Veritas InfoScale™ Operations Manager 8.0.2 Installation and Configuration Guide

VERITAS™

Last updated: 2023-12-27

Legal Notice

Copyright © 2023 Veritas Technologies LLC. All rights reserved.

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

This product may contain third-party software for which Veritas is required to provide attribution to the third-party (“Third-Party Programs”). Some of the Third-Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the third-party legal notices document accompanying this Veritas product or available at:
https://www.veritas.com/about/legal/license-agreements

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

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

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

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054
http://www.veritas.com

Technical Support

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

You can manage your Veritas account information at the following URL:
https://my.veritas.com

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

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

Documentation

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

Documentation feedback

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

You can also see documentation information or ask a question on the Veritas community site:
http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

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

Contents

Section 1 Installing and configuring Veritas InfoScale Operations Manager 14

Chapter 1 Planning your Veritas InfoScale Operations Manager installation 15

About Veritas InfoScale Operations Manager 15
Downloading Veritas InfoScale Operations Manager 8.0.2 16
Downloading Management Server files 17
Downloading managed host files 17
Using the product documentation 18
Host considerations for installing Veritas InfoScale Operations Manager 19
Typical Veritas InfoScale Operations Manager deployment configuration 20
Centralized management of Storage Foundation High Availability hosts 20
Veritas InfoScale Operations Manager 8.0.2 installation overview 21
Choosing a Management Server host 21
Choosing the managed hosts 22

Chapter 2 System requirements 23

Operating system requirements 23
Cloud (AWS, Azure, Google) deployment requirements 24
Third-party required libraries 25
32-bit SNIA Common HBA API required on Windows hosts 25
System resource requirements 25
About space estimation for data logs 27
About the frequency of managed host, enclosure and switch information discovery 30
Supported hardware 33
Web browser requirements 33
Network and firewall requirements 33
Internet Protocol version requirements 36

Proxy server requirements 36

Chapter 3 Installing, upgrading, and uninstalling Veritas InfoScale Operations Manager 38

Packages included in Veritas InfoScale Operations Manager 39
About installing Management Server 39
Installing Management Server on Linux (on premises and cloud) 40
Installing Management Server on Windows (on premises and cloud) 43
Verifying Management Server installation on Linux 42
Verifying Management Server installation on Windows 43
Configuring Veritas InfoScale Operations Manager on Linux and Windows 43
Implementing US Executive Order (EO) requirements 45
Configuring Veritas InfoScale Operations Manager Management Server and Agents in FIPS mode on Linux 46
Configuring Service groups using CLI script 49
Configuring Veritas InfoScale Operations Manager Management Server on Linux using CLI 51
Importing third-party certificates for xprtld 52
About installing managed host 54
Installing managed host on UNIX/Linux 55
Installing managed host on Windows 56
Installing managed host through Solaris JumpStart 57
About cloning virtual machines 58
About migrating virtual machines 58
Verifying managed host installation on UNIX 59
Verifying managed host installation on Windows 59
About upgrading Management Server 60
Upgrading Management Server on Linux 61
Upgrading Management Server on Windows 63
Migrating the managed hosts to 2048-bit certificate 65
About backing up and restoring Veritas InfoScale Operations Manager data 67
Taking regular backups of Veritas InfoScale Operations Manager data on Linux 68
Backing up Veritas InfoScale Operations Manager data on Linux before upgrading to version 8.0.2 69
Restoring backed up data on Linux 70
Taking regular backups of Veritas InfoScale Operations Manager data on Windows 71

Backing up Veritas InfoScale Operations Manager data on Windows before upgrading to version 8.0.2 72
Restoring backed up data on Windows 72
About upgrading managed hosts to Veritas InfoScale Operations Manager 8.0.2 74
Upgrading managed host using the console 74
Upgrading managed host on UNIX/Linux using operating system commands 75
Upgrading managed host on Windows using the installer package 76
Verifying the version of Management Server in the console 77
Verifying the version of a managed host in the console 78
Uninstalling Management Server on Linux 78
Uninstalling Management Server on Windows 79
Uninstalling managed host on UNIX 79
Uninstalling managed host on Windows 80

Chapter 4 Configuring Veritas InfoScale Operations Manager in a high availability and disaster recovery environment 81

Configuring the high availability feature in Veritas InfoScale Operations Manager 82
Configuring a new Veritas InfoScale Operations Manager installation in high availability environment 82
Configuring an existing Veritas InfoScale Operations Manager installation in high availability environment 90
Configuring CMS HA on Linux using Command Line (CLI) 92
Configuring Management Server in one-to-one DR environment 93
Prerequisites for configuring a Management Server in DR environment 94
Performing initial configuration of Management Server installation in DR environment 95
Creating the base service groups for DR configuration 96
Enabling DR configuration 98
Configuring Veritas InfoScale Operations Manager in high availability and disaster recovery environment 98
Prerequisites for configuring a Management Server in HA-DR environment 99
Performing initial configuration of Management Server installation in DR environment 100
Creating the base service groups for DR configuration 101
Enabling DR configuration 104

About upgrading the high availability configurations 104
Upgrading Management Server in high availability environment 105
About upgrading the high availability and disaster recovery configurations 106
Upgrading Management Server in high availability and disaster recovery environment 106
Removing the high availability configuration 107

Chapter 5 Installing and uninstalling Veritas InfoScale Operations Manager add-ons 108

About deploying Veritas InfoScale Operations Manager add-ons 109
Downloading a Veritas InfoScale Operations Manager add-on 110
Uploading a Veritas InfoScale Operations Manager add-on to the repository 111
Upload Solutions to Repository panel options 111
Installing a Veritas InfoScale Operations Manager add-on 112
Install - Download Add-on panel options 113
Install - Select hosts panel options for add-ons 113
Uninstalling a Veritas InfoScale Operations Manager add-on 114
Uninstall panel options 115
Removing a Veritas InfoScale Operations Manager add-on from the repository 115
Remove panel options 116
Canceling deployment request for a Veritas InfoScale Operations Manager add-on 116
Cancel Deployment Request panel options 117
Installing a Veritas InfoScale Operations Manager add-on on a specific managed host 118
Install panel options 118
Uninstalling a Veritas InfoScale Operations Manager add-on from a specific managed host 119
Uninstall panel options 119
Enabling a Veritas InfoScale Operations Manager add-on on a specific managed host 120
Disabling a Veritas InfoScale Operations Manager add-on from a specific managed host 121
Refreshing the repository 121
Restarting the web server 122

Section 2 Setting up the Management Server environment 123

Chapter 6 Basic Veritas InfoScale Operations Manager tasks 124

About the communication between the managed hosts and Management Server 124
Connecting to Veritas InfoScale Operations Manager Management Server 125
Stopping and starting the Web application 126
About the Management Server perspective 127

Chapter 7 Adding and managing hosts 128

Overview of host discovery 128
How Veritas InfoScale Operations Manager discovers hosts 128
Supported features for host discovery options 132
Overview of agentless discovery 134
About agentless discovery using the Control Host 135
About agentless discovery of remote hosts 135
Prerequisites for agentless configuration 136
How agentless discovery of a UNIX or Linux host works 136
How agentless discovery of a Windows host works 137
Requirements for agentless discovery of UNIX hosts 138
Requirements for agentless discovery of Windows hosts 140
Requirements for deep array discovery for agentless hosts 140
Commands that require the root access for agentless discovery of UNIX hosts 141
Using the privilege control software with agentless discovery of UNIX hosts 143
SSH configuration requirements for agentless discovery 144
About installing OpenSSH on a UNIX host 146
Adding the managed hosts to Management Server using an agent configuration 147
Add agent hosts panel options 148
Adding the managed hosts to Management Server using an agentless configuration 151
Add agentless hosts panel options 153
Adding Agentless hosts to the Management Server using Profile 154
Add agentless hosts panel options using Profile 155

Adding managed hosts to Management Server using the Auto Configure (gendeploy.pl) script 157
Editing the agentless host configuration 159
Edit agentless host panel options 160
Refreshing the details of the managed host 160
Removing managed hosts from the Management Server domain 161

Chapter 8 Setting up user access 163

About managing authentication brokers and authentication domains in the Veritas InfoScale Operations Manager domain 164
Adding Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server 165
Add LDAP/AD panel options 166
Add LDAP/AD panel options to specify the domain name 168
Unconfiguring Lightweight Directory Access Protocol or Active Directory configuration from the authentication broker 170
Configuring LDAP using CLI 170
Configuring an LDAP domain 171
Assigning permissions to a user group 172
Unconfiguring an existing LDAP configuration 173
Changing the password for a bind user 174
Configuring Single Sign-On in Veritas InfoScale Operations Manager 174
Enabling the authentication domain 178
Disabling the authentication domain 178
About predefined roles in Veritas InfoScale Operations Manager 179
About Organizations, objects, and roles in Veritas InfoScale Operations Manager 179
Assigning permissions to user groups for a perspective 181
Modifying permissions assigned to user groups for a perspective 182
Deleting permissions assigned to user groups on a perspective 183
Restricting users or user groups from accessing the Veritas InfoScale Operations Manager console 183
Example: Managing user access in Veritas InfoScale Operations Manager using Organizations and existing user groups 184

Chapter 9 Setting up fault monitoring 189

About alerts and rules 189
Creating rules in the Management Server perspective 191
Create Rule - Select the type of fault conditions to trigger this rule panel options 192

Create Rule - Select one or more fault topics which will trigger this rule panel options 193
Create Rule - Setup notifications panel options 193
Create Rule - Enter name and description panel options 194
Editing rules in the Management Server perspective 195
Edit Rule - Select the type of fault condition to trigger this rule panel options 196
Edit Rule - Select one or more fault topics which will trigger this rule panel options 197
Edit Rule - Setup notifications panel options 197
Edit Rule - Enter name and description panel options 198
Deleting rules in the Management Server perspective 199
Delete Rule panel options 199
Enabling rules in the Management Server perspective 200
Enable Rule panel options 200
Disabling rules in the Management Server perspective 200
Disable Rule panel options 201
About faults and risks 201
Suppressing faults in the Management Server perspective 202
Suppress Faults panel options 202
Restoring a suppressed fault in the Management Server perspective 203
Suppressing a fault definition in the Management Server perspective 204
Suppress the fault definition panel options 205
Restoring a suppressed fault definition in the Management Server perspective 205

Chapter 10 Setting up virtualization environment discovery 207

About the virtualization technologies supported 208
About Control Hosts in Veritas InfoScale Operations Manager 209
Requirements for discovering vCenter and ESX servers using Veritas InfoScale Operations Manager 210
About near real-time discovery of VMware events 211
Setting up near real-time discovery of VMware events 212
Configuring the VMware vCenter Server to generate SNMP traps 214
Configuration settings for VMware vCenter discovery 216
Requirements for discovering the Solaris zones 217
Requirements for the zlogin utility on non-Global Zones 218
Requirements for devices exported to non-Global Zones 218

Requirements for file systems exported to non-Global Zones 218
Requirements for discovering Solaris Logical domains 219
Requirements for discovering logical partitions 219
Requirements for Microsoft Hyper-V virtualization discovery 220
Requirements for Kernel-based Virtual Machine (KVM) virtualization discovery 220
Adding a virtualization server 221
Add Virtualization Server panel options 222
Add Virtualization Server panel options 223
Editing a virtualization discovery configuration 224
Edit Configuration panel options 224
Edit Configuration panel options for method selection 225
Refreshing a virtualization discovery configuration 226
Refreshing an ESX Server discovery 226
Removing a virtualization discovery configuration 227
Configuring performance metering for a VMware vCenter server 228
Disable performance metering for a VMware vCenter server 228

Chapter 11 Deploying hot fixes, packages, and patches 230

About deploying Veritas InfoScale Operations Manager hot fixes 230
About deploying maintenance release packages and patches 231
About deploying base release packages 232
Downloading a hot fix, package, or patch 232
Uploading a Veritas InfoScale Operations Manager hot fix or package to the repository 233
Installing a Veritas InfoScale Operations Manager hot fix, package, or patch 234
Install - Download hot fix, package, or patch panel options 234
Install - Select hosts panel options 235
Removing a hot fix, package, or patch from the repository 236
Canceling deployment request for a hot fix, package, or patch 237
Installing a Veritas InfoScale Operations Manager hot fix on a specific managed host 238

Chapter 12 Configuring Management Server settings 239

Configuring the Management Server settings 239
Configuring SMTP settings for email notifications 242
Configuring SNMP trap settings for alert notifications 243
Configuring SNMPv3 settings 244
Configuring the proxy server settings 245
Configuring two-factor authentication (2FA) 246

Setting the period for retaining the alert and the task logs in the database 246
Configuring Web server settings 247
Setting the generation time for subscribed reports 248
Configuring advance authorization settings 248
Enabling or disabling policy signatures for the data center 249
Forwarding audit logs 249

Chapter 13 Setting up extended attributes 251

About using extended attributes 251
Adding an extended attribute 252
Modifying an extended attribute 253
Deleting an extended attribute 253

Chapter 14 Viewing information on the Management Server environment 255

Viewing the details of an add-on, hot fix, package, or patch on SORT website 256
Viewing the hosts configured in the Management Server domain 256
Viewing the details of the authentication broker and the domains associated with the broker 257
Viewing faults in the Management Server perspective 258
Viewing the faults definitions 258
Viewing details of alert logs 259
Viewing the details of rules 260
Viewing the details of active users logged in to Management Server 261
Viewing the Management Server settings 261
Viewing the list of extended attributes 262
Viewing audit information for Management Server 262
Viewing task information for the data center 263
Viewing or exporting a list of available policy signatures 264

Appendix A Troubleshooting 265

Management Server (MS) 265
Veritas InfoScale Operations Manager processes running on Management Server for Linux 265
Veritas InfoScale Operations Manager services running on Management Server for Windows 265
Commands to start and stop the Veritas InfoScale Operations Manager processes on Management Server on Linux 266

Commands to start and stop the Veritas InfoScale Operations Manager processes on Management Server on Windows 266
Management Server log file locations on Linux 266
Management Server log file locations on Windows 266
Managed host (MH) 267
Veritas InfoScale Operations Manager processes running on managed host on Unix/Linux 267
Veritas InfoScale Operations Manager services running on managed host on Windows 267
Commands to start and stop Veritas InfoScale Operations Manager processes on managed host on UNIX/Linux 267
Managed host log files 267
Agentless driver log files 267
Gathering information for troubleshooting 268

Index 269

Section 1

Installing and configuring Veritas InfoScale Operations Manager

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

Chapter 1

Planning your Veritas InfoScale Operations Manager installation

This chapter includes the following topics:

- About Veritas InfoScale Operations Manager
- Downloading Veritas InfoScale Operations Manager 8.0.2
- Using the product documentation
- Host considerations for installing Veritas InfoScale Operations Manager
- Typical Veritas InfoScale Operations Manager deployment configuration
- Veritas InfoScale Operations Manager 8.0.2 installation overview
- Choosing a Management Server host
- Choosing the managed hosts

About Veritas InfoScale Operations Manager

Veritas InfoScale Operations Manager by Veritas gives you a single, centralized management console for the 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 InfoScale Operations Manager helps administrators centrally manage diverse data center environments.

