enter the email address of one or more users who want to receive the notification. Separate multiple entries with a comma (,) or a semicolon (;). Example: 123@example.com, 456@example.com
Send email as daily digest	Select to send the email notification as daily digest. All alert notifications are summarized into one email and sent daily to the subscribed users.
Custom script	Browse the custom script file and upload it. You can only upload the following types of scripts: ■ Perl (.pl) ■ Shell (.sh) ■ Batch (.bat)

See [“Creating rules in the Management Server perspective”](#) on page 168.

Create Rule - Enter name and description panel options

Use this panel to assign a name and description to the alert rule.

Table 9-4 Create Rule - Enter name and description options

Field	Description
Rule Name	Enter the name of the rule. Maximum character limit is 255. Example: Restart stopped ABC program.
Description	Enter a description for this rule. The description should include the purpose of the rule. Maximum character limit is 255. Example: When the ABC program generates a service stopped alert, run the restart program script, and send an alert to the SNMP trap console.
Enable	Clear to disable the rule. An enabled rule monitors alerts for the defined conditions.

See [“Creating rules in the Management Server perspective”](#) on page 168.

Editing rules in the Management Server perspective

Using the Management Server console, you can edit the alert rules.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To edit a rule in the Management Server perspective

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Alert & Rules**.
- 3 Click the **Rules** tab.
- 4 Right-click a rule and select **Edit**.
- 5 In the **Edit Rule - Select the type of fault conditions to trigger this rule** wizard panel, do one of the following:
 - Select **This rule will be trigger for all faults of type:**, click **Next** and skip to [7](#).

- Select **Enter the fault topics that will trigger the actions for this rule separated by (,) or (;):**, enter the fault definitions separated by a comma (,) or a semicolon (;), and click **Next**. Skip to [7](#).
- Select **Choose from a list of fault topics**, click **Next**, and skip to [6](#).

See [“Edit Rule - Select the type of fault condition to trigger this rule panel options”](#) on page 173.

- 6 In the **Edit Rule - Select one or more fault topics which will trigger this rule** wizard panel, select the fault topics, and click **Next**.

See [“Edit Rule - Select one or more fault topics which will trigger this rule panel options”](#) on page 174.

- 7 In the **Edit Rule - Setup notifications** wizard panel, enter the required information and click **Next**.

See [“Edit Rule - Setup notifications panel options”](#) on page 174.

- 8 In the **Edit Rule - Enter name and description** wizard panel, enter the required information and click **Finish**.

See [“Edit Rule - Enter name and description panel options”](#) on page 176.

- 9 In the **Edit Rule - Result** panel, verify that the rule has been successfully created, and click **OK**.

See [“Creating rules in the Management Server perspective”](#) on page 168.

See [“Deleting rules in the Management Server perspective”](#) on page 176.

See [“Enabling rules in the Management Server perspective”](#) on page 177.

See [“Disabling rules in the Management Server perspective”](#) on page 178.

Edit Rule - Select the type of fault condition to trigger this rule panel options

Use this panel to select the type of fault conditions to trigger an alert.

[Table 9-5](#) list the options that you can select to create a rule.

Table 9-5 Edit Rule - Select the type of fault condition to trigger this rule

Field	Description
This rule will be triggered for all faults of type:	Select this option to trigger a rule for any faults of the selected type. You can select the following types of faults: ■ Fault ■ Risk
Enter the fault topics that will trigger the actions for this rule separated by (,) or (;):	Select this option to trigger a rule when the specified fault occurs. You can enter the name of the fault. Use a colon (:) or semicolon (;) to separate multiple entries. Enter event.alert.vom to view the list of fault topics. You can choose a fault topic from the list. You can use wild character (*) to select multiple faults. For example, you can enter event.alert.vom.vm.* to select all the faults on VxVM volumes.
Choose from a list of fault topics	Select this option to choose from a list of existing fault definitions.

See [“Editing rules in the Management Server perspective”](#) on page 172.

Edit Rule - Select one or more fault topics which will trigger this rule panel options

Use this panel to select the fault topics that will trigger the rule.

See [“Editing rules in the Management Server perspective”](#) on page 172.

Edit Rule - Setup notifications panel options

Use this wizard panel to set up notifications for the alert.

[Table 9-6](#) lists the options to set up the notification.

Table 9-6 Edit Rule panel options to set up notifications

Field	Description
Email	Select to set up an email notification when the fault conditions that are specified by the alert rule occur.
SNMP Trap	Select to send an SNMP trap when the alert conditions that are specified by the alert rule occur. This option is disabled if SNMP trap settings are not configured. To configure the SNMP trap settings, See "Configuring SNMP trap settings for alert notifications" on page 219.
Custom script	Select to run a custom script when the alert conditions that are specified by the rule occur. Note: You can run a custom script only if you edit a rule in the Management Server perspective.

You must set up at least one type of notification for the rule that you create.

Table 9-7 Notification options

Field	Description
Email: To	Enter the email address of one or more users who want to receive the notification. Separate the multiple entries with a comma (.). Example: 123@example.com, 456@example.com
Send email as daily digest	Select to send the email notification as daily digest. All alert notifications are summarized into one email and sent daily to the subscribed users.

Table 9-7 Notification options (*continued*)

Field	Description
Custom script	Browse the custom script file and upload it. You can only upload the following types of scripts: ■ Perl (.pl) ■ Shell (.sh) ■ Batch (.bat)

See [“Editing rules in the Management Server perspective”](#) on page 172.

Edit Rule - Enter name and description panel options

Use this panel to assign a name and description to the alert rule.

Table 9-8 Edit Rule - Description

Field	Description
Rule Name	Edit the name of the rule. Maximum character limit is 255. Example: Restart stopped ABC program.
Description	Edit the description for this rule. The description should include the purpose of the rule. Maximum character limit is 255. Example: When the ABC program generates a service stopped alert, run the restart program script, and send an alert to the SNMP trap console.
Enable	Clear to disable the rule. An enabled rule monitors alerts for the defined conditions.

See [“Editing rules in the Management Server perspective”](#) on page 172.

Deleting rules in the Management Server perspective

Using the Management Server console, you can delete the rules that are no longer required.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To delete a rule in the Management Server perspective

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Alert & Rules**.
- 3 Click the **Rules** tab.
- 4 Right-click a rule and select **Delete**.
- 5 In the **Delete Rule** wizard panel, review the information, and click **OK**.
See [“Delete Rule panel options”](#) on page 177.
- 6 In the **Delete Rule - Result** panel, click **OK**.

See [“Creating rules in the Management Server perspective”](#) on page 168.

See [“Editing rules in the Management Server perspective”](#) on page 172.

See [“Enabling rules in the Management Server perspective”](#) on page 177.

See [“Disabling rules in the Management Server perspective”](#) on page 178.

Delete Rule panel options

Use this panel to delete an existing rule. Deleted rules are no longer available for sending emails, generating SNMP traps, or executing custom scripts in response to alerts.

See [“Deleting rules in the Management Server perspective”](#) on page 176.

Enabling rules in the Management Server perspective

Using the Management Server console, you can enable the rules that are in the disabled state.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To enable rules in the Management Server perspective

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Alert & Rules**.
- 3 Click the **Rules** tab.
- 4 Right-click a rule, and select **Enable**.

- 5 In the **Enable Rule** wizard panel, review the information, and click **OK**.
See [“Enable Rule panel options”](#) on page 178.
- 6 In the **Enable Rule - Result** panel, click **OK**.
See [“Disabling rules in the Management Server perspective”](#) on page 178.
See [“Creating rules in the Management Server perspective”](#) on page 168.
See [“Editing rules in the Management Server perspective”](#) on page 172.
See [“Deleting rules in the Management Server perspective”](#) on page 176.

Enable Rule panel options

Use this panel to enable the rule that is in disable state.

See [“Enabling rules in the Management Server perspective”](#) on page 177.

Disabling rules in the Management Server perspective

Using the Management Server console, you can disable the rules that are in the enabled state.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To disable rules in the Management Server perspective

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Alert & Rules**.
- 3 Click the **Rules** tab.
- 4 Right-click a rule, and select **Disable**.
- 5 In the **Disable Rule** wizard panel, review the information, and click **OK**.
See [“Disable Rule panel options”](#) on page 179.
- 6 In the **Disable Rule - Result** panel, click **OK**.
See [“Enabling rules in the Management Server perspective”](#) on page 177.
See [“Creating rules in the Management Server perspective”](#) on page 168.
See [“Editing rules in the Management Server perspective”](#) on page 172.
See [“Deleting rules in the Management Server perspective”](#) on page 176.

Disable Rule panel options

Use this panel to disable the rule that is in enabled state.

See [“Disabling rules in the Management Server perspective”](#) on page 178.

About faults and risks

Veritas Operations Manager enables you to view all possible problems in the data center that it manages at several levels in the user interface. You can monitor the faulty status and possible risks to the managed resources.

You can view the system identified fault conditions along with their corresponding entities and the affected sources. You can automate error handling by developing the rules that trigger specific actions in response to alert conditions. You can also suppress a fault for a specific duration.

You can view the following information on faults in the data center:

- Conditions of the managed objects (applications, storage enclosures, hosts, clusters and so on) in the data center.
- The source of the fault.
- The time when the fault occurred.

See [“Viewing the faults definitions”](#) on page 237.

See [“Viewing faults in the Management Server perspective ”](#) on page 237.

See [“Suppressing a fault definition in the Management Server perspective”](#) on page 182.

See [“Restoring a suppressed fault definition in the Management Server perspective”](#) on page 183.

See [“Suppressing faults in the Management Server perspective”](#) on page 179.

See [“Restoring a suppressed fault in the Management Server perspective”](#) on page 181.

Suppressing faults in the Management Server perspective

Using the Management Server console, you can suppress one or more faults in Veritas Operations Manager. To suppress a fault, you can choose one of the following:

- Temporarily hide the fault.

- Disable the fault for the affected fault sources.
- Disable all the faults for the affected fault sources.

For all the options, you can either specify the date and time to keep the faults in the suppressed state, or you can suppress the faults forever.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To suppress a fault

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Faults & Risks**.
- 3 Click the **Faults** tab.
- 4 Right-click a fault and select **Suppress Faults**.
- 5 In the **Suppress Faults** wizard panel, enter the required information, and click **OK**.

See [“Suppress Faults panel options”](#) on page 180.

See [“Viewing faults in the Management Server perspective ”](#) on page 237.

See [“Restoring a suppressed fault in the Management Server perspective”](#) on page 181.

Suppress Faults panel options

Use this panel to suppress the faults in Veritas Operations Manager. You can hide or disable the faults either temporarily or permanently. You can disable a fault for a specific object; however, the fault definition is still considered as active for other objects.

For all these options, you can either specify the date and time to keep the faults in the suppressed state, or suppress the faults forever.

Table 9-9 Suppress Faults panel options

Field	Description
Hide the selected fault(s). Show again if the problem reoccurs.	Select this option to temporarily hide the selected fault. It is essentially hiding the current instance of the fault. The fault is displayed again when it is detected.
Disable the selected fault(s) for the affected fault sources	Select this option to disable the fault for the affected fault source.

Table 9-9 Suppress Faults panel options (*continued*)

Field	Description
Disable all fault(s) for the affected fault sources	Select this option to disable all faults for the affected fault source.
Hide or disable forever	Select this option to hide the fault without specifying any time interval.
Hide or disable until	You can specify the date until which the fault remains suppressed. After this date, the fault is again considered as active in Veritas Operations Manager.
Reason for hiding or disabling	Provide the reason why the fault was suppressed. You can enter up to 254 characters for the description.

See [“Suppressing faults in the Management Server perspective”](#) on page 179.

Restoring a suppressed fault in the Management Server perspective

You can restore the fault that is suppressed in Veritas Operations Manager.

When you suppress a fault, you set a date until which the fault is suppressed. After the specified date, the fault is again considered as active in the system. However, Veritas Operations Manager also provides you with the option to activate the fault before that set date.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To restore a suppressed fault in the Management Server perspective

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Faults & Risks**.
- 3 Click the **Faults** tab.
- 4 Right-click the suppressed fault, and select **Restore Faults**.
- 5 In the **Restore Faults** panel, click **OK**.

See [“Suppressing faults in the Management Server perspective”](#) on page 179.

See [“Viewing faults in the Management Server perspective ”](#) on page 237.