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

Veritas InfoScale Operations Manager uses two-factor authentication (2FA) to protect user accounts from getting compromised. A combination of your login credentials and a six-digit PIN is used to authenticate every user account. On gaining access to the management console, 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 InfoScale Operations Manager deployment consists of the following:

- Management Server
- Managed hosts

A Veritas InfoScale Operations Manager deployment may also discover the following:

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

Downloading Veritas InfoScale Operations Manager 8.0.2

You can download Veritas InfoScale Operations Manager 8.0.2 packages from the following URL:

https://www.veritas.com/support/

1. Click the **Downloads** icon.
2. Select **InfoScale & Storage Foundation** from the **Product** filter in the left pane.
3. Select the appropriate component from the **Sub product** filter if you want to narrow down the search results in the right pane.
4. Select the version that you want to download and click **Explore**.

See “Downloading Management Server files” on page 17.

See “Downloading managed host files” on page 17.

Downloading Management Server files

To install or upgrade Veritas InfoScale 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 InfoScale Operations Manager 8.0.2 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 Veritas InfoScale Operations Manager Help Add-on.

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

- Linux:
  - Download file name:
    - For Management server along with the add-ons- `Veritas_InfoScale_Operations_Manager_Management_Server_8.0.2_Linux_Full.tar.gz`
  - Installer file name:
    - For Management server along with the add-ons- `Veritas_InfoScale_Operations_Manager_MS_8.0.2_Linux_Full.bin`
- Windows:
  - Download file name:
    - For Management server along with the add-ons- `Veritas_InfoScale_Operations_Manager_Management_Server_8.0.2_Win_Full.zip`
  - Installer file name:
    - For Management server along with the add-ons- `Veritas_InfoScale_Operations_Manager_MS_8.0.2_Win_Full.exe`

See "About installing Management Server" on page 39.

See "About upgrading Management Server" on page 60.

Downloading managed host files

To install or upgrade host management, you need to download the `Veritas_InfoScale_Operations_Manager_Managed_Host_Bundle_8.0.2.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 InfoScale Operations Manager 8.0.2, you can choose to use the Deployment Management feature.

See "About deploying maintenance release packages and patches" on page 231.

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_8.0.2.0_AIX.bff.Z`
Linux	`VRTSsfmh_8.0.2.0_Linux.rpm`
Solaris 11 on SPARC	`VRTSsfmh_8.0.2.0_SunOS_arch_sparc_osr_5.11.p5p`
Solaris 11 on x86	`VRTSsfmh_8.0.2.0_SunOS_arch_i386_osr_5.11.p5p`
Windows 64-bit	`VRTSsfmh_8.0.2.0_Windows_arch_x64.msi`

See "About installing managed host" on page 54.

See "About upgrading managed hosts to Veritas InfoScale Operations Manager 8.0.2" on page 74.

Using the product documentation

Table 1-2 Names of Veritas InfoScale Operations Manager Guides

Title	Description
Veritas InfoScale Operations Manager Hardware and Software Compatibility List (HSCL)	The list of hardware and software compatibility, available here: https://www.veritas.com/support/en_US/doc/viom_hscl_802
Veritas InfoScale Operations Manager Release Notes	The release information such as new features, fixed issues, known issues, and limitations.
Veritas InfoScale Operations Manager Installation and Configuration Guide *Veritas InfoScale Operations Manager User Guide* *Veritas InfoScale Operations Manager Add-ons User Guide*	The information about Veritas InfoScale Operations Manager.

Table 1-2 Names of Veritas InfoScale Operations Manager Guides *(continued)*

Title	Description
Veritas InfoScale Operations Manager Frequently Asked Questions	A list of frequently asked questions about Veritas InfoScale Operations Manager.
Veritas InfoScale Operations Manager Third-Party License Agreements	The information about the third-party software that is used in Veritas InfoScale Operations Manager.
Veritas InfoScale Operations Manager Quick Start Guide	The short and concise information about installation, configuration, and discovery of assets in Veritas InfoScale Operations Manager.

Table 1-3 URLs for Veritas InfoScale Operations Manager documentation

URL	Description
https://sort.veritas.com/documents	The latest version of the product documentation.
https://www.veritas.com/content/support/en_US/article.100051901	The late breaking news that is related to this release.

Veritas InfoScale Operations Manager help content is hosted on the web and is accessed when you launch the product help. The help content can be updated independently of product release.

Host considerations for installing Veritas InfoScale Operations Manager

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

- Before you begin the Veritas InfoScale 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 Storage Foundation High Availability to be entitled to use Veritas InfoScale Operations Manager.

See “About installing Management Server” on page 39.

See "About installing managed host" on page 54.

Typical Veritas InfoScale Operations Manager deployment configuration

If you implement centralized management, a typical full installation of Veritas InfoScale 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 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 InfoScale Operations Manager 8.0.2" on page 16.

Centralized management of Storage Foundation High Availability hosts

In this deployment scenario, you can centrally manage the Storage Foundation High Availability hosts. We recommend this deployment because centralized management offers you the flexibility of performing operations on multiple 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 InfoScale Operations Manager deployment configuration" on page 20.

Veritas InfoScale Operations Manager 8.0.2 installation overview

Installing Veritas InfoScale Operations Manager involves the following:

- Reviewing the Veritas InfoScale Operations Manager architecture and typical deployment configurations
  See "Typical Veritas InfoScale Operations Manager deployment configuration" on page 20.
- Verifying that you have met system requirements
  See "Operating system requirements" on page 23.
  See "System resource requirements" on page 25.
  See "Supported hardware" on page 33.
  See "Web browser requirements" on page 33.
  See "Network and firewall requirements" on page 33.
- Installing and configuring the Veritas InfoScale Operations Manager Management Server
  See "About installing Management Server" on page 39.
  See "Configuring Veritas InfoScale Operations Manager on Linux and Windows" on page 43.
- Installing Veritas InfoScale Operations Manager host management on the hosts that will be centrally managed
  See "About installing managed host" on page 54.

Choosing a Management Server host

Management Server is the central piece of the Veritas InfoScale 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 "Operating system requirements" on page 23.
  See "32-bit SNIA Common HBA API required on Windows hosts" on page 25.
  See "System resource requirements" on page 25.
  See "Web browser requirements" on page 33.
  See "Network and firewall requirements" on page 33.

- 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 InfoScale 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 InfoScale Operations Manager Hardware and Software Compatibility List (HSCL).*

Choosing the managed hosts

A typical Veritas InfoScale 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 InfoScale 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 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 Storage Foundation High Availability products installed on them.

For more information on agent and agentless hosts, see the *Veritas InfoScale Operations Manager 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 InfoScale Operations Manager Hardware and Software Compatibility List (HSCL).*

See “Operating system requirements” on page 23.

Chapter 2

System requirements

This chapter includes the following topics:

- Operating system requirements
- Cloud (AWS, Azure, Google) deployment requirements
- Third-party required libraries
- System resource requirements
- Supported hardware
- Web browser requirements
- Network and firewall requirements
- Proxy server requirements

Operating system requirements

For information on Operating system requirements for Veritas InfoScale Operations Manager 8.0.2, refer to the *Veritas InfoScale Operations Manager Hardware and Software Compatibility List (HSCL)* at the following URL:

https://www.veritas.com/support/en_US/doc/viom_hscl_802

See “System resource requirements” on page 25.

Cloud (AWS, Azure, Google) deployment requirements

This section explains the system resource requirement and prerequisites for the deployment of Veritas InfoScale Operations Manager Management Server on cloud environment.

- Make sure that the swap memory is properly configured, if the swap memory is not already configured then use the below commands to configure the swap memory:
  Following is the example for 1 GB swap memory.
  ```
  sudo dd if=/dev/zero of=/swapf1 bs=1024 count=1048576
  sudo chmod 600 /swapf1
  mkswap /swapf1
  sudo swapon /swap
  ```
  Add swap entry in `/etc/fstab` file.
  ```
  /swapf1 swap swap defaults 0 0
  ```
- Verify that the `libltdl.so.7` file is present on the server. If it is not found then install it using below command:
  On **RHEL platform**, install `libltdl lib` using yum utility
  # yum install `-y libtool-ltdl`
  Verify `libltdl.so.7` file under `/lib64` directory after installed.
  ```
  # ls -ltra /usr/lib64/libltdl.so.7
  ```
  On **SLES platform**, install `libtool` using zypper utility
  # zypper install `libtool`
  Verify `libltdl.so.7` file under `/usr/lib64`
  ```
  # ls -ltra /usr/lib64/libltdl.so.7
  ```
- Permit root or root level access for Veritas InfoScale Operations Manager installation and configuration.
  For Network, firewall requirements and System requirements, see Chapter 2 in *Veritas InfoScale™ Operations Manager 8.0.2 Installation and Configuration Guide*.

Hostname and IP should be added in `/etc/hosts` file.

For example: Ex: xxx.xxx.xxx.xxx example.domain.com example

Note: If DNS is not configured, then please add MH (Managed Hosts) entry in Veritas InfoScale Operations Manager under `/etc/hosts` file. Similarly, Veritas InfoScale Operations Manager entry should be added in MH under `/etc/hosts` file.

Third-party required libraries

This section lists third-party libraries required to run Veritas InfoScale 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 InfoScale 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 InfoScale 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 InfoScale 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)	6	8GB	20GB
Medium (up to 1500 managed hosts)	8	16GB	30GB
Large (up to 3500 managed hosts)	16	32GB	40GB

- Add 8GB of memory and 10GB disk space if Management Server is used for the deep discovery of enclosures using Storage Insight Add-on.
- Add 8GB of memory and 10GB disk space if Management Server is used for the discovery of virtualization infrastructure.

Additional considerations for system resource requirements for Veritas InfoScale 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 8GB 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: 8GB for agentless discovery of every 1000 managed hosts. Add 15GB 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, here:

https://www.veritas.com/support/en_US/article.100051901

About space estimation for data logs

In Veritas InfoScale 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 InfoScale 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 InfoScale 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
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

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
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

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

Name of resource	Number of resources	Metrics collected	Interval of collection	Duration of collection	Size in KB	Size in KB for a single object
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 discovery 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	Cluster Server and the related 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.

Family	Frequency in minutes	Discovered information
PCV_NOTIFY	30	Policy check violations computed on Management Server and on managed hosts earlier than 6.1. Violations computed on managed hosts 6.1 or later do not require separate discovery.
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.

Family	Frequency in minutes	Discovered information
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.
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.
VVRBW	60	Bandwidth usage information for Volume Replicator (VVR).

Family	Frequency in minutes	Discovered information
Docker	120	Docker containters, docker images, and storage exported to containers.

Note: The discovery for the Storage Foundation and 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 InfoScale 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.

See "System resource requirements" on page 25.

Supported hardware

For information on supported hardware for Veritas InfoScale Operations Manager 8.0.2, refer to the Veritas InfoScale Operations Manager Hardware and Software Compatibility List (HSCL) at the following URL:

https://www.veritas.com/support/en_US/doc/viom_hscl_802

See "Operating system requirements" on page 23.

See "System resource requirements" on page 25.

Web browser requirements

For information on Web browser requirements for Veritas InfoScale Operations Manager 8.0.2, refer to the *Veritas InfoScale Operations Manager Hardware and Software Compatibility List (HSCL)*.

https://www.veritas.com/support/en_US/doc/viom_hscl_802

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 InfoScale 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 InfoScale Operations Manager uses the default ports as shown in Table 2-3 to transfer information.

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

Port	Protocol	Initiator	Purpose	Effect if blocked
5634	TCP	Management Server	Management Server configuration	Management Server cannot be configured.
5636	TCP	Management Server	Management Server database 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.

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

Port	Protocol	Initiator	Purpose	Effect if blocked
22			SSH communication	
135			WMI communication	
14161	TCP	Web browser	Run the Management Server console	Users cannot access the Management Server console.
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.

See “Operating system requirements” on page 23.

See “System resource requirements” on page 25.

Internet Protocol version requirements

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

Table 2-4 describes the Veritas InfoScale Operations Manager support for IPV4 and IPV6:

Table 2-4 IPV4 and IPV6 support

Components	IPV6	IPV4	Mixed Mode ((IPv4 and IPv6))
Management Server	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 33.

Proxy server requirements

If a proxy server is configured along with Veritas InfoScale Operations Manager Management Server, the proxy server should have the following capabilities:

- Proxy server should support GET, POST, and CONNECT methods.
- There should be connectivity between Management Server and the proxy server.
- There should be connectivity between the proxy server and the resources that Management Server needs to access. For example, SORT Web services.

Table 2-5 lists the default ports that a proxy server uses to communicate with other resources:

Table 2-5 Default ports for proxy server

Protocol	Port	Effect if blocked
HTTP	80	Management Server cannot connect to SORT.

Table 2-5 Default ports for proxy server *(continued)*

Protocol	Port	Effect if blocked
HTTPS	443	Management Server cannot connect to SORT.
FTP	21	Management Server cannot download patches/updates from SORT.
SFTP	22	Management Server cannot download patches/updates from SORT.

See "System resource requirements" on page 25.

Chapter 3

Installing, upgrading, and uninstalling Veritas InfoScale Operations Manager

This chapter includes the following topics:

- Packages included in Veritas InfoScale Operations Manager
- About installing Management Server
- Verifying Management Server installation on Linux
- Verifying Management Server installation on Windows
- Configuring Veritas InfoScale Operations Manager on Linux and Windows
- Implementing US Executive Order (EO) requirements
- Configuring Veritas InfoScale Operations Manager Management Server and Agents in FIPS mode on Linux
- Configuring Service groups using CLI script
- Configuring Veritas InfoScale Operations Manager Management Server on Linux using CLI
- Importing third-party certificates for xprtld
- About installing managed host
- Verifying managed host installation on UNIX

- Verifying managed host installation on Windows
- About upgrading Management Server
- About backing up and restoring Veritas InfoScale Operations Manager data
- About upgrading managed hosts to Veritas InfoScale Operations Manager 8.0.2
- 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 managed host on Windows

Packages included in Veritas InfoScale Operations Manager

Table 3-1 lists the software packages that are included in Veritas InfoScale Operations Manager.

Table 3-1 Software packages

Package name	Description
VRTSsfmcs	Veritas InfoScale Operations Manager package that is required on Management Server.
VRTSsfmh	Veritas InfoScale 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 InfoScale Operations Manager 8.0.2” on page 16.

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 InfoScale Operations Manager before you can use it.

See "Installing Management Server on Linux (on premises and cloud)" on page 40.

See "Installing Management Server on Windows (on premises and cloud)" on page 43.

Installing Management Server on Linux (on premises and cloud)

You can install the Veritas InfoScale Operations Manager Management Server on a Linux host using the following file:

- For Management server along with the add-ons:
  `Veritas_InfoScale_Operations_Manager_MS_8.0.2_Linux_Full.bin`

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

Note: By default, the `VRTSsfmcs` and the `VRTSsfmh` packages are installed in the `/opt` directory. You cannot specify a different location to install the packages.

You can install Veritas InfoScale Operations Manager Management Server on AWS, Azure, and Google cloud. The procedure for installing Veritas InfoScale Operations Manager Management Server on AWS, Azure, and Google cloud is same as follows.

To install Veritas InfoScale 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.

2. Download and unzip the installation file.

   See "Downloading Management Server files" on page 17.

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 the following directory:

   - **`./Veritas_InfoScale_Operations_Manager_MS_8.0.2_Linux_Full.bin`**

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

   - **`chmod +x Veritas_InfoScale_Operations_Manager_MS_8.0.2_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
Veritas InfoScale Operations Manager Management Server.

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

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

or, run `"/opt/VRTSsfmh/bin/perl /opt/VRTSsfmcs/bin/cli_cms_config.pl"` command in your terminal.

```
Please skip this step if you intend to use this host as a standby
node for Veritas InfoScale 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 InfoScale Operations Manager.

See "Configuring Veritas InfoScale Operations Manager on Linux and Windows" on page 43.

Installing Management Server on Windows (on premises and cloud)

You can install the Veritas InfoScale Operations Manager Management Server on a Windows host using the following file:

- For Management server along with the add-ons:
  `Veritas_InfoScale_Operations_Manager_MS_8.0.2_Win_Full.exe`

Note: By default, the `VRTSsfmcs` and `VRTSsfmh` packages are installed in the system drive. You cannot specify a different location to install the package.

You can install Veritas InfoScale Operations Manager Management Server on AWS, Azure, and Google cloud. The procedure for installing Veritas InfoScale Operations Manager Management Server on AWS, Azure, and Google cloud is same as follows.

To install Veritas InfoScale 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.

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 InfoScale Operations Manager 8.0.2" on page 16.
4. Turn off the Windows firewall, or, open ports 5634 and 14161 for TCP/IP communication.
5. Ensure that there is no restart pending from Windows Update. If there is, restart the host before launching the installer.
6. Make sure that the value for environment variable PATHEXT on the target host includes the extensions .exe, .bat, and .vbs.
7. To launch the installer, run the `Veritas_InfoScale_Operations_Manager_MS_8.0.2_Win_Full.exe` file.
8. To proceed with the Management Server installation, accept the End User License Agreement.
9. Click **Next** and follow through the installation process.
10. After the installation is complete, select **Launch Veritas InfoScale Operations Manager configuration** to configure Veritas InfoScale Operations Manager.

    You can choose to configure Veritas InfoScale Operations Manager later using the **https://*hostname*:5634/** URL.

    Where, *hostname* is the fully qualified name of the host.
11. Click **Finish**.
12. Configure Veritas InfoScale Operations Manager.

    See "Configuring Veritas InfoScale Operations Manager on Linux and Windows" on page 43.
13. Verify that Management Server is installed and the required services are started.

    See "Verifying Management Server installation on Windows" on page 43.

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
   ```

See "Installing Management Server on Linux (on premises and cloud)" on page 40.

Verifying Management Server installation on Windows

You can verify the Management Server installation by making sure that the **Veritas InfoScale 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 InfoScale Operations Manager for Windows** appears in the list of installed programs.
3. On the Windows Services panel, check whether the **Veritas InfoScale Operations Manager Messaging Service** has started.

See "Verifying the version of Management Server in the console" on page 77.

See "Installing Management Server on Windows (on premises and cloud)" on page 43.

Configuring Veritas InfoScale 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 InfoScale Operations Manager. On Windows, if you chose to launch the configuration, the Web browser is automatically launched with the URL.

For browser support, refer to the *Veritas InfoScale Operations Manager Hardware and Software Compatibility List (HSCL)* at the following URL:
https://www.veritas.com/support/en_US/doc/viom_hscl_802

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 InfoScale Operations Manager on Linux and Windows through Web browser

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 Veritas to gather data on your Veritas InfoScale 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 InfoScale 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 InfoScale Operations Manager on the configured Management Server host.

See "Installing Management Server on Linux (on premises and cloud)" on page 40.

See "Installing Management Server on Windows (on premises and cloud)" on page 43.

Implementing US Executive Order (EO) requirements

VIOM supports Event log management requirements (EL1) by US executive order.

If you want to implement the EO, you need to do the following steps manually:

1. In the `/opt/VRTSsfmcs/webgui/tomcat/conf/server.xml` file (Linux), inside `"Valve` `className="org.apache.catalina.valves.AccessLogValve"` tag, change the directory and log statement pattern as mentioned below:

   - Change the directory tag to `directory="${web.log.dir}"`
   - Change the pattern tag as follows:

     ```
     pattern="%{yyyy-MM-dd}tT%{HH:mm:ss.SSSXXX}t ${hostName}
     SourceIP=%a DestinationIP=%A "%r" %b StatusCode=%s
     ResponseTime=%F milliseconds SessionID=%S
     IncomingHeaders="%{User-Agent}i %{Content-Type}i %{Accept}i
     %{Accept-Encoding}i %{Accept-Language}i %{Accept-Charset}i"
     OutgoingHeaders="%{Content-Type}o %{Content-Length}o
     %{Server}o""
     ```

   - Add maxDays tag as follows:

     ```
     maxDays="30"
     ```

Note: For Windows the file path is `C:\Program Files\Veritas\VRTSsfmcs\webgui\tomcat\conf\server.xml`

2. Restart **Web server**.

   After you restart the Web server, you can see the new logs inside the `/var/opt/VRTSsfmcs/logs directory`.

Configuring Veritas InfoScale Operations Manager Management Server and Agents in FIPS mode on Linux

The Federal Information Processing Standards (FIPS) 140-2 standard (commonly referred as FIPS mode) specifies the security requirements for cryptographic modules. The U.S. federal government has set an encryption standard for its non-military agencies, contractors, and service providers who work with the U.S. government must also follow FIPS. Hence, it is mandatory to configure and enable the FIPS 140-2 standard.

You can configure and enable FIPS mode for Veritas InfoScale Operations Manager Management Server and Agents. By default, FIPS-compliant mode is turned off when the Veritas InfoScale Operations Manager Management Server platform is installed. However, you can turn on FIPS mode for one or more nodes in your deployment. Configuration of Veritas InfoScale Operations Manager to run in FIPS mode includes the following sequence of process:

- Enabling the FIPS mode on Veritas InfoScale Operations Manager Management Server (installed on Linux)
- Enabling the FIPS mode on the third-party components that are used in Veritas InfoScale Operations Manager (Tomcat, Java)
- Enabling the FIPS mode on Veritas InfoScale Operations Manager Agents (Linux, Solaris, and AIX)

Prerequisites to configure Veritas InfoScale Operations Manager in FIPS mode

- FIPS mode can be enabled only with a fresh installation of Veritas InfoScale Operations Manager Server on a Linux system. Configuration of an existing Veritas InfoScale Operations Manager to run in FIPS mode is not supported in this release.

- FIPS mode can be enabled only on Agents running on Linux, Solaris, or AIX. In this release, agents that are running on other operating systems cannot be configured in FIPS mode.
- To verify if OpenSSL is installed, run the /usr/bin/openssl version command.

To enable FIPS mode on fresh installation of Veritas InfoScale Operations Manager Management Server on Linux

1. Perform a fresh installation of Veritas InfoScale Operations Manager Management Server on Linux.
2. Open the `VRTSatlocal.conf` configuration file that is located at `/opt/VRTSsfmcs/sec/bin/`.
3. Under the Security\Authentication\Client section, enable the FIPS mode as follows:

   ```
   [Security\Authentication\Client] "FipsMode"=dword:00000001
   "ConnectTimeout"=dword:00000014
   ```

4. Open a browser and configure Veritas InfoScale Operations Manager Management Server.
5. Once the Veritas InfoScale Operations Manager Management Server configuration is successful, you may open the `VRTSatlocal.conf` configuration file that is located at `/var/opt/VRTSsfmcs/sec/root/.VRTSat/profile/` and verify if the “FipsMode"=dword:00000001 is set.

To enable FIPS mode on Tomcat and Java components used in Veritas InfoScale Operations Manager

1. Create a trusted Java KeyStore (JKS) for the Tomcat web server with imported certificates provided by a trusted Certificate Authority. For more information, see https://www.veritas.com/support/en_US/article.100026835
2. Back up the following files:
   - `/opt/VRTSsfmcs/webgui/jre/conf/security/java.security`
   - `/opt/VRTSsfmcs/webgui/tomcat/conf/server.xml`
3. Copy and overwrite the following files as follows:
   - `cp /opt/VRTSsfmcs/webgui/jre/conf/security/java.security.fips /opt/VRTSsfmcs/webgui/jre/conf/security/java.security`
   - `cp/opt/VRTSsfmcs/webgui/tomcat/conf/server.xml.fips /opt/VRTSsfmcs/webgui/tomcat/conf/server.xml`
   - `cp /opt/VRTSsfmcs/webgui/tomcat/bin/setenv.sh.fips /opt/VRTSsfmcs/webgui/tomcat/bin/setenv.sh`

4. Edit the server.xml that is located at `/opt/VRTSsfmcs/webgui/tomcat/conf/` and add the CMS hostname (FQDN) in the Connector tag and Connector > SSLHostConfig tag respectively as follows:
   - `defaultSSLHostConfigName="<FQDN>"`
   - `hostName="<FQDN>"`
5. Convert the Java KeyStore (JKS) to the BC FIPS Keystore (BCFKS) format using the following command:

```
/opt/VRTSsfmcs/webgui/jre/bin/keytool -importkeystore -srckeystore
.keystore -srcstoretype pkcs12 -deststoretype BCFKS -destkeystore
.keystore -srcstorepass changeit -deststorepass changeit
-providerclass
com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider
-J--module-path=/opt/VRTSsfmcs/webgui/jre/lib/ccj-3.0.1.jar
-J--add-modules=ccj
-J--add-exports=java.base/sun.security.provider=ccj
-J--add-exports=java.base/sun.security.internal.spec=ccj
```

Note: To verify the conversion of JKS to BCFKS use the following command:

```
/opt/VRTSsfmcs/webgui/jre/bin/keytool -list -keystore
/opt/VRTSsfmcs/webgui/tomcat/cert/.keystore -storepass changeit
-storetype BCFKS -providername CCJ -providerpath
"/opt/VRTSsfmcs/webgui/jre/lib/ext/ccj-3.0.1.jar" -providerclass
com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider
```

6. Restart VIOM web server using the following command:`/opt/VRTSsfmcs/bin/vomsc --restart web`

To enable FIPS mode on Veritas InfoScale Operations Manager Agents running on Linux, Solaris, AIX

1. Open Veritas InfoScale Operations Manager Management Server in a browser.
2. Add Linux, Solaris, or AIX Agents having Veritas InfoScale Operations Manager version 8.0, 8.0.2 to Veritas InfoScale Operations Manager Management Server.

The FIPS mode can be enabled only on Agents running on Linux, Solaris, or AIX having Veritas InfoScale Operations Manager version 8.0 and 8.0.2

Note: In this release, agents that are running on other operating systems cannot be configured in FIPS mode.