Suppressing a fault definition in the Management Server perspective

You can suppress the fault definitions for the faults that you want to disable permanently. After the definition itself is suppressed, Veritas Operations Manager treats the corresponding faults as non-existing. You can specify a period to keep the selected fault definition in the suppressed state.

Note: Though the option to forever disable a fault definition is provided, you can again activate the fault definition using the **Unsuppress Faults** option.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To suppress a fault definition

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Faults & Risks**.
- 3 Click the **Fault Definition** tab.
- 4 Right-click a fault definition and select **Suppress Faults**.
- 5 In the **Suppress Faults** wizard panel, enter the required information, and click **OK**.

See [“Suppress the fault definition panel options”](#) on page 182.

See [“Viewing the faults definitions”](#) on page 237.

See [“Restoring a suppressed fault definition in the Management Server perspective”](#) on page 183.

Suppress the fault definition panel options

Use this panel to suppress the selected fault definition. After the fault definition is suppressed, it is no longer displayed on Veritas Operations Manager user interface. You can suppress one or more fault definitions simultaneously.

Table 9-10 Suppress Faults panel options

Field	Description
Hide or disable forever	Select this option to disable the fault definition without specifying any time period. Note: Though the fault definition is suppressed forever, you can still activate it. This option provides additional flexibility to the users who want to be able to suppress the definition without specifying the date along with the ability to re-activate the definition.
Hide or disable until	You can specify the date until which the fault definition remains suppressed. After this date, the fault definition is again considered as active in Veritas Operations Manager.
Reason for hiding or disabling	Provide the reason to suppress this fault definition. You can enter up to 254 characters for the description.

See [“Suppressing a fault definition in the Management Server perspective”](#) on page 182.

Restoring a suppressed fault definition in the Management Server perspective

You can restore a suppressed fault definition using the Management Server console. After re-activation, Veritas Operations Manager starts using the fault definition for subsequent fault detections.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To restore a suppressed fault definition

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Faults & Risks**.
- 3 Click the **Fault Definition** tab.
- 4 Right-click a suppressed fault, and select **Restore Faults**.
- 5 In the **Restore Faults** panel, click **OK**.

See [“Suppressing a fault definition in the Management Server perspective”](#) on page 182.

See [“Viewing the faults definitions”](#) on page 237.

Setting up virtualization environment discovery

This chapter includes the following topics:

- [About the virtualization technologies supported](#)
- [About Control Hosts in Veritas Operations Manager](#)
- [Requirements for discovering vCenter and ESX servers using Veritas Operations Manager](#)
- [About near real-time \(NRT\) update of virtual machine states](#)
- [Setting-up near real-time \(NRT\) update of virtual machine states](#)
- [Requirements for discovering the Solaris zones](#)
- [Requirements for discovering Solaris Logical domains](#)
- [Requirements for discovering logical partitions](#)
- [Requirements for Microsoft Hyper-V virtualization discovery](#)
- [Requirements for Kernel-based Virtual Machine \(KVM\) virtualization discovery](#)
- [Configuring the virtualization discovery](#)
- [Editing a virtualization discovery configuration](#)
- [Refreshing a virtualization discovery configuration](#)
- [Removing a virtualization discovery configuration](#)
- [Configuring performance metering for a VMware vCenter server](#)
- [Disable performance metering for a VMware vCenter server](#)

About the virtualization technologies supported

Veritas Operations Manager supports the following virtualization technologies:

- VMware ESX
- Solaris Zones
- Oracle VM Server for SPARC (previously called Sun Logical Domains - LDomS)
- Logical partition (LPAR)
- Microsoft Hyper-V
- Kernel-based Virtual Machine (KVM): Red Hat Enterprise Linux as the KVM Server

For VMware ESX discovery, a designated Control Host discovers the VMware vCenter Server in the data center. This discovery displays those ESX servers that VMware vCenter Server manages and the virtual machines that are configured on the ESX servers.

For Solaris Zones discovery, the zone agentlet that is present in the `VRTSsfmh` package, which is installed on a Solaris managed host, discovers the Global zones that are configured on the host. This discovery displays the non-Global zones that are configured on the Global Zone.

For Sun LDomS discovery, the LDom agentlet that is present in the `VRTSsfmh` package, which is installed on a Solaris managed host, discovers the LDom Server that is configured on the host. This discovery displays the LDom clients that are configured on the LDom Server.

For logical partition (LPAR) discovery, Veritas Operations Manager can use Hardware Management Console (HMC), a `VRTSsfmh` package that is installed on the LPAR client, or a `VRTSsfmh` package installed as a part of DMP on the VIO server. Control Host is required for the HMC discovery.

For Microsoft Hyper-V discovery, Veritas Operations Manager discovers Hyper-V server (with `VRTSsfmh` package on it), and its correlation with the Hyper-V virtual machines. It also discovers the storage that is provisioned to the guests and its correlation with the virtual machine and the Hyper-V server. The Hyper-V guest, when added (using agent or agentless option) to Veritas Operations Manager Management Server domain, provides storage mapping discovery.

For Kernel-based Virtual Machine (KVM) discovery, Veritas Operations Manager discovers KVM virtual machines on the Linux host if the KVM modules are installed, and configured on the virtualization server (KVM Server). Veritas Operations Manager discovers basic information about KVM virtual machines. For example, virtual machine name, CPU, and so on.

See [“Requirements for discovering the Solaris zones”](#) on page 193.

See [“Requirements for discovering logical partitions”](#) on page 194.

See [“Requirements for Microsoft Hyper-V virtualization discovery”](#) on page 195.

See [“Requirements for Kernel-based Virtual Machine \(KVM\) virtualization discovery”](#) on page 196.

About Control Hosts in Veritas Operations Manager

Veritas Operations Manager uses Control Hosts as a discovery mechanism. In Veritas Operations Manager, the Control Hosts discover the following:

- Information on VMware Virtualization infrastructure (vSphere) and Hardware Management Console (HMC) server.
- Agentless hosts.

To configure the Control Host on a managed host, install the Control Host Add-on on the Veritas Operations Manager Management Server or a managed host that reports to Management Server.

Information on VMware Virtualization Infrastructure (vSphere)

In Veritas Operations Manager, you can configure Veritas Operations Manager Management Server or a managed host that reports to Management Server as Control Host to discover the information on the VMware virtualization infrastructure. For this configuration, you must install the Control Host Add-on on the physical or virtual hosts that you want to designate as Control Host. In Veritas Operations Manager, you must download the Control Host Add-on from the Symantec Web site, upload to the **Deployment Management Repository**, and install it on the relevant physical or virtual hosts.

In your data center, Control Hosts help Management Server in discovering the following information on VMware virtualization infrastructure:

- VMware vCenter servers that are configured in your data center.
- VMware ESX servers that vCenters manage.
- VMware Virtual Machines that are configured on the VMware ESX servers.
- VMware HA Clusters.

Note: To administer a Control Host on the Windows platform, Veritas Operations Manager creates a user named 'vomuser' with the administrative privileges.

Ensure that the Control Hosts can ping the vCenter servers from which they can discover the information on VMware Infrastructure.

You can designate a managed host that reports to Management Server as Control Host to address the following situations:

- To discover the vCenter server that is behind a firewall and you do not want to install Management Server inside the firewall.
- To except Management Server from the discovery of VMware infrastructure to reduce the load on Management Server.

Discovery using the Hardware Management Console (HMC)

The HMC server manages LPAR servers and lets you discover information related to VIO servers and VIO clients. You can use the virtualization management option on the Veritas Operations Manager console to add the HMC server to Management Server.

To add the HMC server to Veritas Operations Manager, you need to install the Control Host add-on on the host where the HMC server should be added. Virtual SCSI disks on LPAR client are supported. However, NPIV, or virtual Fibre Channel disks are not supported. Currently, only Virtual SCSI disks backed by native or DMP devices are supported.

By configuring HMC server only (without the VRTSsfmh package), you can discover information about the exported storage from the VIO server to the VIO clients and the devices that are given to the VIO server from the storage area network (SAN).

Agentless discovery of a remote host

You can use Control Hosts to perform agentless discovery of VMware virtual machines. Add the vCenter server that hosts the virtual machine as an Agentless Host to the Management Server.

To perform agentless discovery of hosts, you must install the Control Host Add-on on one of the managed hosts. You can install the Control Host Add-on on Management Server, however it is not recommended as it puts extra load on Management Server.

A UNIX Control Host can only discover UNIX agentless hosts using SSH. A Windows Control Host can discover Windows agentless hosts using WMI or UNIX agentless hosts using SSH. Ensure that you install one or more Control Hosts on the appropriate platform depending on the operating system of the remote hosts you want to discover using agentless method.

See [“About agentless discovery using the Control Host”](#) on page 123.

Requirements for discovering vCenter and ESX servers using Veritas Operations Manager

The following are the requirements for discovering VMware Infrastructure using Veritas Operations Manager:

- Install the `VRTSsfmh` package on the virtual or physical hosts on which you want to install the Control Host Add-on.
- Ensure that the Control Hosts can ping the vCenter servers or the ESX servers from which they can discover the information on VMware Infrastructure.
- Ensure that you have appropriate privileges to log on to the vCenter server or the ESX server.
- Ensure that you have the Browse Datastore privileges on the vCenter or the ESX server that you want Veritas Operations Manager to discover.

About near real-time (NRT) update of virtual machine states

With near real-time (NRT) update of virtual machine states, any change in the power state of a virtual machine in the Veritas Operations Manager Management Server domain is updated in the Veritas Operations Manager database in near real time.

Configure the VMware vCenter Server and the Management Server in the same domain. Note that no other information except the power state of the virtual machine is updated in near real time.

Note: The near real-time update of virtual machines is supported on VMware vCenter Server 4.x and 5.x.

See [“Setting-up near real-time \(NRT\) update of virtual machine states”](#) on page 189.

See [“About the virtualization technologies supported”](#) on page 186.

Setting-up near real-time (NRT) update of virtual machine states

To set up near real-time updates of the virtual machine state, configure the VMware vCenter Server SNMP settings with the VOM server address as the receiver URL. The Management Server receives the updates when you add the VMware vCenter Server to the Management Server.

When a virtual machine's state (powered ON, powered OFF, or suspended) changes, the managing VMware vCenter Server that is discovered in the Management Server, generates the corresponding SNMP trap. It then sends the trap to the Management Server. The SNMP trap contains the information of the virtual machine state, and it is used to update the Management Server database.

Note: SNMP version 1 (SNMPv1) and version 2 (SNMPv2) are supported.

The Veritas Operations Manager component of near real-time update is `xtrapd`. It runs as a daemon on Linux and as a service on Windows. `xtrapd` detects the SNMP trap that is sent from the VMware vCenter Server, updates the virtual machine records in the Veritas Operations Manager database, and subsequently the Management Server console is updated with the latest state of the virtual machine.

To set up the near real-time update of VMware virtual machines, complete the following steps:

Table 10-1 Setting up near real-time (NRT) update of virtual machine states

Steps	Action	Description
Using VMware vCenter Server console:		
Step 1	Provide Management Server details in the VMware vCenter Server console.	Provide information to configure Management Server as the SNMP trap receiver. Also configure the alarm to send the SNMP traps when the state of the virtual machine changes. See “Configuring the VMware vCenter Server to generate SNMP traps” on page 191.
Using the Management Server console:		

Table 10-1 Setting up near real-time (NRT) update of virtual machine states
(continued)

Steps	Action	Description
Step 2	Add VMware vCenter Server to Management Server.	When you add a VMware vCenter Server to Management Server, the <code>xtrapd</code> daemon on the Management Server starts accepting SNMP traps from the specified VMware vCenter Server. See “Configuring the virtualization discovery” on page 196. Note: If you have not configured the VMware vCenter Server before adding it to the Veritas Operations Manager domain, a warning message is displayed. It does not affect the vCenter Server discovery. However, near real-time virtual machine state discovery is not functional. If you want to enable near real-time update of virtual machine states, you need to first configure the VMware vCenter Server, and then refresh the VMware vCenter Server configuration in the Management Server console.

By default, near real-time update of virtual machines is enabled. To disable it, you need to remove Management Server as the SNMP receiver in the VMware vCenter Server.

See [“About near real-time \(NRT\) update of virtual machine states”](#) on page 189.