Configuring Service groups using CLI script

Veritas InfoScale Operations Manager (VIOM), supports CLI script to create SFM_SStore and SFM_Services groups before configure CMS HA on Linux platform.

Follow the procedure to configure Service groups (SFM_SStore and SFM_Services) using CLI script for CMS HA.

To create SFM_SStore and SFM_Services

1. Install InfoScale 8.0.2 on cluster nodes (Primary and Secondary).
2. Plumb VIP on primary node to configure.

   For example: `ifconfig ens192:1 xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx up`
3. Configure VIOM CMS on primary node using VHN and VIP.

   Note: Install VIOM binary and do not configure VIOM CMS on secondary node.
4. Add secondary node (as a Agent) to the configured CMS.
5. Create diskgroup using shared luns on primary node.

   For example: `# vxdg init testdg (disk_name)`
6. Create volume on created diskgroup.

   For example: `# vxassist -g testdg make testvol 10G`
7. Create VxFS filesystem on created volume.

   For example: `# mkfs -t vxfs /dev/vx/rdsk/testdg/testvol`
8. Create empty directory to mount VxFS file system on created volume.

   For example: `# mkdir /testvol`
9. Mount VxFS file system on created volume.

   For example: `# mount -t vxfs /dev/vx/dsk/testdg/testvol /testvol`

   After mounted file system, please note down device path, it will require to provide the inputs while creating service group. For example: `# df -h /dev/vx/dsk/testdg/testvol`
10. Unplumb VIP on primary node.

    For example: `# ifconfig ens192:1 down`
11. Deport Diskgroup.

    For example: `# vxdg deport testdg`

12 Run the script.

For example: `# [root@example1 /]# /opt/VRTSsfmcs/config/vcs/createha.pl`

```
The following script will create the prerequisite VCS resources
to configure VIOM in a High Availability configuration:

Please ensure that you have addressed the following items
prior to running the script:

1.  The virtual IP to be chosen must be within the same IP subnet,
    and should not be plumbed.
    The VIP Will be brought online using the SFM_Services_IP resource
2.  A VxVM disk group and volume for the VIOM data must have already
    been created, with a VxFS filesystem written to that volume
3.  The filesystem should be unmounted, and the disk group
    should be deported prior to running the script
    as VCS will import it with cluster reservations.
4.  The VIOM virtual IP and virtual hostname should be added
    as a new entry to /etc/hosts on each of the cluster nodes.

VIP :xxx.xxx.xxx.xxx
NetMask :xxx.xxx.xxx.xxx
Nic :ens192
DiskGroup :testdg
MountPoint :/testvol
BlockDevice :/dev/vx/dsk/testdg/testvol
VCS WARNING V-16-1-10364 Cluster already writable.
VCS NOTICE V-16-1-10136 Group added; populating SystemList and
setting the Parallel attribute recommended before adding resources
/opt/VRTSvcs/bin/hagrp -modify SFM_SStore SystemList
example1 0 example2 1
VCS NOTICE V-16-1-10242 Resource added. Enabled attribute
must be set before agent monitors
VCS NOTICE V-16-1-10136 Group added; populating SystemList
and setting the Parallel attribute recommended before adding resources
VCS NOTICE V-16-1-10242 Resource added. Enabled attribute
must be set before agent monitors
VCS NOTICE V-16-1-10242 Resource added. Enabled attribute
must be set before agent monitors
VCS NOTICE V-16-1-10242 Resource added. Enabled attribute
```

```
must be set before agent monitors
[root@example1 /]#
```

13 Verify the created SFM_SStore and SFM_Services service groups.

```
# hagrp -state
 [root@example1 /]# hagrp -state
 #Group       Attribute            System      Value
 SFM_SStore   State                example1 |ONLINE|
 SFM_SStore   State                example2 |OFFLINE|
 SFM_Services State                example1 |ONLINE|
 SFM_Services State                example2 |OFFLINE|
 cvm          State                example1 |ONLINE|
 cvm          State                example2 |ONLINE|
[root@example1.com /]#
```

Configuring Veritas InfoScale Operations Manager Management Server on Linux using CLI

You can configure Veritas InfoScale Operations Manager CMS using CLI on Linux.

To configure Veritas InfoScale Operations Manager CMS using CLI

1 Install Veritas InfoScale Operations Manager CMS on the Linux host. After installation, from the command prompt, run the following command to start the configuration:

See "About installing Management Server" on page 39.

2 `# /opt/VRTSsfmh/bin/perl /opt/VRTSsfmcs/bin/cli_cms_config.pl`

3 By default, the **Hostname**, **IP address**, and the **Database** location for the CMS is displayed. You can either accept the default values or enter the values manually.

4 Enter (**Y**) to start the configuration using the default values.

After successful configuration, the Veritas InfoScale Operations Manager CMS URL is displayed.

5 Copy and paste the URL in the browser and sign in to the Veritas InfoScale Operations Manager CMS GUI.

Note: If you enter (N), CLI quits the configuration and displays two options. Choose any one of the options that you want to do.

Importing third-party certificates for xprtld

Veritas InfoScale Operations Manager (VIOM)lets you import third-party certificates for the xprtld service on Management Servers that run on Linux. It also lets you import third-party certificates for the agents on AIX, Linux, and Solaris, provided that the agent version is 7.3.1 or later. VIOM supports the use of a third-party certificate without a passphrase for xprtld that runs on port 5634. However, it only supports 2048-bit certificates.

To generate a third-party certificate for xprtld

1. Use the `openssl` command as follows to generate a private key and a certificate signing request (CSR):

   ```
   openssl req -newkey rsa:2048 -nodes -keyout
   sfmAgentPrivateKeyFileName -out sfmAgentCSRFileName
   ```

   For example:

   ```
   openssl req -newkey rsa:2048 -nodes -keyout sfm_agent.private.key
   -out sfm_agent.csr
   ```

2. The `openssl` command prompts you to provide some information that is to be added to the CSR. Specify the exact values that are provided in the following example:

   ```
   Country Name (2 letter code) [XX]: .
   State or Province Name (full name) []: .
   Locality Name (eg, city) [Default City]: .
   Organization Name (eg, company) [Default Company Ltd]: vx
   Organizational Unit Name (eg, section) []: sfm_domain@nameOfCMS
   Common Name (eg, your name or your server's hostname) []: sfm_agent
   Email Address []:
   ```

   Note: The *nameOfCMS* value should match exactly with the value of the `cs_config_name` attribute that is present in the `/etc/default/sfm_resolv.conf` file on the Central Management Server (CMS).

   Specify the exact values that are provided in the following example for this additional information that is also to be sent with the CSR:

   ```
   A challenge password []: .
    An optional company name []:
   ```

3. Send the CSR file—for example, `sfm_agent.csr`–to your certificate signing authority and ask them to provide the corresponding certificate. The certificate should be provided in the `pem` format, along with the intermediate CA certificate and the root CA certificate, and it should support SSL clients. Veritas recommends that you assign a validity of 10 years to the certificate, or the maximum duration possible.

4. Optionally, run the following command to verify the purpose of the certificate, including the support for SSL clients:

   ```
   openssl x509 -purpose -noout -in sfmAgentCertFileName
   ```

   For example:

   ```
   openssl x509 -purpose -noout -in sfm_agent.cert.pem

   Certificate purposes:

   SSL client : Yes SSL client CA :No

   SSL server : Yes SSL server CA :No

   Netscape SSL server : Yes Netscape SSL server CA : No
   ```

5. Ensure that you have the following files ready before you import the certification on a Management Server:

File	Sample file name
Private key file for `sfm_agent`	`sfm_agent.private.key`
Certificate file for `sfm_agent`	`sfm_agent.cert.pem`
Certificate file for intermediate CA	`intermediate.cert.pem`
Certificate file for root CA	`ca.cert.pem`

To import a third-party certificate on a Management Server and on the agents

1. Copy all the files that are mentioned in the last step of the previous procedure on the Management Server at the appropriate location, for example: `/viom/certs/`.

2. Run the following command to import the certificates:

   ```
   /opt/VRTSsfmh/bin/perl
   /opt/VRTSsfmh/util/import_sfm_agent_certificate.pl
   --import_sfm_agent_cert
   --sfm_agent_certificate=/viom/certs/sfmAgentCertificateFileName
   --sfm_agent_privatekey=/viom/certs/sfmAgentPrivateKeyFileName
   ```

```
--subCA_certificate=/viom/certs/intermediateCertificateFileName
--rootCA_certificate=/viom/certs/caCertificateFileName
```

For example:

```
/opt/VRTSsfmh/bin/perl
/opt/VRTSsfmh/util/import_sfm_agent_certificate.pl
--import_sfm_agent_cert
--sfm_agent_certificate=/viom/certs/sfm_agent.cert.pem
--sfm_agent_privatekey=/viom/certs/sfm_agent.private.key
--subCA_certificate=/viom/certs/intermediate.cert.pem
--rootCA_certificate=/viom/certs/ca.cert.pem
```

The certificates are imported on the agents automatically.

3. Follow the instructions and provide the appropriate input at the prompts that the command displays.

   You may encounter certain situations that you can address as follows:

   - The certificate import process restarts all the VIOM services on the Management Server and the xprtld service on all the managed hosts. After the certificate is successfully imported, if a managed host does not yet use the new certificate, check whether that host is registered on multiple Management Servers. If so, unconfigure the managed host from the Management Servers other than the one on which this new certificate was installed, and then restart the xprtld service on the host.
   - The certificate cannot be imported on the managed hosts that are on VIOM 7.3 or an earlier version. Upgrade such hosts to VIOM 8.0 or a later supported version (refer to the Veritas InfoScale Operations Manager Hardware and Software Compatibility Lists document), and then run the command to import the certificate again.
   - The certificate cannot be imported on managed hosts that are unreachable from the Management Server. After the import process is complete, address the connectivity issue for the managed hosts that were unreachable. Then, add the managed hosts to the Management Server again; the new certificate gets automatically installed on the managed hosts.

About installing managed host

You must install the `VRTSsfmh` package on a host so you can manage it using Veritas InfoScale Operations Manager Management Server. By default, a compatible version of `VRTSsfmh` package is packaged with Storage Foundation High Availability 7.3, 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 InfoScale 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 InfoScale Operations Manager Management Server User Guide*.

See "Adding the managed hosts to Management Server using an agent configuration" on page 147.

See "Adding the managed hosts to Management Server using an agentless configuration" on page 151.

See "Adding managed hosts to Management Server using the Auto Configure (gendeploy.pl) script" on page 157.

See "Operating system requirements" on page 23.

See "About cloning virtual machines" on page 58.

See "About migrating virtual machines" on page 58.

Installing managed host on UNIX/Linux

You can install Veritas InfoScale Operations Manager managed host 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 InfoScale Operations Manager managed host on a UNIX/Linux host

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

   See "Operating system requirements" on page 23.

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

   See "Downloading managed host files" on page 17.

3. Open an operating system console.

4. On the host where you plan to install managed host, log on as root.

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

On AIX 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_8.0.2.0_AIX.bff VRTSsfmh
```

- For Linux, enter the following:

```
rpm -ivh VRTSsfmh_8.0.2.0_Linux.rpm
```

- For Solaris 11 on SPARC, enter the following:

```
pkg install --accept -g
VRTSsfmh_8.0.2.0_SunOS_arch_sparc_osr_5.11.p5p VRTSsfmh
```

- For Solaris 11 on x86, enter the following:

```
pkg install --accept -g
VRTSsfmh_8.0.2.0_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 59.

See "About installing managed host" on page 54.

Installing managed host on Windows

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

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

To install Veritas InfoScale Operations Manager managed host on a Windows host

1 Log on to the target host as a user with administrator privileges.

2 Make sure that the value for environment variable PATHEXT on the target host includes the extensions .exe, .bat, and .vbs.

3 Make sure that the host where you plan to install managed host meets or exceeds system and operating system requirements.

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

   See "Downloading managed host files" on page 17.

5 From the directory to which you unzipped the installation files bundle, do the following:

   - On a 64-bit host, run `VRTSsfmh_8.0.2.0_Windows_arch_x64.msi`

6 On the welcome screen of the Installation Wizard, click **Next**.

7 On the **Ready to Install the Program** screen, click **Install** to start the installation.

8 Click **Finish** to exit the Installation Wizard.

9 Verify that the managed host program is installed and the required services have started.

   See "Verifying managed host installation on Windows" on page 59.

See "About installing managed host" on page 54.

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 InfoScale Operations Manager managed host as a part of the Solaris JumpStart installation:

- A script which will install `VRTSsfmh` 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 147.

See "Adding the managed hosts to Management Server using an agentless configuration" on page 151.

See "Adding managed hosts to Management Server using the Auto Configure (gendeploy.pl) script" on page 157.

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 InfoScale 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 InfoScale 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 InfoScale Operations Manager database. After you reset the host id of the clone, Veritas InfoScale 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 54.

About migrating virtual machines

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

Veritas InfoScale 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 InfoScale 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 InfoScale Operations Manager Management Server.

See "About installing managed host" on page 54.

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:

    ```
    lslpp -l VRTSsfmh
    ```

  - On Linux, enter the following:

    ```
    rpm -q VRTSsfmh
    ```

  - On Solaris 11, use the following command:

    ```
    pkg info VRTSsfmh
    ```

See "Verifying the version of a managed host in the console" on page 78.

See "Installing managed host on UNIX/Linux" on page 55.

Verifying managed host installation on Windows

You can verify the managed host installation on Windows by making sure that the Veritas InfoScale Operations Manager (Host Component) program is installed, and the required services have started.

To verify the managed host installation on Windows

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

See "Verifying the version of a managed host in the console" on page 78.

See "Installing managed host on Windows" on page 56.

About upgrading Management Server

You can upgrade your Veritas InfoScale Operations Manager Management Server installation to 8.0.2 only from version 8.0 or later. To upgrade, you have to download and install the required packages. You can upgrade Management Server on Linux and Windows hosts.

Note: To upgrade to Veritas InfoScale Operations Manager 8.0.2 from versions before 7.4.2, you first need to upgrade to Veritas InfoScale Operations Manager version 8.0 then, you can upgrade to version 8.0.2.

From version 7.0 onwards, Veritas InfoScale Operations Manager supports 2048-bit certificates for communication between Management Server and the managed hosts. In case of an upgrade to Veritas InfoScale Operations Manager 7.0 or later, you need to migrate the Management server domain to 2048-bit certificates after you upgrade your Management Server.

Prerequisites for upgrading your Veritas InfoScale Operations Manager management server from 7.3.1 to 7.4

1. To upgrade from 7.3.1 HF2 (onwards) to 7.4 download the fix from SORT:

   https://sort.veritas.com/patch/finder

2. Apply the fix on the Veritas InfoScale Operations Manager management server:

   - For Linux run the following command:

     ```
     /opt/VRTSsfmcs/pgsql/bin/psql -p 5636 -d SFMdb3
     habdbsync -f <Upgrade_from_7.3.1_to_7.4.sql file path>
     ```

   - For windows run the following command:

```
C:\Program Files\Veritas\VRTSsfmcs\pgsql\bin\psql -p 5636 -d
SFMdb3 habdbsync -f <Upgrade_from_7.3.1_to_7.4.sql file path>
```

See "Migrating the managed hosts to 2048-bit certificate" on page 65.

See "Downloading Veritas InfoScale Operations Manager 8.0.2" on page 16.

See "Upgrading Management Server on Linux" on page 61.

See "Upgrading Management Server on Windows" on page 63.

See "Backing up Veritas InfoScale Operations Manager data on Linux before upgrading to version 8.0.2" on page 69.

See "Backing up Veritas InfoScale Operations Manager data on Windows before upgrading to version 8.0.2" on page 72.

Upgrading Management Server on Linux

First you need to upgrade your existing VIOM Management Server to version 8.0 then, you can upgrade VIOM Management Server on a Linux host to Veritas InfoScale Operations Manager 8.0.2 using.

`Veritas_InfoScale_Operations_Manager_MS_8.0.2_Linux_Full.bin` file.

When you run the `.bin` file, the installer first attempts to upgrade the Veritas InfoScale 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 InfoScale Operations Manager is restored.

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

See "Backing up Veritas InfoScale Operations Manager data on Linux before upgrading to version 8.0.2" on page 69.

Note: If the existing Management server has its database at a non-default location, the installer gives read and execute permission to other users for the non-default location as a part of the upgrade process.

To upgrade Management Server to Veritas InfoScale Operations Manager 8.0.2 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 23.

   See "System resource requirements" on page 25.

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

3. Download and unzip the installation file.

   See "Downloading Veritas InfoScale Operations Manager 8.0.2" on page 16.

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

5. At the command prompt, run one of the following commands:

   - For Management Server along with the add-ons-

     `./Veritas_InfoScale_Operations_Manager_MS_8.0.2_Linux_Full.bin`

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

   - For Management Server along with the add-ons-

     `chmod +x`

     `Veritas_InfoScale_Operations_Manager_MS_8.0.2_Linux_Full.bin`

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

7. In response to the message that confirms if you want to upgrade to Veritas InfoScale Operations Manager 8.0.2, type **y**.

8. 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% of *DB size*) + 150 MB

   where *DB size* is the size of your database. The size of the database is actually the size of the `/var/opt/VRTSsfmcs/db/` database directory.

9. The upgrade is complete when you see message similar to the following:

   `Veritas InfoScale Operations Manager upgrade is complete.`

10 To verify the upgrade, run the following command:

```
rpm -q VRTSsfmcs
```

Verify that the version for the `VRTSsfmcs` package is displayed as 8.0.2.

See "Verifying Management Server installation on Linux" on page 42.

11 After a successful upgrade to Veritas InfoScale Operations Manager 8.0.2, 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.

12 To check whether the Veritas InfoScale Operations Manager services are running, run the following command:

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

See "About upgrading Management Server" on page 60.

Upgrading Management Server on Windows

You can upgrade an existing Management Server on a Windows host to Veritas InfoScale Operations Manager 8.0.2 using the `Veritas_InfoScale_Operations_Manager_MS_8.0.2_Win_Full.exe` file. When you run the `.exe` file, the installer first attempts to upgrade the Veritas InfoScale 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 InfoScale Operations Manager is restored.

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

See "Backing up Veritas InfoScale Operations Manager data on Windows before upgrading to version 8.0.2" on page 72.

To upgrade Management Server to Veritas InfoScale Operations Manager 8.0.2 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 23.

See "System resource requirements" on page 25.

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 InfoScale Operations Manager 8.0.2" on page 16.

4 Turn off the Windows firewall, or, open ports 5634 and 14161 for TCP/IP communication.

5 Ensure that there is no restart pending from Windows Update. If there is, restart the host before launching the installer.

6 To launch the installer, run the following file:

- For Management Server along with the add-ons-
  `Veritas_InfoScale_Operations_Manager_MS_8.0.2_Win_Full.exe`

7 In the message window that confirms if you wish to upgrade to Veritas InfoScale Operations Manager 8.0.2, click **Yes** to continue with the upgrade.

8 In the **Veritas InfoScale Operations Manager 8.0.2 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% of *DB size*) + 350 MB

where, *DB size* is the size of your database. The size of the database is actually the size of the `C:\ProgramData\Symantec\VRTSsfmcs\db` database directory.

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

Completed the Veritas InfoScale Operations Manager 8.0.2 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 8.0.2, select the **Veritas InfoScale 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 77.

15 After a successful upgrade to Veritas InfoScale Operations Manager 8.0.2, 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 InfoScale Operations Manager Messaging Service** and **Veritas InfoScale Operations Manager Database Service** are running.

See "About upgrading Management Server" on page 60.

See "Upgrading managed host on Windows using the installer package" on page 76.

Migrating the managed hosts to 2048-bit certificate

You need to run the `at_migration.pl` Perl script on Management Server to migrate the Management Server domain (all the managed hosts reporting to Management Server) to 2048-bit certificate.

In case any managed host is not reporting to Management Server or any managed host fails to migrate when the script is run, you need to manually migrate that particular host by running the script on the host.

Note: All those managed hosts that fail to migrate after running the script, may not be able to communicate with Management server unless they are manually migrated to 2048-bit certificates.

To migrate the managed hosts to 2048-bit certificate

1 On your Management Server, run the `at_migration.pl` Perl script.

- On Linux Management Server:

```
/opt/VRTSsfmh/util/at_migration.pl --migrate
```

- On Windows Management Server:

```
C:\Program Files\Veritas\VRTSsfmh\bin\perl.exe
 "C:\Program Files\Veritas\VRTSsfmh\util\at_migration.pl"
  --migrate
```

2 The script displays the following information:

- Number of managed hosts that have host package version 7.0 or later, and are reporting to Management Server.

- Number of managed hosts that are not reachable from management Server.
- Number of managed hosts that have host package version lower than 7.0.

You need to confirm if you want to continue with the migration, or you want to perform the migration only after updating the managed host packages or fixing the communication issue. Enter **n** to cancel the migration or **y** to continue with the migration process without fixing any of the above mentioned issues.

3 Once the migration of eligible managed hosts is complete, verify the list of managed hosts that are not yet migrated to 2048-bit and are still on 1024-bit certificates.

- On Linux Management Server:

```
/opt/VRTSsfmh/util/at_migration.pl --list_1024_hosts
```

- On Windows Management Server:

```
C:\Program Files\Veritas\VRTSsfmh\bin\perl.exe
 "C:\Program Files\Veritas\VRTSsfmh\util\at_migration.pl"
  --list_1024_hosts
```

4 On the managed hosts that are still on 1024-bit, run the `at_migration.pl` script to manually migrate them to 2048-bit.

- On Linux/UNIX hosts:

```
/opt/VRTSsfmh/util/at_migration.pl --import_credentials
 --xml_filename=Path_to_xml_file
 --cs_hostname=ms_hostname
 --sfm_password=db_password
```

- On Windows hosts:

```
C:\Program Files\Veritas\VRTSsfmh\bin\perl.exe
 "C:\Program Files\Veritas\VRTSsfmh\util\at_migration.pl"
 --import_credentials
 --xml_filename=Path_to_xml_file
 --cs_hostname=ms_hostname
 --sfm_password=db_password
```

where,

- *Path_to_xml_file* is the path to the xml file that is generated when you run the `at_migration.pl` script on Management Server. Copy this file to the

managed host where you need to run the script to manually migrate the host.

- *ms_hostname* is the hostname of Management Server. In case of HA environment, it should be IP address of Management Server.
- *db_password* is the encrypted database password of Management Server. Run the following command to get this password:
  - On Linux Management Server:

    ```
    /opt/VRTSsfmh/bin/xdbadm
     -g -u habdbsync -c
     /var/opt/VRTSsfmcs/conf
    ```

  - On Windows Management Server:

    ```
    "C:\Program Files\Veritas\VRTSsfmh\bin\xdbadm.exe"
     -g -u habdbsync -c
     "c:\ProgramData\Symantec\VRTSsfmcs\conf"
    ```

Note: Migration to 2048-bit certificates is not supported on a Windows Management Server that is configured in high availability environment.

About backing up and restoring Veritas InfoScale Operations Manager data

You need to back up Veritas InfoScale 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 InfoScale Operations Manager data on Linux" on page 68.
  See "Taking regular backups of Veritas InfoScale Operations Manager data on Windows" on page 71.
- Before you upgrade Management Server to version 8.0.2
  See "Backing up Veritas InfoScale Operations Manager data on Linux before upgrading to version 8.0.2" on page 69.
  See "Backing up Veritas InfoScale Operations Manager data on Windows before upgrading to version 8.0.2" on page 72.

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

- To restore the Management Server to the last backed up state, when the Veritas InfoScale Operations Manager 8.0.2 application fails.
- To restore the Management Server for the previous version, when the Management Server upgrade to version 8.0.2 fails.

See "Restoring backed up data on Linux" on page 70.

See "Restoring backed up data on Windows" on page 72.

Points to remember when you back up or restore Veritas InfoScale 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 8.0.2 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 7.4.2, you cannot restore the backup to a version 8.0 Management Server. You can restore a version 7.4.2 backup only to a version 7.4.2 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 Veritas Technical Support.

Note: Veritas InfoScale 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 InfoScale Operations Manager processes before backing up the data.

Taking regular backups of Veritas InfoScale 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 InfoScale 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 InfoScale Operations Manager data" on page 67.

To take regular backups of Veritas InfoScale 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 70.

Backing up Veritas InfoScale Operations Manager data on Linux before upgrading to version 8.0.2

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 InfoScale Operations Manager data" on page 67.

To back up Veritas InfoScale Operations Manager data on Linux before upgrade to version 8.0.2

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 70.

See "Upgrading Management Server on Linux" on page 61.

Restoring backed up data on Linux

After you have backed up the Veritas InfoScale 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 InfoScale Operations Manager 8.0.2 failed, use the same script that you used to take the backup. For more information on restoring the data, refer to the *Veritas InfoScale 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 InfoScale Operations Manager Management Server. The Veritas InfoScale Operations Manager version should be the same as the version on the system that was used to back up the data.
- Configure Veritas InfoScale 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 InfoScale Operations Manager data" on page 67.

To restore the Veritas InfoScale 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
   ```

See "Taking regular backups of Veritas InfoScale Operations Manager data on Linux" on page 68.

See "About installing Management Server" on page 39.

Taking regular backups of Veritas InfoScale 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 InfoScale 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 InfoScale Operations Manager data" on page 67.

To take regular backups of Veritas InfoScale 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 72.

Backing up Veritas InfoScale Operations Manager data on Windows before upgrading to version 8.0.2

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 InfoScale Operations Manager data" on page 67.

To back up Veritas InfoScale Operations Manager data on Windows before upgrade to version 8.0.2

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:

   ```
   "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:

   - `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 72.

See "Upgrading Management Server on Windows" on page 63.

Restoring backed up data on Windows

After you have backed up the Veritas InfoScale 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 InfoScale Operations Manager 8.0.2 failed, use the same script that you used to take the backup. For more information on restoring the data, refer to the *Veritas InfoScale 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 InfoScale Operations Manager Management Server. The Veritas InfoScale Operations Manager version should be the same as the version on the system that was used to back up the data.
- Configure Veritas InfoScale 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 InfoScale Operations Manager data" on page 67.

To restore the Veritas InfoScale Operations Manager data on Windows

1. Run the following command to restore the data:

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

   where, *installdir* 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:

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

See "Taking regular backups of Veritas InfoScale Operations Manager data on Windows" on page 71.

See "About installing Management Server" on page 39.

About upgrading managed hosts to Veritas InfoScale Operations Manager 8.0.2

You can upgrade managed hosts in your Management Server domain to Veritas InfoScale Operations Manager 8.0.2 to make them compatible with the 8.0.2 Management Server. You can upgrade both the UNIX-based and the Windows-based managed hosts. You can upgrade to Veritas InfoScale Operations Manager 8.0.2 from Veritas InfoScale Operations Manager 7.2 managed host and later.

Note: You must upgrade Management Server to 8.0.2 before you upgrade the managed hosts in its domain to 8.0.2.