Configuring the VMware vCenter Server to generate SNMP traps

Provide the following information:

- Using the VMware vCenter Server console, configure the Management Server as the SNMP trap receiver in the VMware vCenter Server. In the Home page of vSphere Client, select **vCenter Server Settings** and then select SNMP configuration. Enable one of the SNMP receivers and enter details as follows:

Field	Description
Receiver URL	Provide the host name of the Management Server which will be connected to the VMware vCenter Server. VMware vCenter Server sends the SNMP traps to this Management Server. Also, configure port 162 as the SNMP port. Ensure that port 162 is not used by any other application.

- | Field | Description |
|------------------|--|
| Community String | Provide community string. SNMP versions v1 and v2 are supported. |
- Configure alarm for generating SNMP traps when the virtual machine state changes. It includes adding alarm to monitor the change in the virtual machine state and adding the appropriate action (for example, send notification email).
 - In the Home page of the VMware vSphere Client, select **Hosts and Clusters** and right-click on the VMware vCenter Server, data-center or an individual virtual machine to set the alarm. You can set the alarm at an individual virtual machine level, at the data center level, or at the entire VMware vCenter Server level. It is recommended to set it at the VMware vCenter Server level.
 - In the **General** tab, provide alarm details with alarm type set for monitoring the virtual machines. Enter the details as listed in the following table:

Field	Description
Alarm Name	Provide the name of the alarm.
Description	Provide additional information about the alarm.
Alarm Type	Select Virtual Machines in the Monitor drop-down list. Select Monitor for specific events occurring on this object, for example, VM powered On option. Ensure that Enable this alarm check box is selected.

- In the **Triggers** tab, add the required triggers to monitor the states of the virtual machine - VM powered on, VM powered off, VM suspended, and DRS VM powered on (for clustered environment with DRS enabled). The values of the fields are as follows:

For the following value of an event...	Select the following status...
DRS VM powered on	Unset
VM powered on	Unset
VM powered off	Unset
VM suspended	Unset

- Provide information on when to send the notification trap.

In the **Actions** tab of the **Alarm Settings** panel, click **Add** to add a new action. In the **Action** drop-down list, select **Send a notification trap** option. Set action as provided in the following figure:



See [“About near real-time \(NRT\) update of virtual machine states”](#) on page 189.

See [“Setting-up near real-time \(NRT\) update of virtual machine states”](#) on page 189.

Requirements for discovering the Solaris zones

The following are the requirements for discovering Solaris zones in Veritas Operations Manager:

- Install the `VRTSsfmh` package on one or more traditional hosts that contains Global Zones. This helps Veritas Operations Manager discover non-global-zones that are configured on the Global Zones.
- Ensure that the managed hosts with the Solaris 10 or 11 operating system contain non-Global Zones.
- Ensure that the managed hosts with the Solaris 10 or 11 operating system do not contain any LDoms.
- Enable the `zlogin` command if it is disabled on the non-Global Zones.
- Ensure that using the `zlogin` command, you can log on to the non-Global Zones.
- Ensure that the non-Global Zones can access the devices that are exported from the Global Zone.
- Ensure that the file systems that are exported from the Global Zone to the non-Global Zones are mounted in the non-Global Zones.

See [“About the virtualization technologies supported”](#) on page 186.

See [“Requirements for the `zlogin` utility on non-Global Zones”](#) on page 193.

See [“Requirements for devices exported to non-Global Zones”](#) on page 194.

See [“Requirements for file systems exported to non-Global Zones”](#) on page 194.

Requirements for the `zlogin` utility on non-Global Zones

Veritas Operations Manager uses the `zlogin` utility to discover non-Global Zones. By default, the `zlogin` utility is enabled on non-Global Zones. If you have disabled

the `zlogin` utility on non-Global Zones, you need to enable it. You can use the following command to verify:

```
global# zlogin my-zone zonename
```

See [“Requirements for discovering the Solaris zones”](#) on page 193.

Requirements for devices exported to non-Global Zones

Veritas Operations Manager can discover the devices that are exported from the Global Zone to non-Global Zones. However, if the storage is not accessible to the non-Global Zone, Veritas Operations Manager cannot discover that storage as exported from the Global Zone. For example, the storage may not be accessible to the non-Global Zone because the non-Global Zone is not yet restarted. Ensure that the non-Global Zones can access the devices that are exported from the Global Zone.

See [“Requirements for discovering the Solaris zones”](#) on page 193.

Requirements for file systems exported to non-Global Zones

Veritas Operations Manager can discover the file systems that are exported from the Global Zone to non-Global Zones. However, if a file system is not mounted in a non-Global Zone, Veritas Operations Manager does not discover that file system as exported from the Global Zone. Ensure that the file systems that are exported from the Global Zone to the non-Global Zones are mounted in the non-Global Zones.

See [“Requirements for discovering the Solaris zones”](#) on page 193.

Requirements for discovering Solaris Logical domains

The following are the requirements for discovering Solaris LDoms using Veritas Operations Manager:

- Install the `VRTSsfmh` package on one or more traditional hosts with the Solaris operating system on which you want Veritas Operations Manager to discover Solaris LDoms.
- Ensure that the managed hosts with the Solaris operating system contain LDoms.

See [“About the virtualization technologies supported”](#) on page 186.

Requirements for discovering logical partitions

Logical partition (LPAR) virtualization discovery pre-requisites are as follows:

For basic LPAR discovery you need to:

- Add Hardware Management Console (HMC) to Veritas Operations Manager domain by control host.
- Configure the required storage arrays (providing storage to the LPAR servers) using the Storage Insight Add-on. This is required to discover the correlation of storage inside the VIO server with the storage arrays.
- For VIO servers with Veritas dynamic multi-pathing installed: Install the `VRTSsfmh` package on the VIO servers and configure them in Veritas Operations Manager as agents.
- You must have at least `hmcoperator` role in HMC to perform these tasks.

Note: The Veritas Operations Manager supports only legitimate filename characters in an LPAR profile name. The special characters reserved for Operating System usage (for example space, “\”, “\$”, “!”, “&”) are not supported. It is recommended to use upper and lower case alphabets, numeric values (0-9), “_” and “-” for the LPAR profile name.

For storage correlation discovery, in addition to the above mentioned pre-requisites, ensure that:

- You configure LPAR guests with `VRTSsfmh` package. It provides the discovery of correlation of storage inside LPAR guests with that exported from the VIO servers.

See [“About the virtualization technologies supported”](#) on page 186.

Requirements for Microsoft Hyper-V virtualization discovery

The requirements for the discovery of Microsoft Hyper-V virtualization discovery are listed below:

Virtual machine discovery

- `VRTSsfmh` package should be installed on the Hyper-V server (parent partition).
- Hyper-V role should be enabled.
- Windows Management Instrumentation (WMI) service should be running.

Exported storage discovery

- The Hyper-V server must be running Microsoft Windows 2008 R2, or later operating system.
- Windows Management Instrumentation (WMI) should be running on the guest. See [“About the virtualization technologies supported”](#) on page 186.

Requirements for Kernel-based Virtual Machine (KVM) virtualization discovery

Kernel-based Virtual Machine (KVM) discovery pre-requisites are as follows:

- `VRTSsfmh` package must be present on the Linux host.
- KVM modules must be installed and configured on the virtualization server.

To verify if the KVM modules are installed and configured, run the following command:

- `file /dev/kvm`

The output should be `/dev/kvm: character special`.

See [“About the virtualization technologies supported”](#) on page 186.

Configuring the virtualization discovery

In Veritas Operations Manager, you must configure the virtualization discovery to let a Control Host discover the virtual servers. You can configure the virtualization discovery for VMware discovery, or HMC discovery.

The VMware discovery provides the following information:

- Information on VirtualCenter servers
- Information on the ESX servers that the VirtualCenter server manages
- Information on the virtual machines that are configured on the ESX servers

The HMC discovery provides the following information:

- Information on HMC servers
- Information on the LPAR servers that the HMC server manages
- Information on the virtual machines that are configured on the LPAR servers

After you configure virtualization discovery, to view all ESX servers that the VirtualCenter server manages, click **vCenter** under **Data Center**. Similarly to view all the LPAR servers that the HMC server manages click **HMC** under **Data Center**.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective. The root user can also perform this task.

To configure virtualization discovery in Veritas Operations Manager

- 1 In the Home page on the Management Server console, click **Settings**.
 - 2 Do one of the following:
 - Click **Configure Virtualization Server**
 - Click **Virtualization**, and then click **Configure Virtualization Server**.
 - Click **Virtualization**, right-click **Data Center** and select **Configure Virtualization Server**.
 - 3 In the **Configure Virtualization Server** wizard panel, enter the details, and click **Next**.
- See [“Configure Virtualization Server panel options”](#) on page 197.
- 4 In the **Select option** wizard panel, select the method for virtualization discovery of the servers, and click **Finish**.
- See [“Configure Virtualization Server panel options”](#) on page 199.
- 5 In the **Result** panel, view the progress of the configuration. After the configuration is complete, click **OK**.

See [“Editing a virtualization discovery configuration”](#) on page 199.

See [“Refreshing a virtualization discovery configuration”](#) on page 202.

See [“Removing a virtualization discovery configuration”](#) on page 202.

Configure Virtualization Server panel options

Use this wizard panel to configure virtualization server discovery in Veritas Operations Manager.

Table 10-2 Configure Virtualization Server panel options

Field	Description
Configuration Type	Select the configuration type from the drop-down list.
Configuration Name	Enter a name for the virtualization server discovery configuration. You can reference the new virtualization server discovery configuration with the name that you specify in this field.

Table 10-2 Configure Virtualization Server panel options (*continued*)

Field	Description
Control host	Select the name of the control host from the drop-down list: ■ In case of VMware configuration, Veritas Operations Manager uses the control host that you specify in this field to discover the VMware environment that VirtualCenter and ESX servers manage. The control host and the VirtualCenter or the ESX servers should belong to the same subnet. ■ In case of HMC configuration, Veritas Operations Manager uses the control host that you specify in this field to discover the HMC environment that HMC servers manage. The control host and the HMC servers should belong to the same subnet.
VMware vCenter Server	This field is displayed only when you configure a VMware configuration. Specify the fully-qualified name of the VirtualCenter that you want the control host to discover along with its port number, separated by a colon. If the VirtualCenter Web service is running on a default port, you do not need to specify the port number.
HMC Server	This field is displayed only when you configure an HMC configuration. Specify the fully-qualified name of the HMC server that you want the control host to discover. Alternatively, you can also specify the IP address of the server.
User Name	Enter the user name that you can use to log on to the virtualization servers that you want the control host to discover. You can use a read-only user account if it has the Browse Datastore permissions on the virtualization servers. Note: Ensure that you have appropriate privileges to log on to the virtualization servers.
Password	Enter the password that you can use with the user name to log on to the virtualization servers that you want the control host to discover.

See [“Configuring the virtualization discovery”](#) on page 196.

Configure Virtualization Server panel options

Use this wizard panel to choose a method to enable the virtualization discovery configuration of servers.

Table 10-3 Select option panel

Field	Description
Auto Discover ESX Servers Auto Discover LPAR servers	Select this method to discover the ESX Servers or LPAR Servers automatically. When Auto Discover option is enabled, the list of configured servers is not displayed.
Select ESX Servers Select LPAR servers	Select this method to selectively discover the ESX Servers or LPAR Servers .
Name	The name of the server.
Discovery Enabled	Select the check box to enable discovery of the server.
Configuration Name	The configuration name of the server.

See [“Configuring the virtualization discovery”](#) on page 196.

Editing a virtualization discovery configuration

Using the Management Server console, you can edit the virtualization discovery that you have already configured.

You can edit a virtualization discovery configuration to modify the following information:

- Name of the configuration.
- Credentials to log on to the VirtualCenter or HMC server.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective. The root user can also perform this task.

To edit a virtualization discovery configuration in Veritas Operations Manager

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Virtualization**.
- 3 In the **Virtualization Configurations** details list, right-click the configuration that you want to edit.

- 4 In the **Edit Configuration** wizard panel, modify the required information, click **Next**.

See [“Edit Configuration panel options”](#) on page 200.

- 5 In the **Edit Configuration** wizard panel, edit the method for virtualization discovery of the servers, click **Finish**.

See [“Edit Configuration panel options for method selection”](#) on page 201.

- 6 In the **Result** panel, view the progress of the configuration, click **OK**.

See [“Configuring the virtualization discovery”](#) on page 196.