You can choose one of the following methods to upgrade a managed host to Veritas InfoScale Operations Manager 8.0.2:

- Upgrade the managed host using **Settings** > **Deployment** in the Veritas InfoScale Operations Manager console.
  See "Upgrading managed host using the console" on page 74.
  For more information on deploying packages, see the *Veritas InfoScale Operations Manager Management Server User Guide*.
- Upgrade the managed host using the console or operating system commands.
  See "Upgrading managed host using the console" on page 74.
  See "Upgrading managed host on Windows using the installer package" on page 76.
  See "Upgrading managed host on UNIX/Linux using operating system commands" on page 75.

Note: If you upgrade a managed host that has Control Host add-on installed on it to 8.0, you need to upgrade the Control Host add-on to a compatible version. For compatibility matrix of managed host version and control Host add-on, see *Veritas InfoScale Operations Manager Hardware and software Compatibility List (HSCL).*

Upgrading managed host 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 InfoScale Operations Manager console

1. In the Home page on the Management Server console, click **Settings**.
2. Select **Deployment**, and then select **Maintenance Releases**.
3. Right-click the `vom-8.0.2.0-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 234.
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 235.
6. In the **Result** panel, click **Close**.

See "Adding the managed hosts to Management Server using an agent configuration" on page 147.

See "Adding the managed hosts to Management Server using an agentless configuration" on page 151.

Upgrading managed host on UNIX/Linux using operating system commands

You can upgrade an existing managed host on UNIX to Veritas InfoScale Operations Manager 8.0.2 by upgrading the `VRTSsfmh` package on it.

To upgrade managed host to Veritas InfoScale Operations Manager 8.0.2 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 23.

   See "System resource requirements" on page 25.
2. Download the managed host installation files bundle, and unzip it.

   See "Downloading Veritas InfoScale Operations Manager 8.0.2" on page 16.

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 host, decompress the downloaded file.

   See "Downloading managed host files" on page 17.
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_8.0.2.0_AIX.bff VRTSsfmh
     ```
   - For Linux, enter the following:
     ```
     rpm -U VRTSsfmh_8.0.2.0_Linux.rpm
     ```
   - For Solaris on SPARC versions 11 or later, enter the following:
     ```
     pkg update --accept -g
     VRTSsfmh_8.0.2.0_SunOS_arch_sparc_osr_5.11.p5p package_path
     VRTSsfmh
     ```
8. To verify that the package has been upgraded and the version has changed to 8.0.2, enter one of the following at the command prompt:
   - On AIX, enter the following:
     ```
     lslpp -l 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 78.

Upgrading managed host on Windows using the installer package

You can upgrade an existing managed host on Windows to Veritas InfoScale Operations Manager 8.0.2 by upgrading the `.msi` package on it.

To upgrade managed host to Veritas InfoScale Operations Manager 8.0.2 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 InfoScale Operations Manager 8.0.2" on page 16.
3. From the directory to which you unzipped the installation files bundle, run `VRTSsfmh_8.0.2.0_Windows_arch_x64.msi`.

   See "Downloading managed host files" on page 17.
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, go to the Windows **Control Panel** and open the **Programs and Features** panel.
8. In the list of currently installed programs, verify that the version for the **Veritas InfoScale Operations Manager for Windows (Host Component)** program has changed to 8.0.2.

See "Verifying the version of a managed host in the console" on page 78.

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 43.

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 59.

See "Verifying managed host installation on Windows" on page 59.

Uninstalling Management Server on Linux

You can uninstall Veritas InfoScale 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 InfoScale 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:

   ```
   rpm -e VRTSsfmcs
   ```

4. To remove the `VRTSsfmh` package, run the following command:

   ```
   rpm -e VRTSsfmh
   ```

See "About installing Management Server" on page 39.

Uninstalling Management Server on Windows

You can uninstall Veritas InfoScale 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 InfoScale 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 InfoScale 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 InfoScale 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 InfoScale 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 Linux, enter the following:

```
rpm -e VRTSsfmh
```

- On Solaris 11, enter the following:

```
pkg uninstall VRTSsfmh
```

See "About installing managed host" on page 54.

Uninstalling managed host on Windows

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

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

To uninstall Veritas InfoScale Operations Manager managed host on Windows

1. Log on to the target host as a user with administrator privileges.
2. Go to the Windows **Control Panel**, and click **Programs and Features**.
3. From the list of installed programs, select **Veritas InfoScale Operations Manager (Host Component)**.
4. Do one of the following:
   - Select **Uninstall** at the top of the list.
   - Right click and select **Uninstall**.
5. In the dialog box, do one of the following:
   - To confirm that you want to uninstall managed host, click **Yes**.
   - To exit without uninstalling managed host, click **No**.

See "About installing managed host" on page 54.

Chapter 4

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

This chapter includes the following topics:

- Configuring the high availability feature in Veritas InfoScale Operations Manager
- Configuring CMS HA on Linux using Command Line (CLI)
- Configuring Management Server in one-to-one DR environment
- Configuring Veritas InfoScale 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 the high availability feature in Veritas InfoScale Operations Manager

You can configure the high availability (HA) feature in Veritas InfoScale Operations Manager to improve the availability of the Management Server. This configuration also improves the availability of the applications and the services that Veritas InfoScale Operations Manager provides. You can configure the HA feature on a Linux or a Windows based Management Server.

A Veritas InfoScale Operations Manager installation with HA feature typically consists of:

- Veritas InfoScale Operations Manager.
- Two nodes (Node1 and Node2) in the same data centre.
- Storage Foundation Enterprise version for cluster and storage software or Storage Foundation 8.0 or later versions.

In the event of a failure or a planned maintenance, Veritas InfoScale Operations Manager in HA can failover from Node1 to Node2, which are in the same data centre and are part of the same cluster.

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. You need to follow different set of procedures for a new and an existing Management Server:

- See "Configuring a new Veritas InfoScale Operations Manager installation in high availability environment" on page 82.
- See "Configuring an existing Veritas InfoScale Operations Manager installation in high availability environment" on page 90.

Configuring a new Veritas InfoScale Operations Manager installation in high availability environment

You can configure Veritas InfoScale 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 InfoScale Operations Manager installation in high availability environment.

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

Table 4-1 Configuring a new Veritas InfoScale 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 83.
2	Perform initial configuration of Management Server installation in high availability environment.	See "Performing initial configuration of Management Server in HA environment" on page 84.
3	Create the base service groups in VCS.	See "Creating the base service groups for HA configuration" on page 85.
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 89.

See "Configuring an existing Veritas InfoScale Operations Manager installation in high availability environment" on page 90.

See "Configuring Veritas InfoScale Operations Manager in high availability and disaster recovery environment" on page 98.

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 InfoScale Operations Manager in high availability environment. This IP is used and configured in the cluster and should not be shared with other applications.
- Storage Foundation HA 8.0, 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.
- Enough shared storage is available to hold the Veritas InfoScale Operations Manager database and shared configuration files. This storage should be used in a Storage Foundation diskgroup, with a volume and a filesystem for the data.

For more information on estimating the storage, see *Veritas InfoScale Operations Manager Installation and Configuration Guide*.

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

- Node1 and Node2 must have their clocks synchronized in Universal Time Clock (UTC/UC) format.

See "Configuring a new Veritas InfoScale Operations Manager installation in high availability environment" on page 82.

Performing initial configuration of Management Server in HA environment

Performing the initial configuration involves the following high-level steps:

- Install Management Server on both the nodes (Node1 and Node2).
- configure Management Server only on Node1.
- Add Node2 as a managed host to the Management server that is configured on Node1.

For information on installing and configuring Management Server, see *Veritas InfoScale Operations Manager Installation and configuration Guide.*

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 a location other than the default database location, you must make sure that it is not part of the shared storage that is used for failover. Later on during the configuration process, the database is moved to the shared storage.

4 In the Analytics Setting page, select **Enable Analytics Gathering** to allow Veritas to gather data on your Veritas InfoScale 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 InfoScale 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 InfoScale Operations Manager installation in high availability environment" on page 82.

See "Configuring an existing Veritas InfoScale Operations Manager installation in high availability environment" on page 90.

See "Configuring Management Server in one-to-one DR environment" on page 93.

See "Configuring Veritas InfoScale Operations Manager in high availability and disaster recovery environment" on page 98.

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 the 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

Table 4-2 *(continued)*

Service group	Resource
SFM_Services	■ SFM_Services_IP ■ SFM_Services_NIC ■ SFM_Services_Mount

Note: 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	■ **Device**: Name of the NIC where virtual IP is plumbed.

Resource name	Resource type	Attributes
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.
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, `/dev/vx/dsk/`*`disk group`*`/`*`volume name`*. ■ **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 InfoScale Operations Manager installation in high availability environment" on page 82.

See "Configuring an existing Veritas InfoScale Operations Manager installation in high availability environment" on page 90.

Creating the base service groups for CFS HA configuration

For Cluster File System (CFS) HA configuration, you need to create some base service groups and resources and add some dependencies between the resources.

Note: In CFS HA mode, VIOM does not support disaster recovery (DR).

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.

Create the following service groups with their respective resources:

Table 4-3

Service group	Resource
SFM_SStore Create in parallel mode	▪ SFM_SStore_DG ▪ SFM_Services_Mount
SFM_Services Create in failover mode	▪ SFM_Services_IP ▪ SFM_Services_NIC

Refer to the following table for the resources that you can create:

Resource name	Resource type	Attributes
SFM_SStore_DG	Diskgroup	▪ **Diskgroup**: Disk group that is specified for the failover.
SFM_Services_IP	IP	▪ **Address**: 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. ■ **BlockDevice**: Complete path of the storage device that is specified for failover. `Example: /dev/vx/dsk/disk group/`*`volume_name`* ■ **FSType**: Type of the file system (VxFS). ■ **FsckOpt**: File check option (fsckpt = -n or -y).

Type of the SFM_SStore_DG is CVMVolDg and SFM_Services_Mount is CFSMount.

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	Firm

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

For **SFM_SStore** service group, link the **SFM_Services_Mount** resource as parent and **SFM_SStore_DG** as child resource.

See "Creating the base service groups for HA configuration" on page 85.

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 InfoScale 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 InfoScale Operations Manager HA configuration and do one of the following:

   - Click the link that is displayed on the panel to log on to Veritas InfoScale Operations Manager that is configured in high availability environment.
   - Click **Quit** to quit the configuration dialog.

See "Configuring a new Veritas InfoScale Operations Manager installation in high availability environment" on page 82.

See "Configuring an existing Veritas InfoScale Operations Manager installation in high availability environment" on page 90.

Configuring an existing Veritas InfoScale Operations Manager installation in high availability environment

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

Configuring an existing Veritas InfoScale 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 initially configuring the Management Server, follow the process of configuring a new Veritas InfoScale Operations Manager installation in high availability environment, see Configuring a new Veritas InfoScale 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, a new hostname and IP would be required for HA configuration. see Table 4-4

Table 4-4 Configuring an existing Veritas InfoScale 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 91.
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" on page 92.
Step 3	Create the base service groups in VCS to ensure failover.	See "Creating the base service groups for HA configuration" on page 85.
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 89.

See "Configuring a new Veritas InfoScale Operations Manager installation in high availability environment" on page 82.

See "Configuring Management Server in one-to-one DR environment" on page 93.

See "Configuring Veritas InfoScale Operations Manager in high availability and disaster recovery environment" on page 98.

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 8.0 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 InfoScale 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 InfoScale Operations Manager installation in high availability environment" on page 90.

Modifying the default IP address and host name of the existing Management Server

If you have not used a virtual host name and IP during the configuration of the Management Server, you need to change the default IP address and host name to a new IP address and a new host name. Based on the operating system of your 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 gets released in this case and can be used as a virtual IP and virtual host name for configuring the Management Server in HA environment.

See "Configuring an existing Veritas InfoScale Operations Manager installation in high availability environment" on page 90.

Configuring CMS HA on Linux using Command Line (CLI)

You can configure Veritas InfoScale Operations Manager CMS high availability (HA) on Linux using CLI.

See "Prerequisites for configuring a new Management Server in high availability environment" on page 83.

To configure CMS HA using CLI

1. Install Veritas InfoScale Operations Manager Management Server on the Linux host. After installation, run the following command to start the configuration:

   ```
   /opt/VRTSsfmh/bin/perl
   /opt/VRTSsfmcs/bin/cli_ha_config.pl
   ```

2. Enter (Y). CLI prepares for CMS HA configuration by stopping the database and WEBGUI and shows VCS information.
3. Again enter (Y) to start the configuration.

Note: If you enter (N) CLI quits the configuration and database and WEBGUI starts again.

Configuring Management Server in one-to-one DR environment

Following is an overview of the process of configuring Management Server in one-to-one symmetrical DR environment:

- 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 InfoScale Operations Manager database and the domain-wide information that is stored in the shared storage to the secondary node. You can use 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 InfoScale Operations Manager installation in disaster recovery environment involves the following steps:

Table 4-5 Configuring a Veritas InfoScale Operations Manager 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 94.
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 95.
3	Create the base service groups in VCS for DR configuration.	See "Creating the base service groups for DR configuration" on page 96.
4	Enable Veritas InfoScale Operations Manager DR configuration.	See "Enabling DR configuration" on page 98.

See "Configuring a new Veritas InfoScale Operations Manager installation in high availability environment" on page 82.

See "Configuring an existing Veritas InfoScale Operations Manager installation in high availability environment" on page 90.

Prerequisites for configuring a Management Server in DR environment

Before you configure Veritas InfoScale 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 InfoScale Operations Manager database in high availability environment.
- A virtual IP and a virtual host name are available for installing and using Veritas InfoScale 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.
- If you are using VVR for replication, ensure that Storage Foundation HA 8.0 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).