See [“Refreshing a virtualization discovery configuration”](#) on page 202.

See [“Removing a virtualization discovery configuration”](#) on page 202.

Edit Configuration panel options

Use this wizard panel to edit the virtualization server discovery that you have configured in Veritas Operations Manager.

Table 10-4 Virtualization configuration panel options for editing configurations

Field	Description
Configuration Type	Displays the configuration type.
Configuration Name	Displays the name that is provided to the virtualization discovery configuration. You can modify the name of the configuration in this field.
Control host	Displays the name of the Control Host that is specified for discovering the virtual servers that Veritas Operations Manager manages.
VMware VCenter Server	This field is displayed only when you edit a VMware configuration. Displays the name of the VirtualCenter server that you have specified when you configured the VMware discovery.
HMC Server	This field is displayed only when you edit an HMC configuration. Displays the name of the HMC server that you have specified when you configured the HMC discovery.

Table 10-4 Virtualization configuration panel options for editing configurations
(continued)

Field	Description
User Name	Displays the user name that you can use to log on to the virtual servers that you have specified. You can modify the user name in this field. Note: Ensure that you have appropriate privileges to log in to the virtual servers.
Password	Displays the password that you can use with the user name to log on to the virtual servers that you have specified. You can modify the password in this field.

See [“Editing a virtualization discovery configuration”](#) on page 199.

Edit Configuration panel options for method selection

Use this wizard panel to choose a method to edit the virtualization discovery configuration of servers.

Table 10-5 Virtualization configuration panel options for method selection

Field	Description
Auto Discover ESX Servers Auto Discover LPAR servers	Select this method to discover the ESX servers or LPAR servers automatically. When Auto Discover option is selected, the list of configured servers is not displayed.
Select ESX Servers Select LPAR servers	Select this method to selectively edit the discovery of ESX servers or LPAR servers.
Discovery Enabled	Select the check box to enable discovery of the server.
Name	The name of the server.
Configuration Name	The configuration name of the server.

See [“Editing a virtualization discovery configuration”](#) on page 199.

Refreshing a virtualization discovery configuration

Using the Management Server console, you can refresh the virtualization server that Veritas Operations Manager has already been discovered.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To refresh a virtualization discovery configuration

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Virtualization**.
- 3 Right-click the virtualization server and select **Refresh Configuration**.
- 4 In the **Refresh Virtualization Configuration** wizard panel, click **Refresh**.
- 5 In the **Result** panel, click **OK**.

See [“Configuring the virtualization discovery”](#) on page 196.

See [“Editing a virtualization discovery configuration”](#) on page 199.

See [“Removing a virtualization discovery configuration”](#) on page 202.

Removing a virtualization discovery configuration

Using the Management Server console, you can remove a virtualization discovery configuration.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective. The root user can also perform this task.

To remove a virtualization discovery configuration

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Virtualization**.
- 3 Right-click the virtualization server and select **Remove Configuration**.
- 4 In the **Remove Virtualization Configuration** wizard panel, click **Remove**.
- 5 In the **Result** panel, click **OK**.

See [“Configuring the virtualization discovery”](#) on page 196.

See [“Editing a virtualization discovery configuration”](#) on page 199.

See [“Refreshing a virtualization discovery configuration”](#) on page 202.

Configuring performance metering for a VMware vCenter server

Using the Management Server console, you can enable or disable performance metering for a VMware vCenter server and its configured ESX servers.

Performance metering is enabled by default. To disable performance metering, clear the **Enable performance metering** check box.

You can enter an interval period for which you want the performance data to be collected. The interval period should be between 5 minutes and 1440 minutes and in the multiples of five. The default interval period is five minutes.

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

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

Note: To perform this operation you must have Control Host Add-on 6.0.

To configure performance metering for a VMware vCenter server

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Virtualization**.
- 3 Right-click a VMware vCenter server and select **Configure metering**.
- 4 In the **Configure performance metering** panel, and enter an interval period for which you want the performance data to be collected, and click **Finish**.

See [“Disable performance metering for a VMware vCenter server”](#) on page 203.

Disable performance metering for a VMware vCenter server

Use this option to disable performance metering for a VMware vCenter server and the configured ESX servers.

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

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To disable performance metering for a VMware vCenter server

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Virtualization**.
- 3 Right-click a VMware vCenter server and select **Configure metering**.
- 4 In the **Configure performance metering** panel, clear the **Enable performance metering** check box, and click **Finish**.

See [“Configuring performance metering for a VMware vCenter server”](#) on page 203.

Deploying hot fixes, packages, and patches

This chapter includes the following topics:

- [About deploying Veritas Operations Manager hot fixes](#)
- [About deploying maintenance release packages and patches](#)
- [About deploying base release packages](#)
- [Downloading a hot fix, package, or patch](#)
- [Uploading a Veritas Operations Manager hot fix or package to the repository](#)
- [Installing a Veritas Operations Manager hot fix, package, or patch](#)
- [Uninstalling a Veritas Operations Manager hot fix](#)
- [Removing a hot fix, package, or patch from the repository](#)
- [Canceling deployment request for a hot fix, package, or patch](#)
- [Installing a Veritas Operations Manager hot fix on a specific managed host](#)
- [Uninstalling a Veritas Operations Manager hot fix from a specific managed host](#)

About deploying Veritas Operations Manager hot fixes

You can download and install hot fixes for Veritas Operations Manager in one of the following ways:

- Download from Symantec Operations Readiness Tolls (SORT) website. In the Management Server console, upload the hot fix to the repository using **Upload Solutions**, and then install.

- Use the Management Server console to download and install the hot fix.

You can upload multiple hot fixes to the repository.

Hot fixes are of the following types:

- Install on Management Server only.
- Install on managed host only.
- Install on Management Server and managed host.

In case of hot fixes that can be installed on Management Server and managed host, you need to first install the hot fix on Management Server, and then on the managed host.

Note: For deploying Symantec Storage Foundation High Availability hot fixes, you need to install the Patch Installer add-on. For more information on deploying Symantec Storage Foundation High Availability hot fixes using the Patch Installer add-on, refer to *Veritas Operations Manager Management Server Add-ons User Guide*.

See [“About deploying Veritas Operations Manager add-ons”](#) on page 97.

See [“About deploying maintenance release packages and patches”](#) on page 206.

See [“Downloading a Veritas Operations Manager add-on”](#) on page 98.

See [“Uploading a Veritas Operations Manager hot fix or package to the repository”](#) on page 208.

See [“Installing a Veritas Operations Manager hot fix, package, or patch”](#) on page 209.

About deploying maintenance release packages and patches

You can download and install the maintenance release packages and patches for Veritas Operations Manager that are **VOM Deployable** in one of the following ways.

- Download from Symantec Operations Readiness Tools (SORT) website. In the Management Server console, upload the package or patch to the repository using **Upload Solutions**, and then install.
- Use the Management Server console to download and install the package or patch.

Packages or patches for Veritas Operations Manager are available in tape archive (tar.gz) format, Storage Foundation archive (.sfa) format, or compress (.zip) format.

See [“About deploying Veritas Operations Manager add-ons”](#) on page 97.

See [“About deploying Veritas Operations Manager hot fixes”](#) on page 205.

See [“Downloading a Veritas Operations Manager add-on”](#) on page 98.

See [“Uploading a Veritas Operations Manager hot fix or package to the repository”](#) on page 208.

See [“Installing a Veritas Operations Manager hot fix, package, or patch”](#) on page 209.

About deploying base release packages

You can download and install the base release packages for Veritas Operations Manager that are **VOM Deployable** in one of the following ways.

- Download from Symantec Operations Readiness Tools (SORT) website. In the Management Server console, upload the package to the repository using **Upload Solutions**, and then install.
- Use the Management Server console to download and install the package.

See [“About deploying Veritas Operations Manager add-ons”](#) on page 97.

See [“About deploying Veritas Operations Manager hot fixes”](#) on page 205.

See [“Downloading a Veritas Operations Manager add-on”](#) on page 98.

See [“Uploading a Veritas Operations Manager hot fix or package to the repository”](#) on page 208.

See [“Installing a Veritas Operations Manager hot fix, package, or patch”](#) on page 209.

Downloading a hot fix, package, or patch

Using the Management Server console, you can download a hot fix, package, or patch on your local computer. You can download the hot fixes, packages, and patches for Veritas Operations Manager, Storage Foundation, and Symantec Storage Foundation High Availability products.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To download a hot fix, package, or patch

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**.

- 3 Locate the hot fix, package, or patch which you want to download.
 - 4 Right-click the hot fix, package, or patch, and select **Download** to download on your local computer.
- See [“Uploading a Veritas Operations Manager hot fix or package to the repository”](#) on page 208.
- See [“Installing a Veritas Operations Manager hot fix, package, or patch”](#) on page 209.

Uploading a Veritas Operations Manager hot fix or package to the repository

You need to download the hot fix or the package from the SORT website or using the Management Server console. After you upload the hot fix or package using the Management Server console, you need to install it, and then you can start using it.

You can upload a single package to the repository or upload all the packages together as a zip file.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To upload a Veritas Operations Manager hot fix or package to the repository

- 1 In the Home page on the Management Server console, click **Settings**.
 - 2 Do one of the following:
 - Click **Upload Solutions**.
 - Click **Deployment**, and then click **Upload Solutions**.
 - 3 In the **Upload Solutions to Repository** wizard panel, click **Browse** to select the hot fix or package that you want to upload.
- See [“Upload Solutions to Repository panel options”](#) on page 99.
- 4 Click **Upload** to upload to the repository.
 - 5 Click **Close**.

See [“Installing a Veritas Operations Manager hot fix, package, or patch”](#) on page 209.

See [“Removing a Veritas Operations Manager add-on from the repository”](#) on page 103.

See [“Uninstalling a Veritas Operations Manager add-on”](#) on page 102.

Installing a Veritas Operations Manager hot fix, package, or patch

Using the Management Server console, you can install a Veritas Operations Manager hot fix, package, or patch on the Management Server.

In case of hot fixes that can be installed on Management Server and managed host, you need to first install the hot fix on Management Server, and then on the managed host.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To install a Veritas Operations Manager hot fix, package, or patch

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**.
- 3 Expand **Hot Fixes**, **Maintenance Release**, or **Base Release** to select the hot fix, package, or patch.
- 4 Right-click the hot fix, package, or patch, click **Install**.
- 5 In the **Install -Download Add-on** wizard panel, select a download option and click **Next**.
See [“Install - Download hot fix, package, or patch panel options”](#) on page 209.
- 6 In the **Install Select hosts** wizard panel, select the managed hosts on which you want to install the hot fix, package, or patch, and click **Finish**.
See [“Install - Select hosts panel options”](#) on page 210.
- 7 In the **Result** panel, click **OK**

See [“Uninstalling a Veritas Operations Manager add-on”](#) on page 102.

See [“Removing a Veritas Operations Manager add-on from the repository”](#) on page 103.

See [“Canceling deployment request for a Veritas Operations Manager add-on”](#) on page 104.

See [“Viewing the details of an add-on, hot fix, package, or patch on SORT website”](#) on page 235.

Install - Download hot fix, package, or patch panel options

Use this wizard panel to select the download method for downloading a hot fix, package, or a patch.

Table 11-1 Select the download method for hot fix, package, or patch

Field	Description
Download from SORT	Select to download the hot fix, package, or patch from SORT website.
Available Packages	Displays the packages which are already downloaded on Management Server. Note: This list is displayed only when you choose to install a VOM deployable package.
Upload local copy	Select if you have already downloaded the hot fix, package, or patch from SORT website.
Proceed with available packages	Select if you have already downloaded the packages on Management Server. Note: This option is displayed only when you choose to install a VOM deployable package.

See [“Installing a Veritas Operations Manager hot fix, package, or patch”](#) on page 209.

See [“Upgrading managed hosts using the console”](#) on page 64.

Install - Select hosts panel options

Use this wizard panel to select the managed hosts on which you want to install the hot fix, package, or patch.

You can either select the hosts explicitly and install the hot fix, package, or patch on the selected hosts, or you can select the platform.

If you select a specific platform, the hot fix, package, or patch is installed on all the managed hosts using that platform. Also the hot fix, package, or patch will be installed on all the new managed hosts that are added to the domain in the future. For example, if you select Windows the hot fix, package, or patch is installed on all the hosts that use Windows platform. Also when a new Windows host is added to the domain, the hot fix, package, or patch is installed on the host.

Table 11-2 Select hosts panel options

Field	Description
Hosts	Select to view the list of all managed hosts where the hot fix, package, or patch is not installed. Select Show all applicable hosts (Overwrites existing installation) to list all the managed hosts on which you can install the hot fix, package, or patch. It includes: - Managed hosts on which the hot fix, package, or patch is not installed currently. - Managed hosts on which the hot fix, package, or patch is installed currently. In this case, Veritas Operations Manager overwrites the existing hot fix, package, or patch installation.
Platform	Select to install the hot fix, package, or patch on all managed hosts using the specific operating system. This option is useful to install the hot fix, package, or patch whenever a new managed host using the specific operating system is added to Management Server. Select Force install (Overwrites existing installation) to overwrite existing add-on installation on the managed hosts.

See [“Installing a Veritas Operations Manager hot fix, package, or patch”](#) on page 209.

See [“Upgrading managed hosts using the console”](#) on page 64.

Uninstalling a Veritas Operations Manager hot fix

You can uninstall only Veritas Operations Manager hot fixes from the Management Server and managed host.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To uninstall a Veritas Operations Manager hot fix

- 1 In the Home page on the Management Server console, click on **Settings**.
- 2 Click **Deployment**.
- 3 Expand **Hot Fixes** to locate the hot fix.
- 4 In the **Hot Fixes** tab, right-click the hot fix that you want to uninstall, select **Uninstall**.
- 5 In the **Uninstall** panel, review the information, and click **Yes**.

See [“Uninstall panel options”](#) on page 103.

See [“Installing a Veritas Operations Manager add-on”](#) on page 100.

See [“Installing a Veritas Operations Manager hot fix, package, or patch”](#) on page 209.

See [“Removing a Veritas Operations Manager add-on from the repository”](#) on page 103.

Removing a hot fix, package, or patch from the repository

You can remove a hot fix, package, or patch from the repository. Detailed information about the hot fix, package, or patch is not displayed in the **Repository** view within **Deployment**.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To remove a hot fix, package, or patch from the repository

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**.
- 3 Right-click the add-on, hot fix, package, or patch that you want to remove, select **Remove**.
- 4 In the **Remove** panel, click **Yes**.

See [“Remove panel options”](#) on page 104.

See [“Refreshing the repository”](#) on page 109.

See [“Installing a Veritas Operations Manager add-on”](#) on page 100.

See [“Installing a Veritas Operations Manager hot fix, package, or patch”](#) on page 209.

See [“Uninstalling a Veritas Operations Manager add-on”](#) on page 102.

Canceling deployment request for a hot fix, package, or patch

Using the Management Server console, you can cancel the deployment request for a Veritas Operations Manager hot fix, package, or patch.

Deployment requests are of two types, **Deploy by host** and **Deploy by platform**. **Deploy by host** type lets you select the hosts on which you want to deploy the hot fix, package, or patch. If you select **Deploy by platform**, then the hot fix, package, or patch is deployed on all the hosts having the selected platform.

Request of the type **Deploy by host** cannot be canceled.

If you initiate an install request of **Deploy by platform** type, then the request is applicable for all the existing hosts as well as the new hosts that are added to the Management Server domain on a later date. In case of **Deploy by platform** request, if you cancel the deployment request, the hot fix, package, or patch installation on all the existing hosts is completed. But the hot fix, package, or patch is not installed on the hosts that are added to the domain after cancellation of the deployment request.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To cancel deployment request for a hot fix, package, or patch

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**.
- 3 Expand **Hot Fixes** to locate the hot fix, package, or patch whose deployment request you want to cancel.
- 4 Select the **Requests** tab.
- 5 Right-click the request and select **Cancel Request**.
- 6 In the **Cancel Deployment Request** wizard panel, click **OK**.

See [“Cancel Deployment Request panel options”](#) on page 105.

See [“Installing a Veritas Operations Manager add-on”](#) on page 100.

See [“Installing a Veritas Operations Manager hot fix, package, or patch”](#) on page 209.

See [“Uninstalling a Veritas Operations Manager add-on”](#) on page 102.

Installing a Veritas Operations Manager hot fix on a specific managed host

Using the Management Server console, you can install the Veritas Operations Manager hot fix on the selected managed host. If the hot fix is already installed on the selected host, then Veritas Operations Manager overwrites the existing installation. It is referred to as a force installation.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To install a Veritas Operations Manager hot fix on a specific managed host

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**.
- 3 Expand **Hot Fixes** to select a hot fix.
- 4 In the **Applicable Hosts** tab, right-click the host, and select **Install**.
- 5 In the **Install** wizard panel, review the information, and click **OK**
See [“Install panel options”](#) on page 106.
- 6 In the **Install - Result** panel, click **OK**.

See [“About deploying Veritas Operations Manager add-ons”](#) on page 97.

See [“About deploying Veritas Operations Manager hot fixes”](#) on page 205.

Uninstalling a Veritas Operations Manager hot fix from a specific managed host

Using the Management Server console, you can uninstall the Veritas Operations Manager hot fix from the selected managed host. You can uninstall the add-on irrespective of its state (enabled or disabled).

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To uninstall a Veritas Operations Manager hot fix from a specific managed host

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**.
- 3 Expand **Hot Fixes** to select a hot fix.
- 4 In the **Applicable Hosts** tab, right-click the host, and select **Uninstall**.

- 5 In the **Uninstall** wizard panel, review the information, and click **OK**.
See [“Uninstall panel options”](#) on page 107.
- 6 In the **Uninstall - Result** panel, click **OK**.
See [“About deploying Veritas Operations Manager add-ons”](#) on page 97.
See [“About deploying Veritas Operations Manager hot fixes”](#) on page 205.

Configuring Management Server settings

This chapter includes the following topics:

- [Configuring the Management Server settings](#)
- [Configuring SMTP settings for email notifications](#)
- [Configuring SNMP trap settings for alert notifications](#)
- [Configuring the proxy server settings](#)
- [Enabling the analytics gathering on Management Server](#)
- [Setting the period for retaining the alert and the task logs in the database](#)
- [Configuring Web server settings](#)
- [Setting the generation time for subscribed reports](#)
- [Configuring advance authorization settings](#)
- [Enabling or disabling policy signatures for the data center](#)

Configuring the Management Server settings

You can perform the following tasks in the **Server settings** tab in **Management Server**:

Table 12-1 Management Server settings

Task	Description
Configuring SMTP settings	You can configure SMTP settings for Management Server to receive email notifications for alert rules or policy check scan completion, or to send a report by email. See “Configuring SMTP settings for email notifications” on page 218.
Configuring SNMP trap settings	You can configure SNMP trap for Management Server to receive notifications for alert rules. See “Configuring SNMP trap settings for alert notifications” on page 219.
Configuring proxy settings	You can download the information on the patch and the price tiers for Storage Foundation and High Availability products from the Symantec Operations Readiness Tools (SORT) website. If Management Server is not continuously connected to the Internet, you can set up an alternate proxy server that can access the website See “Configuring the proxy server settings” on page 220.
Analytics gathering settings	Veritas Operations Manager provides statistical information such as the frequency of use of particular features or views of the Veritas Operations Manager user interface in your organization to help analyze product usage. You can allow Symantec to analyze this data by enabling the analytics gathering feature on Management Server See “Enabling the analytics gathering on Management Server” on page 221.
Data retention policy settings	You can set the period for retaining the alert and the task logs using the Database Retention Policy Settings. See “Setting the period for retaining the alert and the task logs in the database” on page 222.

Table 12-1 Management Server settings (*continued*)

Task	Description
Web server settings	You can set the log levels, such as debug, info, or warning, for the log files using the Web Server setting. You can also set the user session timeout period time for the web server. See “Configuring Web server settings” on page 222.
Report subscription settings	You can create a report schedule so that the report is generated and shared with the subscribed users at the time and frequency that you specify. You can set the report schedule using Report run settings. See “Setting the generation time for subscribed reports” on page 223.
Configure advanced authorization	You can configure the advanced authorization settings to prompt the user to enter a reason for performing an operation. See “Configuring advance authorization settings” on page 224.
View active users	You can view the details of all the active users that are logged in to Management Server in the Environment tab. See “Viewing the details of active users logged in to Management Server” on page 240.

See [“Viewing the Management Server settings”](#) on page 240.

Configuring SMTP settings for email notifications

In the Management Server console, you can configure the SMTP setting for Management Server to receive email notifications. You must configure these settings to receive email notifications for alert rules or policy check scan completion, or to send a report by email.

You can also send a test email to the recipient's account to verify the SMTP settings that you have configured.

Enter the following details to configure the SMTP settings:

SMTP server	Valid formats for SMTP server include: Fully Qualified Domain Name (FQDN), IP address, or, if the network handles DNS resolution for host names, a shortened host name. Examples: Host123, Host123.example.com, xxx.yyy.zzz.aaa.
Sender account	The email address that is entered in the Sender account appears as the sender of all the emails that a rule sends out.
SMTP port	Enter the SMTP mail server port number.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To configure the SMTP settings for email notifications

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 In the **Settings** tab, click **Management Server**.
- 3 In the **Server settings** tab, under **SMTP settings**, do the following:
 - Enter the SMTP mail server host name in **SMTP server**.
 - Enter a valid email address in **Sender account**.
 - Enter the SMTP mail server port number in **SMTP port**.
- 4 Click **Save Settings**.

To verify the SMTP settings

- 1 In **SMTP Settings**, under **Test SMTP**, do the following:
 - Enter a valid email address of the recipient in **Recipient Account**.
 - Enter the test email message that you want to send to the recipient in **Test Message**.
- 2 Click **Send test mail**.

See [“Configuring the Management Server settings”](#) on page 216.

See [“Viewing the Management Server settings”](#) on page 240.

Configuring SNMP trap settings for alert notifications

Using the Management Server console, you can configure the SNMP trap settings.

When an event takes place, some objects that are not polled, send traps or unsolicited asynchronous SNMP messages to the server. Some of the rules that Veritas Operations Manager uses to monitor objects in the environment rely on SNMP trap-based messages.

Enter the following details to configure the SNMP trap settings:

SNMP server	Enter the IP Address or name of the host where the SNMP trap console is located. Visible only when SNMP Trap is selected. Example: Host123.example.com
SNMP port	Enter the SNMP port number. The default port for the trap is 162. You can edit the port number, if required.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To configure the SNMP trap settings for alert notifications

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 In the **Settings** tab, click **Management Server**.
- 3 In the **Server settings** tab, under **SNMP Trap settings**, do the following:
 - Enter the SNMP server host name in **SNMP server**.
 - Enter the SNMP server port number in **SNMP port**.
- 4 Click **Save Settings**.

See [“Configuring the Management Server settings”](#) on page 216.

See [“Viewing the Management Server settings”](#) on page 240.

Configuring the proxy server settings

In the Management Server console, when Management Server is not continuously connected to the Internet, you can use a proxy server to connect to SORT.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To configure the proxy server settings

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 In the **Settings** tab, click **Management Server**.

- 3 In the **Server settings** tab, under **Proxy settings**, do the following:
 - Enter the name or IP address of the proxy server in **Proxy server**.
 - Enter the port number of the proxy server in **Proxy server port**.
 - Enter the user name that you use to access the proxy server in **Proxy user**.
 - Enter the password that you use to access the proxy server in **Proxy password**.
 - 4 Click **Test SORT connectivity** to check the connectivity to SORT.
 - 5 Click **Save Settings**.
- See [“Configuring the Management Server settings”](#) on page 216.
- See [“Viewing the Management Server settings”](#) on page 240.

Enabling the analytics gathering on Management Server

Veritas Operations Manager uses Web beacons (also known as single pixel or clear GIFS) to provide statistical information such as the frequency of use of particular features or views of the Veritas Operations Manager user interface in your organization to help analyze product usage. The information does not identify the users. Symantec analyzes this data to understand the information that is of most interest to the customers and the features that the customers use most.

In the **Management Server, Server settings** view, you can enable analytics gathering on Management Server.

If the **Enable Analytics Gathering** check box is enabled while you configure Management Server, the **Enable Analytics Gathering** check box appears selected. Clear the **Enable Analytics Gathering** check box to disable analytics gathering on Management Server.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To enable analytics gathering on Management Server

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 In the **Settings** tab, click **Management Server**.
- 3 In the **Server settings** tab, under **Analytics gathering settings**, select **Enable Analytics Gathering**, and click **Save Settings**.