- If you are using VVR for replication, ensure that Global Cluster Option (GCO) is enabled in VCS in Site A and Site B. For more information on enabling GCO, see *Cluster Server Administrator's Guide*.
- If you are using VVR for replication, ensure that Volume Replicator (VVR) should be configured in Site A and Site B at VxVM level. For more information on configuring VVR, see *Volume Replicator Administrator's Guide*.
- Both the nodes on which you want to configure Veritas InfoScale 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 InfoScale 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 Management Server in one-to-one DR environment" on page 93.

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 in HA environment" on page 84.
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 Management Server in one-to-one DR environment" on page 93.

Creating the base service groups for DR configuration

You need to create the base service groups in 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 Cluster Server control. No naming convention is required for the VVR rlink resources. For more information, refer to the *Cluster Server Bundled Agents Reference Guide* and *Cluster Server Agents for Volume Replicator Configuration Guide* depending on the version of the 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 85.
  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 *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 Management Server in one-to-one DR environment" on page 93.

Enabling DR configuration

To enable Veritas InfoScale Operations Manager DR configuration

- Run the following script on Site A to configure Site B as part of the Veritas InfoScale 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 Management Server in one-to-one DR environment" on page 93.

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

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

the Veritas InfoScale Operations Manager HADR setup that is enabled with disaster recovery enhances the failover support.

You can configure Veritas InfoScale Operations Manager in high availability and disaster recovery environment in the following two ways:

- Using symmetrical nodes
- Using asymmetrical nodes

Prerequisites for configuring a Management Server in HA-DR environment

Before you configure Veritas InfoScale 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 InfoScale 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 8.0, 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. In case of HADR configuration using asymmetrical nodes, only one node is configured on the remote site (Node3).
- Global Cluster Option (GCO) is enabled in VCS in Site A and Site B. For more information on enabling GCO, see *Cluster Server Administrator's Guide*.
- Volume Replicator (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 InfoScale 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 InfoScale 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 InfoScale 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 InfoScale Operations Manager in high availability and disaster recovery environment" on page 98.

Performing initial configuration of Management Server installation in 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. In case of HADR configuration using symmetrical nodes, install Management Server on Node1 and Node2 in Site A and Node3 and Node4 in Site B. In case of HADR configuration using asymmetrical nodes, install Management server on Node1 and Node2 in Site A and Node3 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 in HA environment" on page 84.

3. In case of HADR configuration using symmetrical nodes, add Node3 and Node4 as managed hosts to the Management Server that is configured on Node1. In case of HADR configuration using asymmetrical nodes, add Node3 as managed host to the Management Server.
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 "Configuring Veritas InfoScale Operations Manager in high availability and disaster recovery environment" on page 98.

Creating the base service groups for DR configuration

You need to create the base service groups in 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 the cluster that contains Node1 and Node2 on site A:

Service group	Resource
SFM_SStore	■ SFM_SStore_DG ■ SFM_SStore_IP ■ SFM_SStore_NIC ■ 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 above. Failure to do so may result in configuration failure.

It is recommended to set up the VVR rlinks under Cluster Server control. No naming convention is required for the VVR rlink resources. For more information, refer to the *Cluster Server Bundled Agents Reference Guide* and *Cluster Server Agents for Veritas Volume Replicator Configuration Guide* depending on the version of the 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.
SFM_SStore_IP	IP	**Address**: Virtual IP address, which you have configured as a Replication IP. **Device**: Name of the NIC where virtual IP is plumbed. **NetMask**: Subnet mask that is associated with the virtual IP address.
SFM_SStore_NIC	NIC	**Device**: Name of the NIC where Replication virtual IP is plumbed

- For 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 85.
  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

Selection	Option
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_Services_Mount	SFM_Services_RVGPRI
SFM_Services_RVGPRI	SFM_Services_IP
SFM_SStore_RVG	SFM_SStore_DG
SFM_SStore_RVG	SFM_SStore_IP
SFM_SStore_IP	SFM_SStore_NIC

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. In case of HADR configuration using asymmetrical nodes, the procedure needs to be repeated only for Node3 in site B.

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 Management Server in one-to-one DR environment” on page 93.

See “Configuring Veritas InfoScale Operations Manager in high availability and disaster recovery environment” on page 98.

Enabling DR configuration

To enable Veritas InfoScale Operations Manager DR configuration

- Run the following script on Node1 at Site A to configure Site B as part of the Veritas InfoScale 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_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 Site B.

In case of DR configuration using asymmetrical (one-to-two) nodes, only Node3 needs to be mentioned in Site B.

See "Configuring Veritas InfoScale Operations Manager in high availability and disaster recovery environment" on page 98.

About upgrading the high availability configurations

You can upgrade Veritas InfoScale Operations Manager 8.0 or later versions, Linux-based, or Windows-based Management Server that is configured in the high availability (HA) environment to version 8.0.2. To upgrade, you can download and use the installer for Management Server.

See "Downloading Veritas InfoScale Operations Manager 8.0.2" on page 16.

Note: You must upgrade VIOM CMS first, before upgrading InfoScale on the primary and secondary nodes. After CMS HA upgrade, ensure that you apply the latest VIOM patch on the primary and secondary CMS hosts.

After the upgrade, you can use the HA environment on the upgraded Veritas InfoScale Operations Manager 8.0.2 Management Server.

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

See "Upgrading Management Server in high availability environment" on page 105.

Upgrading Management Server in high availability environment

Before you upgrade Veritas InfoScale Operations Manager in the high availability 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 InfoScale Operations Manager in the high availability environment, which is the active node.
- Veritas recommends that you take a backup of the Management Server data.
  See "Backing up Veritas InfoScale Operations Manager data on Linux before upgrading to version 8.0.2" on page 69.
  See "Backing up Veritas InfoScale Operations Manager data on Windows before upgrading to version 8.0.2" on page 72.

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

To upgrade Management Server in high availability environment to 8.0.2

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 61.

   See "Upgrading Management Server on Windows" on page 63.

   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:

     ```
     "installdir\VRTSsfmh\bin\perl.exe"
     "installdir\VRTSsfmcs\config\vcs\sfmha" start
     ```

     where, *installdir* 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 104.

See "Upgrading Management Server in high availability and disaster recovery environment" on page 106.

About upgrading the high availability and disaster recovery configurations

You can upgrade Veritas InfoScale Operations Manager 8.0 or later versions, UNIX-based Management Server that is configured in the high availability and disaster recovery (HA-DR) environment to version 8.0.2. To upgrade, you can download and use the installer for Management Server.

See "Downloading Veritas InfoScale Operations Manager 8.0.2" on page 16.

Note: You must upgrade VIOM CMS HA-DR first, before upgrading InfoScale on the primary and secondary nodes. After CMS HA-DR upgrade, ensure that you apply the latest VIOM patch on the primary and secondary CMS hosts.

After the upgrade, you can use the HA-DR environments on the upgraded Veritas InfoScale Operations Manager 8.0.2 Management Server.

See "Upgrading Management Server in high availability and disaster recovery environment" on page 106.

Upgrading Management Server in high availability and disaster recovery environment

Before you upgrade Veritas InfoScale 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 InfoScale 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 8.0.2

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 61.

   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_XprtId service groups are online on the active node.

See "About upgrading the high availability and disaster recovery configurations" on page 106.

See "Upgrading Management Server in high availability environment" on page 105.

Removing the high availability configuration

You can not remove the high availability configuration from a Veritas InfoScale Operations Manager Linux-based Management Server.

Note: In Veritas InfoScale Operations Manager 8.0.2, you cannot remove the Veritas InfoScale 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 a high availability environment	My_virtual-host_1

Chapter 5

Installing and uninstalling Veritas InfoScale Operations Manager add-ons

This chapter includes the following topics:

- About deploying Veritas InfoScale Operations Manager add-ons
- Downloading a Veritas InfoScale Operations Manager add-on
- Uploading a Veritas InfoScale Operations Manager add-on to the repository
- Installing a Veritas InfoScale Operations Manager add-on
- Uninstalling a Veritas InfoScale Operations Manager add-on
- Removing a Veritas InfoScale Operations Manager add-on from the repository
- Canceling deployment request for a Veritas InfoScale Operations Manager add-on
- Installing a Veritas InfoScale Operations Manager add-on on a specific managed host
- Uninstalling a Veritas InfoScale Operations Manager add-on from a specific managed host
- Enabling a Veritas InfoScale Operations Manager add-on on a specific managed host

- Disabling a Veritas InfoScale Operations Manager add-on from a specific managed host
- Refreshing the repository
- Restarting the web server

About deploying Veritas InfoScale Operations Manager add-ons

Veritas InfoScale 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 InfoScale 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 Veritas Services and 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 InfoScale Operations Manager add-ons and their supported versions, refer to the *Veritas InfoScale 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 InfoScale Operations Manager Management Server 8.0.2 from a previous version of Veritas InfoScale Operations Manager, you may need to upgrade the add-ons. The previous version of the add-on may not be supported with Veritas InfoScale Operations Manager 8.0.2.

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 maintenance release packages and patches" on page 231.

See "Downloading a Veritas InfoScale Operations Manager add-on" on page 110.

See "Uploading a Veritas InfoScale Operations Manager add-on to the repository" on page 111.

See "Downloading Management Server files" on page 17.

Downloading a Veritas InfoScale Operations Manager add-on

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

- Download individual Veritas InfoScale Operations Manager add-ons using the Management Server console.
- Download the zip file which contains all the Veritas InfoScale Operations Manager add-ons from Download center. The zip file or compressed file for a version contains all the add-ons applicable for that particular version.

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

To download a Veritas InfoScale 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 InfoScale Operations Manager add-on to the repository" on page 111.

See "Installing a Veritas InfoScale Operations Manager add-on" on page 112.

Uploading a Veritas InfoScale Operations Manager add-on to the repository

You need to download the zip file containing the add-ons bundle 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 InfoScale 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.

4 Click **Upload** to upload the add-on to the repository.

5 Click **Close**.

See "Installing a Veritas InfoScale Operations Manager add-on" on page 112.

See "Removing a Veritas InfoScale Operations Manager add-on from the repository" on page 115.

See "About deploying Veritas InfoScale Operations Manager add-ons" on page 109.

Upload Solutions to Repository panel options

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

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

To upload 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, refer to the *Veritas InfoScale Operations Manager Add-ons User Guide*.

See "Uploading a Veritas InfoScale Operations Manager add-on to the repository" on page 111.

See "Uploading a Veritas InfoScale Operations Manager hot fix or package to the repository" on page 233.

Installing a Veritas InfoScale 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 InfoScale 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 113.
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 113.

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 122.

See "Uninstalling a Veritas InfoScale Operations Manager add-on" on page 114.

See "Removing a Veritas InfoScale Operations Manager add-on from the repository" on page 115.

See "Canceling deployment request for a Veritas InfoScale Operations Manager add-on" on page 116.

See "Viewing the details of an add-on, hot fix, package, or patch on SORT website" on page 256.

Install - Download Add-on panel options

Use this wizard panel to select the download method for downloading a Veritas InfoScale 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 InfoScale Operations Manager add-on" on page 112.

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 InfoScale 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 InfoScale 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 InfoScale Operations Manager add-on" on page 112.

Uninstalling a Veritas InfoScale Operations Manager add-on

You can uninstall a Veritas InfoScale 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 InfoScale 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 115.
6. Those add-ons which require web server restart, click **Restart Web server**.

See "Restarting the web server" on page 122.

See "Installing a Veritas InfoScale Operations Manager add-on" on page 112.

See "Removing a Veritas InfoScale Operations Manager add-on from the repository" on page 115.

Uninstall panel options

Use this wizard panel to uninstall the Veritas InfoScale 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 InfoScale Operations Manager packages and patches cannot be uninstalled.

See "Uninstalling a Veritas InfoScale Operations Manager add-on" on page 114.

Removing a Veritas InfoScale Operations Manager add-on from the repository

You can remove a Veritas InfoScale 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 InfoScale 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 116.

See "Refreshing the repository" on page 121.

See "Installing a Veritas InfoScale Operations Manager add-on" on page 112.

See "Installing a Veritas InfoScale Operations Manager hot fix, package, or patch" on page 234.

See "Uninstalling a Veritas InfoScale Operations Manager add-on" on page 114.

Remove panel options

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

See "Removing a Veritas InfoScale Operations Manager add-on from the repository" on page 115.

See "Removing a hot fix, package, or patch from the repository" on page 236.

Canceling deployment request for a Veritas InfoScale Operations Manager add-on

Using the Management Server console, you can cancel the deployment request for a Veritas InfoScale 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 InfoScale 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 117.

See "Installing a Veritas InfoScale Operations Manager add-on" on page 112.

See "Installing a Veritas InfoScale Operations Manager hot fix, package, or patch" on page 234.

See "Uninstalling a Veritas InfoScale Operations Manager add-on" on page 114.

Cancel Deployment Request panel options

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

See "Canceling deployment request for a Veritas InfoScale Operations Manager add-on" on page 116.

See "Canceling deployment request for a hot fix, package, or patch" on page 237.

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

Using the Management Server console, you can install the Veritas InfoScale Operations Manager add-on on the selected managed host. If the add-on is already installed on the selected host, then Veritas InfoScale 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 InfoScale 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 118.
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 122.

See "About deploying Veritas InfoScale Operations Manager add-ons" on page 109.

Install panel options

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

Table 5-3 lists the options for Veritas InfoScale 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.

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

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

See "Installing a Veritas InfoScale Operations Manager add-on on a specific managed host" on page 118.

See "Installing a Veritas InfoScale Operations Manager hot fix on a specific managed host" on page 238.

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

Using the Management Server console, you can uninstall the Veritas InfoScale 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 InfoScale 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 119.
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 122.

See "About deploying Veritas InfoScale Operations Manager add-ons" on page 109.