See [“Configuring the Management Server settings”](#) on page 216.

See [“Viewing the Management Server settings”](#) on page 240.

Setting the period for retaining the alert and the task logs in the database

In the **Management Server**, **Server setting** view, you can set the period for retaining the alert and the task logs. After this period, the alert and the task logs are removed from the Veritas Operations Manager database.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To set the period for retaining the alert and the task logs in the database

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 In the **Settings** tab, click **Management Server**.
- 3 In the **Server settings** tab, under **Database Retention Policy Settings**, select the number of days from the drop-down list in the following:
 - **Alert Log (Days)**
 - **Task Log (Days)**
- 4 Click **Save Settings**.

See [“Configuring the Management Server settings”](#) on page 216.

See [“Viewing the Management Server settings”](#) on page 240.

Configuring Web server settings

In the Management Server console, you can configure the following:

- Log level for the log files in the web server.
- User session timeout period for the web server.

You can select the following options for log level:

- Debug.
- Info
- Warning

By default, Veritas Operations Manager sets the log level as **Info**.

You can manage the user session timeout period for the web server. By default, the user session timeout period is 30 minutes. If you want to disable the user session timeout period for the web server, you must enter -1 in the **Timeout** field.

Although the default timeout period 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.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To configure the web server settings

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 In the **Settings** tab, click **Management Server**.
- 3 In the **Server settings** tab, under **Web Server Settings**, select the log level, and set the timeout period.
- 4 Click **Save Settings**

See [“Configuring the Management Server settings”](#) on page 216.

See [“Viewing the Management Server settings”](#) on page 240.

Setting the generation time for subscribed reports

You can use the Management Server console to create a report schedule for subscribed reports. You can specify the time of the day when the reports are to be generated and shared with the subscribers. The default time of the day is 1.00 AM.

For more information on reports, refer to the *Veritas Operations Manager Management Server User Guide*.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To set the generation time for subscribed reports

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 In the **Setting** tab, click **Management Server**.

3 In the **Server settings** tab, under **Report subscription settings**, select the time of the day.

4 Click **Save Settings**.

See [“Configuring the Management Server settings”](#) on page 216.

See [“Viewing the Management Server settings”](#) on page 240.

Configuring advance authorization settings

You can use the Management Server console to configure advance authorization settings. These settings are applicable for all operations that are performed on the Management Server console. The **Reason** panel appears after an operation is performed and the user is asked to enter a reason for performing the operation.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To configure advance authorization settings

1 In the Home page on the Management Server console, click **Settings**.

2 In the **Setting** tab, click **Management Server**.

3 In the **Server settings** tab, under **Advanced authorization**, select **Ask reason for all operations**.

4 Click **Save Settings**.

See [“Configuring the Management Server settings”](#) on page 216.

See [“Viewing the Management Server settings”](#) on page 240.

See [“Viewing audit information for Management Server”](#) on page 241.

Enabling or disabling policy signatures for the data center

In the Management Server console, you can enable or disable policy signatures for the data center. In the data center view, signatures are enabled by default.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

Note: Registered signatures can also be enabled or disabled from the perspectives where they are registered: for hosts on the **Server** perspective or for clusters on the **Availability** perspective. The most recent enable or disable operation takes precedence.

See the *Veritas Operations Manager Management Server User Guide*.

To enable or disable policy signatures for the data center

- 1 In the Home page, click **Settings**.
- 2 Click **Policy Signatures**.
- 3 Select one or more signatures to enable or disable.
- 4 Right-click and choose the appropriate menu option for the operation you want to perform.
 - **Enable Signatures**
 - **Disable Signatures**
- 5 Confirm to perform the operation on all hosts registered for that signature.

See [“Configuring the Management Server settings”](#) on page 216.

Setting up extended attributes

This chapter includes the following topics:

- [About using extended attributes](#)
- [Adding an extended attribute](#)
- [Modifying an extended attribute](#)
- [Deleting an extended attribute](#)

About using extended attributes

An extended attribute is an additional user-defined attribute that provides additional details about an object in Veritas Operations Manager. This information about an object is in addition to the details that Veritas Operations Manager discovers for that object. You can define multiple extended attributes on the objects using the Management Server console. You can use the extended attributes to search, filter, and sort the objects in the Management Server console. You can also manage the extended attributes using the Veritas Operations Manager Web services API.

You can define an extended attribute and associate it with the relevant objects. You need to set the value for the extended attribute when you associate it with the object.

[Table 13-1](#) lists the object types supporting extended attributes and the perspective to which these objects belong to.

Table 13-1 Object types supporting extended attributes

Objects	Perspective
Host, disk, disk group, volume, snapshot, exchange server, database	Server
Cluster, service group	Availability
Enclosure, switch, fabric, fabric zone	Storage
Virtualization server, virtual machine	Virtualization

You can set the value for the extended attribute on the objects in one of the following ways:

- By selecting an object in a perspective
- By searching and filtering the objects in the data center in a perspective

Note: For more information on setting the extended attribute value and Web services API, refer to the *Veritas Operations Manager Management Server User Guide*.

See [“Viewing the list of extended attributes”](#) on page 241.

See [“Adding an extended attribute”](#) on page 227.

Adding an extended attribute

Using the Management Server console, you can add one or more extended attributes for multiple object types. You can add up to 20 extended attributes on an object type. An extended attribute is displayed in the **Properties** column in the perspective view. You can right-click the attribute and select **Show as column** to display the attribute as a column in the table.

The extended attribute name can be same as the default attribute name of an object type. You cannot have two extended attributes having the same name.

For example, in the **Server** perspective, Veritas Operations Manager discovers the condition of a disk which is displayed in the **Condition** column. You can create an extended attribute named **Condition** on **Disk**. This extended attribute is displayed in the **Properties** panel. You cannot create two extended attributes with the same name for example **Condition** on **Disk**.

The maximum length of the extended attribute name can be 256 characters. It can contain alphanumeric characters, hyphen (-), and space.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To add an extended attribute

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Extended Attributes**.
- 3 In the **Extended Attribute** view, click **Add**.
- 4 In the **Add** panel, enter a name for the extended attribute, and select one or more object types. Click **Finish**.
- 5 In the **Add - Result** panel, click **Close**.

See [“About using extended attributes”](#) on page 226.

See [“Modifying an extended attribute”](#) on page 228.

See [“Viewing the list of extended attributes”](#) on page 241.

Modifying an extended attribute

Using the Management Server console, you can modify the name of an extended attribute. The name of the extended attribute should be unique.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To modify an extended attribute

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Extended Attributes**.
- 3 In the **Extended Attribute** view, right-click an extended attribute, and select **Modify**.
- 4 In the **Updated Name** field, enter a new name for the extended attribute, and click **OK**.
- 5 In the **Modify - Result** panel, click **Close**.

See [“About using extended attributes”](#) on page 226.

See [“Adding an extended attribute”](#) on page 227.

See [“Viewing the list of extended attributes”](#) on page 241.

Deleting an extended attribute

Using the Management Server console, you can delete an extended attribute. When you delete an extended attribute, the association with the objects is also deleted, and the extended attribute is not visible in the properties of the object.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To delete an extended attribute

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Extended Attributes**.
- 3 In the **Extended Attribute** view, right-click the extended attribute, and select **Delete**.
- 4 In the **Delete** panel, click **OK**.
- 5 In the **Delete - Result** panel, click **Close**.

See [“Adding an extended attribute”](#) on page 227.

See [“Modifying an extended attribute”](#) on page 228.

See [“Viewing the list of extended attributes”](#) on page 241.

Downloading price tier information from SORT

This chapter includes the following topics:

- [About assigning price tiers to hosts](#)
- [About updating the price tier information on Management Server](#)
- [Updating the price tier information automatically on Management Server](#)
- [Updating the price tier information manually on Management Server](#)

About assigning price tiers to hosts

You can use operating system-specific commands to find host characteristics. This includes the make and model of the host, processor type, and processor count. However, although you can discover hardware information for most hosts, you may not have all the characteristics of a host. In that case, it is called an "unknown tier".

The assign price tier feature lets you assign price tiers to an unknown host. It eliminates the need to find host characteristics manually.

You can assign a price tier to a host by selecting the server price tier, processors price tier, operating system price tier, or the Symantec Price Value Unit (SPVU) price tier.

See ["About updating the price tier information on Management Server"](#) on page 231.

See ["Updating the price tier information automatically on Management Server"](#) on page 232.

See ["Updating the price tier information manually on Management Server"](#) on page 232.

About updating the price tier information on Management Server

To find the appropriate price tier or the Symantec Performance Value Unit (SPVU) for the licenses of the Storage Foundation and high availability products that are installed on the managed hosts, Veritas Operations Manager requires the latest information on the price tiers for these products. Symantec updates the latest information of the price tiers on the Symantec Operations Readiness Tools (SORT) website. Management Server requires HTTPS connectivity with the SORT server for downloading this information.

The Veritas Operations Manager console provides you with various methods to update the price tier information on Management Server. You can use any one of the following methods to update the price tier information on Management Server:

- Configure Management Server to update the latest price tier information automatically when Management Server is continuously connected to the Internet.
- Set up a proxy server to update the latest price tier information automatically when Management Server is not connected to the Internet.
- Download a script file manually from Management Server when Management Server is not continuously connected to the Internet, or you cannot set up a proxy server. You must run the file on a Windows system that is connected to the Internet to extract a text file that contains the latest information on the price tiers, and upload the extracted text file to Management Server

The price tiers assigned to the managed hosts do not change automatically when you upload a new price tier file to Management Server. You need to manually assign the price tier to the host using the Veritas Operations Manager console.

The automatic update of the price tier information on a Management Server occurs according to the schedule set by you. By default, the price tier information is updated on Management Server on the first day of every month.

Note: Veritas Operations Manager downloads the price tier information from the SORT website only if a newer version is available on the website.

See [“About assigning price tiers to hosts”](#) on page 230.

See [“Updating the price tier information automatically on Management Server”](#) on page 232.

Updating the price tier information automatically on Management Server

You can configure Management Server to connect to the Symantec Operations Readiness Tool (SORT) website and update the price tier information automatically when Management Server is continuously connected to the Internet. When Management Server is not connected to Internet, you can use a proxy server to update the price tier information automatically. By default, the automatic download of the price tier information occurs on the first day of every month at 00.00 hours.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To update the price tier information automatically on Management Server

- 1 In the Home page on the Management Server console, click **Settings**.
 - 2 Click **SORT**.
 - 3 In the **Price Tier Download Settings** tab, under **Price Tier Automatic Download** do the following:
 - Select the day of the month from the drop-down list in **Day of month**.
 - Select the time of the day from the drop-down list in **Time of day**.
 - 4 Click **Save**.
 - 5 In the **Success** panel click **OK**, and click **Close**.
- See [“About updating the price tier information on Management Server”](#) on page 231.
- See [“Updating the price tier information manually on Management Server”](#) on page 232.
- See [“Configuring the proxy server settings”](#) on page 220.

Updating the price tier information manually on Management Server

You can update the price tier information manually when Management Server is not connected to the Internet, or you cannot set up a proxy server to access the Symantec Operations Readiness Tool (SORT) website

To do this, you must download the `pricetier.vbs` script file from Management Server and run it on a Windows system that has Internet connectivity. Extract the text file that contains the latest information on the price tiers. You must copy this

text file to the system where Management Server is running and manually upload this text file.

Note: You must use a Windows system to perform this operation.

To perform this task, your user group must be assigned the Admin role on the Management Server perspective.

To update the price tier information manually on Management Server

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **SORT**.
- 3 In the **Price Tier Download Settings** tab, under **Price Tier Manual Download** do the following:
 - Click **Download** to download the `pricetier.vbs` script.
 - Copy the `pricetier.vbs` file to a Windows system that has Internet connectivity.
 - Run the following command to extract the `pricetier.txt` file that contains the information on the price tiers:


```
cscript/NoLogo pricetier.vbs
```

Alternatively, you can double-click the script file to extract the text file. The `pricetier.txt` file is generated in the folder where you have downloaded the `pricetier.vbs` script file.
 - Copy the `pricetier.txt` file to the system where Management Server is running.
- 4 Click **Browse** to select the `pricetier.txt` file.
- 5 Click **Upload**.
- 6 Click **Close**.

See [“About updating the price tier information on Management Server”](#) on page 231.

See [“Updating the price tier information automatically on Management Server”](#) on page 232.

Viewing information on the Management Server environment

This chapter includes the following topics:

- [Viewing the details of an add-on, hot fix, package, or patch on SORT website](#)
- [Viewing the hosts configured in the Management Server domain](#)
- [Viewing the details of the authentication broker and the domains associated with the broker](#)
- [Viewing faults in the Management Server perspective](#)
- [Viewing the faults definitions](#)
- [Viewing details of alert logs](#)
- [Viewing the details of rules](#)
- [Viewing the details of active users logged in to Management Server](#)
- [Viewing the Management Server settings](#)
- [Viewing the list of extended attributes](#)
- [Viewing audit information for Management Server](#)
- [Viewing task information for the data center](#)
- [Viewing or exporting a list of available policy signatures](#)

Viewing the details of an add-on, hot fix, package, or patch on SORT website

Using the Management Server console, you can view the details of an add-on, hot fix, package, or patch on the SORT website.

You can view this information, if your user group has Admin role assigned on the Management Server perspective.

To view the details of an add-on, hot fix, package, or patch on the SORT website

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Deployment**.
- 3 Expand **Repository** to locate the add-on, hot fix, package, or patch whose details you want to view.
- 4 Right-click the add-on, hot fix, package, or patch, and select **Details** to view the details on the SORT website.

See [“Installing a Veritas Operations Manager add-on”](#) on page 100.

See [“Installing a Veritas Operations Manager hot fix, package, or patch”](#) on page 209.

Viewing the hosts configured in the Management Server domain

You can use the Management Server console to view the details of the hosts that are configured in the Management Server domain. You can view the details of hosts such as name, configuration type, status, platform, OS version, MH version, and the discovery state.

In this view you can perform the refresh and remove host tasks.

You can view this information, if your user group has Admin role assigned on the Management Server perspective. The root user can also view this information.

To view the hosts configured in the Management Server domain

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Host**.
- 3 Do one of the following to view the details of the configured hosts:
 - Select **Data Center** to view all the configured hosts.
 - Select **Agent** to view all the agent hosts.
 - Select **Agentless** to view all the agentless hosts.

See [“Refreshing the details of the managed host”](#) on page 146.

See [“Removing managed hosts from the Management Server domain”](#) on page 147.

Viewing the details of the authentication broker and the domains associated with the broker

Using the Management Server console, you can view the name of the authentication broker and the details of the domains that are associated with the broker.

In **Broker**, you can view the name of the authentication broker and the port number on which the authentication broker is configured to run.

You can view the following details for each authentication domain.

- Name of the authentication domain
- Type of the authentication domain
- Whether the authentication domain is enabled or disabled

You can perform the following tasks in this view:

- Configure LDAP/AD.
- Unconfigure the LDAP configuration.

You can view this information, if your user group has Admin role assigned on the Management Server perspective. The root user can also view this information.

To view the details of the authentication broker and the domains associated with the broker

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Security** to view the **Brokers & Domain** tab.

See [“About managing authentication brokers and authentication domains in the Veritas Operations Manager domain”](#) on page 149.

See [“Configuring Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server”](#) on page 151.

See [“Unconfiguring Lightweight Directory Access Protocol or Active Directory configuration from the authentication broker”](#) on page 156.

Viewing faults in the Management Server perspective

Using the Management Server console, you can view the system identified fault conditions. You can view the fault condition, the source of the fault, and the time when the fault occurred.

You can perform the following tasks in this view:

- Suppress the fault.
- Restore the suppress fault.
- Create a rule that determines the action that Management Server performs when it receives the alert that is related to a faulty entity.

You can view this information, if your user group has Admin role assigned on the Management Server perspective.

To view faults in the Management Server perspective

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Faults & Risks**.
- 3 Click the **Faults** tab.

See [“About faults and risks”](#) on page 179.

See [“Suppressing faults in the Management Server perspective”](#) on page 179.

See [“Restoring a suppressed fault in the Management Server perspective”](#) on page 181.

See [“Creating rules in the Management Server perspective”](#) on page 168.

Viewing the faults definitions

You can view a comprehensive list of all the fault definitions that Veritas Operations Manager uses to generate all faults. You can use this list to view the definitions of the faults that are already generated and yet to generate. Some of the information that you can obtain from this view:

- **Message:** Displays information about the fault.
- **Entity Type:** Displays the source object on which the fault occurs.
- **Affected Types:** Displays all the object types that are affected by the fault on the source object. For example, if a service group is faulted, it is listed under the **Entity Type** column. Since a service group is associated with managed hosts, clusters, and other objects, Veritas Operations Manager generates derived faults for these objects. All such associated objects are listed in this column.

You can perform the following tasks in this view:

- Suppress a fault.
- Restore a fault.

You can disable a fault definition by suppressing the fault. After the fault definition is disabled, all associated faults are automatically suppressed. You can suppress the fault definition until a specific date, or disable it forever.

Though the option to forever disable a fault definition is provided, you can again activate the fault definition using the **Restore Faults** option.

You can view this information, if your user group has Admin role assigned on the Management Server perspective.

To view the faults definitions

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Faults & Risks**.
- 3 Click the **Fault Definition** tab.

See [“About faults and risks”](#) on page 179.

See [“Suppressing a fault definition in the Management Server perspective”](#) on page 182.

See [“Restoring a suppressed fault definition in the Management Server perspective”](#) on page 183.

Viewing details of alert logs

Using the Management Server console, you can quickly ascertain the condition of all resources in the Veritas Operations Manager domain. The Alert Log displays alerts from all hosts that the Management Server manages. Alert logs are retained for 30 days.

You can view the following information:

- **Topic:** Displays the fault definition name.
- **Message:** Displays the message which is a part of the alert. You can view the name of the host on which the alert condition occurred.
- **Classification:** Displays the classification of the alert, for example, volume alert, subdisk alert, and path enabled.
- **Source Host:** Displays the host on which the alert condition occurred.
- **Time:** Displays the date and time when the alert was generated.

You can view this information, if your user group has Admin role assigned on the Management Server perspective.

To view details of alert logs

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Alert & Rules**.
- 3 Click the **Alert Log** tab.

See [“About alerts and rules”](#) on page 166.

Viewing the details of rules

You can view the details of alert rules in the Management Server console. You can view the name and description of the rule. The owner of the rule, last updated time, and whether the rule is enabled or disabled.

You can perform the following tasks in this view:

- Create a rule.
- Edit a rule.
- Enable a rule.
- Disable a rule.
- Delete a rule.

You can view this information, if your user group has Admin role assigned on the Management Server perspective.

To view the details of alert rules

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Alert & Rules**.
- 3 Click the **Rules** tab.

See [“Creating rules in the Management Server perspective”](#) on page 168.

See [“Editing rules in the Management Server perspective”](#) on page 172.

See [“Enabling rules in the Management Server perspective”](#) on page 177.

See [“Disabling rules in the Management Server perspective”](#) on page 178.

See [“Deleting rules in the Management Server perspective”](#) on page 176.

Viewing the details of active users logged in to Management Server

In the Management Server console, you can view the following details of the active users who are logged in to Management Server.

- User name with which the active user has logged in to Management Server.
- Date and time at which the user has logged in to Management Server.
- The time for which the user was idle.
- Host name or IP address of the host from which the user logs in.

You can view this information, if your user group has Admin role assigned on the Management Server perspective.

To view the details of active users logged in to Management Server

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Management Server**.
- 3 Click the **Environment** tab to view the details.

See [“Configuring the Management Server settings”](#) on page 216.

See [“Viewing the Management Server settings”](#) on page 240.

Viewing the Management Server settings

You can perform the following tasks in the Management Server settings view:

- Configure the SMTP settings for Management Server.
- Configure the SNMP trap settings for Management Server.
- Configure proxy server settings.
- Enable the analytics gathering on Management Server.
- Set the Database Retention policy.
- Set log levels for log files in the web server.
- Set report subscription settings.
- Set advance authorization settings.

You can view this information, if your user group has Admin role assigned on the Management Server perspective.

To view the Management Server settings

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Management Server** and click the **Server Settings** tab to view the settings.

See [“Configuring the Management Server settings”](#) on page 216.

Viewing the list of extended attributes

Using the Management Server console, you can view the list of all the extended attributes that are defined.

You can view the following details:

- Unique name of the extended attribute.
- Object type that is associated with the extended attribute.

You can perform the following tasks in this view:

- Add an extended attribute.
- Modify an existing extended attribute.
- Delete an extended attribute.

You can view this information, if your user group has Admin role assigned on the Management Server perspective.

To view the list of extended attributes

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Extended Attribute**.

See [“About using extended attributes”](#) on page 226.

See [“Adding an extended attribute”](#) on page 227.

See [“Modifying an extended attribute”](#) on page 228.

See [“Deleting an extended attribute”](#) on page 229.

Viewing audit information for Management Server

You can use the Management Server console to view audit information collected by Management Server. For audit purposes, Management Server collects information on all activities initiated using the Management Server console. This audit tracking also includes activities which were prevented from being carried out because they were not authorized.

Management Server collects the following audit information:

- The date and time of the activity.
- The activity, for example, configuring an enclosure.
- The location where the activity occurred.
- The target on which the activity was performed.
- The user.
- Whether the activity was authorized.
- The reason for the operation.
For a reason to be collected, the advanced authorization settings for Management Server must be enabled. If enabled, the Reason panel appears after an operation is performed and the user is asked to enter a reason for performing the operation. See [“Configuring advance authorization settings”](#) on page 224.

You can view this information, if your user group has Admin role assigned on the Management Server perspective.

You can also export the information to a file.

To view audit information for Management Server

- 1 In the Home page on the Management Server console, click **Settings** and select **Audit & Tasks**.
- 2 Click the **Audit** tab.

If you want to export the audit information, click the **Save** icon in the upper right of the tab.

Viewing task information for the data center

In the Management Server console, you can view information such as the following about all tasks performed in the data center:

- Task name
- State (completed, failed, and so on)
- The source, for example, a host or cluster
- The object
- The user
- Start and end time

You can view this information, if your user group has Admin role assigned on the Management Server perspective.

To view task information for the data center

- 1 In the Home page on the Management Server console, click **Settings** and select **Audit & Tasks**.
- 2 Click the **Tasks** tab.
- 3 To view more details about a task, right-click it and select **Properties**.

See [“Setting the period for retaining the alert and the task logs in the database”](#) on page 222.

Viewing or exporting a list of available policy signatures

In the Management Server console, you can view all policy signatures and export them to a file. You must have the appropriate permissions for the Veritas Operations Manager **Settings** perspective.

You can view this information, if your user group has Admin role assigned on the Management Server perspective.

To view or export a list of available policy signatures

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Policy Signatures**.
- 3 If you want to export the signatures to a file, click the **Save** icon in the upper right of the window.

Troubleshooting

This appendix includes the following topics:

- [Management Server \(MS\)](#)
- [Managed host \(MH\)](#)

Management Server (MS)

Veritas Operations Manager processes running on Management Server for Linux

- /opt/VRTSsfmcs/pgsql/bin/postgres
- /opt/VRTSsfmh/bin/xprtld
- /opt/VRTSsfmcs/webgui/jre/bin/java
- /opt/VRTSsfmcs/sec/bin/sfmsecd
- /opt/VRTSsfmh/bin/xtrapd

Commands to start and stop the Veritas Operations Manager processes on Management Server on Windows

`service` option of `vomadm` command can be used to start/stop the individual services and is the recommended method especially when the Management Server is configured for HA.

```
C:\Program Files\Veritas\VRTSsfmh\bin>perl.exe vomadm service {--start  
| --stop | --restart | --status | --version | --help}
```

Commands to start and stop the Veritas Operations Manager processes on Management Server on Linux

`service` option of `vomadm` command can be used to start/stop the individual services and is the recommended method especially when the Management Server is configured for HA.

```
/opt/VRTSsfmh/bin/vomadm service {--start | --stop | --restart |  
--status | --version | --help}
```

Veritas Operations Manager services running on Management Server for Windows

- Veritas Operations Manager Authentication Service
- Veritas Operations Manager Service
- Veritas Storage Foundation Messaging Service
- Veritas Operations Manager Database Service
- Veritas Operations Manager SNMP Trap Service

Management Server log file locations (Linux)

- General: `/var/opt/VRTSsfmcs/logs`
- Installer log file: `/var/opt/VRTSsfmh/logs/`
- DB engine: `/var/VRTSsfmcs/SFMdb3.dblog`

Management Server log file locations (Windows)

General: `%AllUsersAppData%\Symantec\VRTSsfmcs\logs`

Management Server database configuration and upgrade logs

`%AllUsersAppData%\Symantec\VRTSsfmcs\config_db`

Windows Installer log file

`C:\Program Files\Veritas\VRTSsfmcs\install.log`

Managed host (MH)

Veritas Operations Manager processes running on managed host on Unix/Linux

- `/opt/VRTSsfmh/bin/xprtld`
- `/opt/VRTSsfmh/bin/sfmh-discovery.pl`
- `/opt/VRTSsfmh/bin/vxdclid`

Commands to start and stop Veritas Operations Manager processes on managed host on UNIX/Linux

- **xprtld:** `/opt/VRTSsfmh/adm/xprtldctrl <start | stop>`
- **sfmh-discovery:** `/opt/VRTSsfmh/adm/vxvmdiscovery-ctrl.sh <start | stop>`
- **vxdclid:** `/opt/VRTSsfmh/etc/vxdcli.sh <start | stop | restart>`

Veritas Operations Manager services running on managed host on Windows

Veritas Storage Foundation Messaging Service

Note: sfmh-discovery and dcli processes do not run on a Windows managed host.

Managed host log files

- **UNIX/Linux:** `/var/opt/VRTSsfmh/logs`
- **Windows:** `C:\ProgramData\Symantec\VRTSsfmh\logs`

Gathering information for troubleshooting

Use the `vomgather.pl` script to gather logs for troubleshooting issues on Veritas Operations Manager Management Server and managed hosts:

- **On Unix/Linux:**
`/opt/VRTSsfmh/adm/vomgather.pl --dir mydir`
- **On Windows:**

```
"C:\Program Files\Veritas\VRTSsfmh\bin\perl.exe" "C:\Program
Files\Veritas\VRTSsfmh\adm\vomgather.pl" --dir mydir
```

where, *mydir* is the directory to store gathered data.

Use the `--full` option of `vomgather.pl` script to gather following data for troubleshooting issues:

- Management Server: Database, Spool, and store data
- Managed hosts: Spool data

Index

A

- about
 - communication between managed host and Management Server 112
- Active Directory removing 156
- ActiveX 34
- add-on
 - canceling deployment request 104
 - disabling 109
 - downloading 98
 - enabling 108
 - installing 100
 - removing 103
 - uninstalling 102
- advance authorization settings 224
- agentless discovery
 - about 116
 - Commands that require the root access 130
 - control hosts 123
 - Linux 124
 - prerequisites 124
 - privilege control software for UNIX hosts 132
 - remote hosts 123
 - requirements for deep array discovery 129
 - requirements for UNIX hosts 126
 - requirements for Windows hosts 128
 - SSH configuration requirements 133
 - supported features 120
 - UNIX 124
 - Windows 125
- alert log retention period 222
- alerts and rules 166
- array management capabilities 123
- assigning price tier
 - processor price tier 230
 - server price tier 230
- audit information 241
- authentication broker
 - managing 149
 - viewing 236

- authentication domains
 - managing 149
 - viewing 236

B

- backing up Veritas Operations Manager
 - on Linux 58–59
 - on Windows 60–61
- browsers 34

C

- configuring
 - Control Host 187
 - existing Management Server installation in HA environment 78
 - Management Server 43
 - Management Server in DR environment 80
 - Management Server in HA environment 71
 - Management Server in HADR environment 86
 - new Management Server installation in HA environment 72
 - virtualization discovery 196
- Configuring Management Server settings
 - advance authorization 224
 - report scheduling 223
- Control Host 123
 - discover VMware Virtualization Infrastructure 187

D

- deep array discovery 129
- deploying
 - add-ons 97
 - hot fixes 205
 - package 207
 - packages or patches 206
 - Veritas Operations Manager 23
- disable performance metering
 - VMware vCenter server 203
- domains 34

- downloading
 - managed host files 20
 - Management Server files 19
 - Veritas Operations Manager 19
- DR configuration 80
 - creating base service groups 83
 - enabling configuration 85
 - performing initial configuration 83
 - prerequisites 81

E

- enabling analytics gathering 221
- extended attribute
 - adding 227
 - deleting 229
 - modifying 228
 - using 226

F

- fault definition
 - restoring 183
 - suppressing 182
- faults
 - restoring 181
 - suppressing 179
 - viewing 237
- faults and risks 179
- fibre channel switch capabilities 123
- firewalls ports
 - ports 34

G

- gendeploy.pl 48

H

- HA configuration 71
 - completing the configuration 78
 - creating base service groups 75
 - modify default IP address and host name 80
 - performing initial configuration 74
 - prerequisites for existing MS 79
 - prerequisites for new MS 73
- HA-DR configuration
 - creating base service groups 89
 - enabling configuration 91
 - performing initial configuration 88
 - prerequisites 87
- HADR configuration 86

- host discovery 116
 - See also* agentless discovery of hosts
 - about 116
 - supported features 120
- hot fix
 - cancel deployment request 213
 - deploying 205
 - install on specific host 214
 - installing 209
 - removing 212
 - uninstall from specific host 214
 - uninstalling 211
 - uploading 208

I

- installation resources
 - Veritas Operations Manager 23
- installing
 - host management through Solaris JumpStart 48
 - managed host 44
 - managed host on UNIX 45
 - managed host on Windows 46
 - Management Server 39
 - Management Server on Linux 39
 - Management Server on Windows 41
- Intranet zone security level 34
- IPV 36

J

- JavaScript 34
- JScript 34

L

- LDAP
 - configuring authentication 151
 - removing 156
- LDom discovery
 - prerequisites 194
 - requirements 194

M

- managed host
 - add using gendeploy.pl 143
 - installation files for UNIX 45
 - installation files for Windows 46
 - installing 44
 - installing on UNIX 45
 - installing on Windows 46

- managed host *(continued)*
 - installing through Solaris JumpStart 48
 - package 39
 - removing 147
 - uninstalling on UNIX 69
 - uninstalling on Windows 70
 - upgrading 63
 - upgrading on UNIX 65
 - upgrading on Windows 66
 - verifying installation on UNIX 49
 - verifying installation on Windows 49
- managed hosts
 - refresh host details 146
 - upgrade using console 64
 - verifying version using the console 67
- Management Server
 - advance authorization settings 240
 - alert log retention period settings 222
 - analytics gathering 240
 - configuring 43
 - configuring a new installation in HA environment 72
 - configuring an existing installation in HA environment 78
 - configuring DR 80
 - configuring HA 71
 - configuring HADR 86
 - configuring proxy server 220
 - configuring settings 216
 - configuring SNMP trap 219
 - database retention policy 240
 - editing agentless hosts 145
 - enabling analytics gathering 221
 - installation files for Linux 39
 - installation files for Windows 41
 - installing 39
 - installing on Linux 39
 - installing on Windows 41
 - LDAP based authentication 151
 - package 39
 - proxy settings 240
 - remove managed host 147
 - report subscription settings 240
 - SMTP settings 240
 - SMTP settings for email 218
 - SNMP trap settings 240
 - task log retention period settings 222
 - uninstalling on Linux 68
 - uninstalling on Windows 68

- Management Server *(continued)*
 - upgrading 50
 - upgrading in HA DR environment 94
 - upgrading in HA environment 92
 - upgrading on Linux 53
 - upgrading on Windows 55
 - verifying installation on Linux 42
 - verifying installation on Windows 42
 - verifying version using the console 67
 - Web server settings 222
 - web server settings 240

N

- network requirements 34

O

- OpenSSH
 - about 135
 - installing on AIX 135
 - installing on Linux 135
 - installing on Solaris 136
- operating system requirements 27
- organization 157

P

- package
 - base release 207
 - cancel deployment request 213
 - deploying 207
 - installing 209
 - removing 212
 - uploading 208
- packages or patches
 - deploying 206
 - maintenance release 206
- patch
 - cancel deployment request 213
 - installing 209
 - removing 212
 - uploading 208
- performance metering
 - disable for VMware vCenter server 203
- permissions
 - assigning for perspective 158
 - deleting on perspective 160
 - modifying for perspective 159
- perspective
 - assigning permissions 158

- perspective (*continued*)
 - deleting permissions 160
 - modifying permissions 159
- policy checks
 - enabling or disabling signatures for data center 224
 - exporting signatures 243
- pop-up blockers 34
- price tier information
 - update automatically 232
 - update manually 232
- proxy server settings 220

R

- removing
 - Active Directory 156
 - LDAP 156
- report scheduling 223
- resolv.conf 34
- restoring Veritas Operations Manager
 - on Linux 59
 - on Windows 62
- roles 156
- rules
 - about 166
 - creating 168
 - deleting 176
 - disabling 178
 - editing 172
 - enabling 177

S

- security level 34
- signatures
 - exporting 243
- signatures for data center
 - enabling or disabling 224
- SNMP trap settings 219
- Solaris JumpStart installation 48
- solaris zones discovery
 - prerequisites 193
 - requirements 193
- space estimation data logs 29
- SSL 34
- system resource requirements 28

T

- task information for the data center 242

- task log retention period 222

- TCP 34

- toolbars 34

U

- UC 23

- UDP 34

- uninstalling

- add-on 102
- managed host on UNIX 69
- managed host on Windows 70
- Management Server on Linux 68
- Management Server on Windows 68

- upgrading

- disaster recovery 93
- HA 92
- HA-DR 93
- managed host 63
- managed host on UNIX 65
- managed host on Windows 66
- managed host using installer package 66
- managed host using operating system
 - commands 65
- managed hosts using console 64
- Management Server 50
- Management Server in HA DR environment 94
- Management Server in HA environment 92
- Management Server on Linux 53
- Management Server on Windows 55
- migrating objects and features 50

- upload

- add-on 99

- user

- restricting 160

- user group permissions

- assigning for perspective 158
- deleting on perspective 160
- modifying for perspective 159
- restricting 160

- UTC 23

V

- verifying

- managed host installation on UNIX 49
- managed host installation on Windows 49
- managed host version using the console 67
- Management Server installation on Linux 42
- Management Server installation on Windows 42

verifying *(continued)*

- Management Server version using the console 67

Veritas Operations Manager

- about 18
- backing up on Linux 58–59
- backing up on Windows 60–61
- choosing managed hosts 25
- choosing Management Server hosts 24
- choosing Web console hosts 34
- configuring for disaster recovery 80
- configuring for high availability 71
- configuring HADR 86
- configuring Management Server 43
- deployment configuration 23
- downloading 19
- downloading managed host files 20
- downloading Management Server files 19
- installation resources 23
- installing managed host on UNIX 45
- installing managed host on Windows 46
- installing Management Server on Linux 39
- installing Management Server on Windows 41
- IPV requirements 36
- network requirements 34
- operating systems 27
- organization 157
- packages 39
- restoring on Linux 59
- restoring on Windows 62
- system resource requirements 28
- uninstalling UNIX managed host 69
- upgrading managed host on UNIX 65
- upgrading managed host on Windows 66
- upgrading Management Server in HA DR environment 94
- upgrading Management Server in HA environment 92
- upgrading Management Server on Linux 53
- upgrading Management Server on Windows 55
- URL 19

Veritas Operations Manager deployment

- centralized management 24

Veritas Operations Manager HA

- configuring a new installation 72
- configuring an existing installation 78
- removing configuration 94
- upgrading 92

viewing

- alert log 238

viewing *(continued)*

- authentication broker 236
- authentication domains 236
- extended attributes 241

virtual machines

- cloning 47
- migrating 47

virtualization discovery

- configuring 196
- editing configuration 199
- refreshing configuration 202
- removing configuration 202

virtualization technology

- kernel-based virtual machine 186
- LPAR 186
- Microsoft Hyper-V 186
- Solaris LDom 186
- Solaris zones 186
- VMware 186

VMware discovery

- near real-time update of virtual machine states 189
- prerequisites 189
- requirements 189

VRTSsfmcs package 39

VRTSsfmh package 39, 44–45, 65

W

Web browsers requirements 34

Web console 34

Web server

- settings 222

web server

- CLI command 110
- restart 110

Web UI framework

- starting and stopping 114