Uninstall panel options

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

Table 5-4 lists the uninstall options for Veritas InfoScale 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.
Ignore checks (if any) before installing	Select to ignore checks before installing.

See "Uninstalling a Veritas InfoScale Operations Manager add-on from a specific managed host" on page 119.

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

Using the Management Server console, you can enable a Veritas InfoScale 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 InfoScale 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 122.

See "Installing a Veritas InfoScale Operations Manager add-on on a specific managed host" on page 118.

See "Uninstalling a Veritas InfoScale Operations Manager add-on from a specific managed host" on page 119.

See "Disabling a Veritas InfoScale Operations Manager add-on from a specific managed host" on page 121.

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

Using the Management Server console, you can disable a Veritas InfoScale 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 InfoScale 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 122.

See "Installing a Veritas InfoScale Operations Manager add-on on a specific managed host" on page 118.

See "Uninstalling a Veritas InfoScale Operations Manager add-on from a specific managed host" on page 119.

See "Enabling a Veritas InfoScale Operations Manager add-on on a specific managed host" on page 120.

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 InfoScale Operations Manager add-on from the repository" on page 115.

See "About deploying Veritas InfoScale Operations Manager add-ons" on page 109.

Restarting the web server

Depending on the Veritas InfoScale 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 InfoScale Operations Manager add-on" on page 112.

Section 2

Setting up the Management Server environment

- Chapter 6. Basic Veritas InfoScale 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. Viewing information on the Management Server environment

Chapter 6

Basic Veritas InfoScale Operations Manager tasks

This chapter includes the following topics:

- About the communication between the managed hosts and Management Server
- Connecting to Veritas InfoScale 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 InfoScale 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 InfoScale Operations Manager lets administrators centrally manage diverse data center environments.

A typical Veritas InfoScale Operations Manager deployment consists of a Management Server and the managed hosts. The managed host can run on any platform that Veritas InfoScale 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 InfoScale 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 InfoScale Operations Manager Management Server" on page 125.

Connecting to Veritas InfoScale Operations Manager Management Server

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

See "Installing Management Server on Linux (on premises and cloud)" on page 40.

See "Installing Management Server on Windows (on premises and cloud)" on page 43.

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

To connect to Veritas InfoScale 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 browser support, see *Veritas InfoScale Operations Manager Hardware and Software Compatibility List (HSCL)* at the following URL:https://www.veritas.com/support/en_US/doc/viom_hscl_802

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 InfoScale Operations Manager dashboard.

See "About installing managed host" on page 54.

Stopping and starting the Web application

You can stop and restart Veritas InfoScale Operations Manager Web UI framework.

To stop and restart Veritas InfoScale 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 InfoScale 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 InfoScale Operations Manager Management Server" on page 125.

About the Management Server perspective

The Veritas InfoScale 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 InfoScale Operations Manager Management Server" on page 125.

Chapter 7

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 Agentless hosts to the Management Server using Profile
- 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 "Supported features for host discovery options" on page 132.

How Veritas InfoScale Operations Manager discovers hosts

Veritas InfoScale 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 InfoScale 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 InfoScale Operations Manager installed on them	Agent-based discovery is also used for the non-Storage Foundation hosts that have Veritas InfoScale Operations Manager installed on them.
Discovery of the non-Storage Foundation hosts using agentless discovery scripts, for the hosts that do not have Veritas InfoScale Operations Manager installed on them	Veritas InfoScale 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 InfoScale Operations Manager identifies this type of the host as an agentless host.

Note: Agentless discovery is not supported on the hosts that have Veritas Storage Foundation or Veritas InfoScale 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 InfoScale Operations Manager discovers virtualization servers and virtual machines.

Figure 7-1 Veritas InfoScale Operations Manager components and discovery (basic)

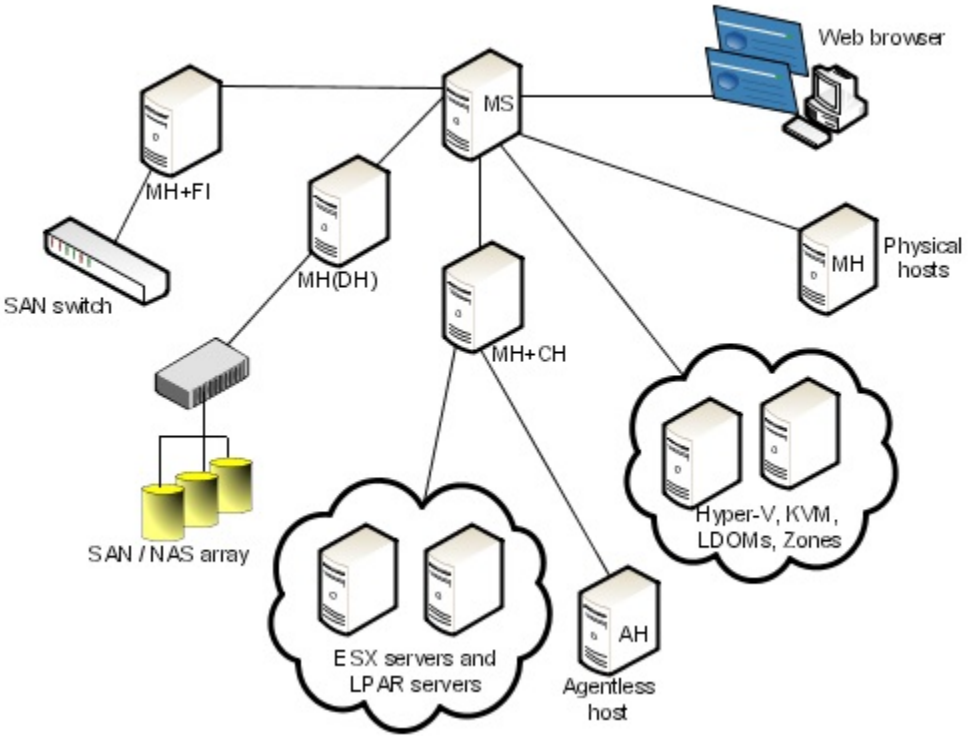
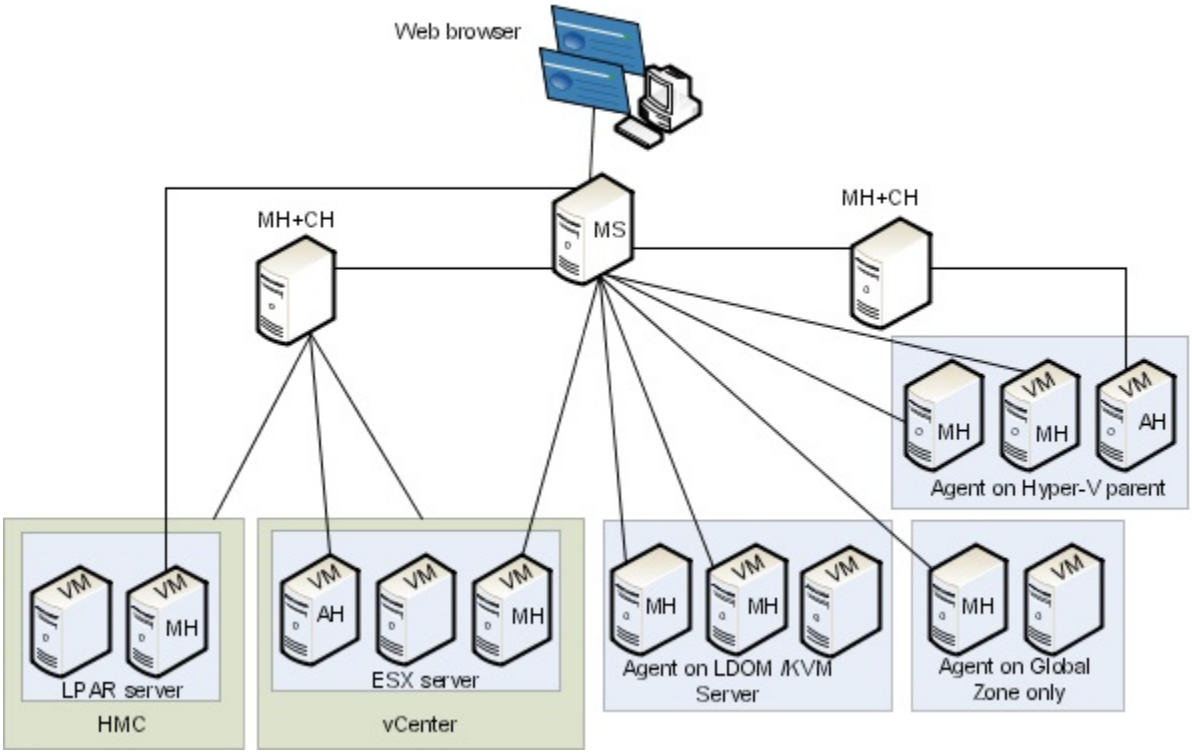


Figure 7-2 Veritas InfoScale Operations Manager components and discovery (virtualization servers and virtual machines)



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 InfoScale Operations Manager Add-ons User Guide*.

See "About Control Hosts in Veritas InfoScale Operations Manager" on page 209.

See "Requirements for discovering vCenter and ESX servers using Veritas InfoScale Operations Manager" on page 210.

See "Requirements for discovering the Solaris zones" on page 217.

See "Requirements for discovering Solaris Logical domains" on page 219.

Supported features for host discovery options

Veritas InfoScale Operations Manager provides several ways to discover hosts and their associations to storage resources and network devices.

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 InfoScale 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 InfoScale Operations Manager has the ability to discover VMware guest operating systems. The information that Veritas InfoScale 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 InfoScale Operations Manager can discover and report on with each host discovery option.

Table 7-2 compares the storage resources that Veritas InfoScale 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 iSCSCI 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 135.

See “About agentless discovery of remote hosts” on page 135.

See "How agentless discovery of a UNIX or Linux host works" on page 136.

See "How agentless discovery of a Windows host works" on page 137.

See "Prerequisites for agentless configuration" on page 136.

See "Requirements for agentless discovery of UNIX hosts" on page 138.

See "Requirements for agentless discovery of Windows hosts" on page 140.

See "Requirements for deep array discovery for agentless hosts" on page 140.

See "Commands that require the root access for agentless discovery of UNIX hosts" on page 141.

See "Using the privilege control software with agentless discovery of UNIX hosts" on page 143.

See "SSH configuration requirements for agentless discovery" on page 144.

See "About installing OpenSSH on a UNIX host" on page 146.

About agentless discovery using the Control Host

Veritas InfoScale 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.

Platform support for a host that can act as a Control Host is the same as that of Management Server.

Note: A Linux 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 agentless method.

See "About Control Hosts in Veritas InfoScale Operations Manager" on page 209.

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 InfoScale 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 136.

See "How agentless discovery of a Windows host works" on page 137.

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 InfoScale 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 135.

How agentless discovery of a UNIX or Linux host works

To perform agentless discovery of a remote UNIX or Linux host, Veritas InfoScale 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.

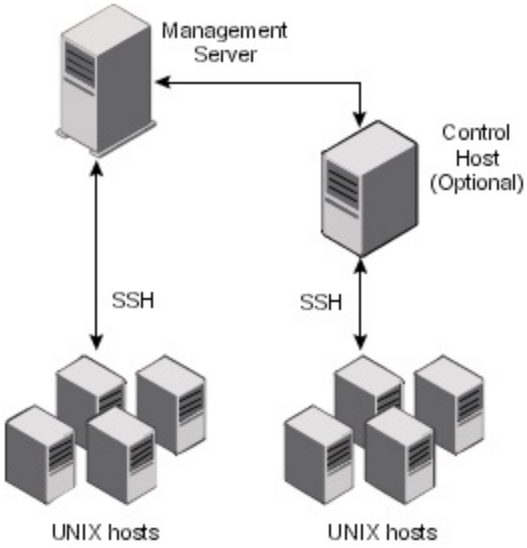
- Deletes the files from the remote host that it used for discovery.

To perform this discovery process, Veritas InfoScale 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 138.

Figure 7-3 depicts how Veritas InfoScale 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 135.

How agentless discovery of a Windows host works

To perform agentless discovery of a remote Windows host, Veritas InfoScale 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 InfoScale 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 InfoScale Operations Manager Control Host and the remote host, WMI uses port 135.

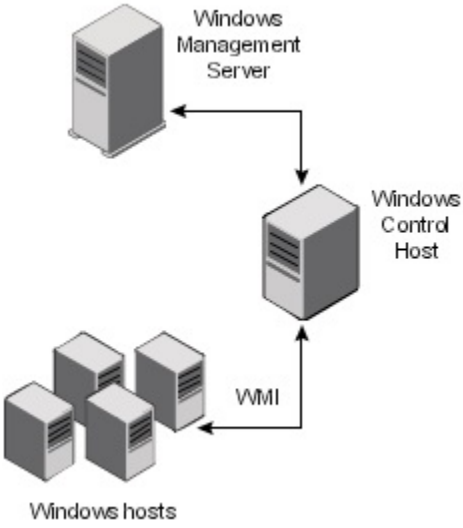
Veritas InfoScale Operations Manager uses WMI in two ways:

- 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 InfoScale Operations Manager copies the file from the host's mapped admin$ filestore, sends it to Veritas InfoScale Operations Manager Control Host, and deletes the file from the remote host.

To perform this discovery process, Veritas InfoScale Operations Manager requires a local administrator account for the remote host.

Figure 7-4 depicts how Veritas InfoScale 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 135.

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. ■ Veritas 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 141. See "Using the privilege control software with agentless discovery of UNIX hosts" on page 143.
Network access between hosts	Ensure there is network access between the host that you want to discover and Veritas InfoScale 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.
A shell on the remote host	Veritas InfoScale Operations Manager requires a shell on the remote host (sh, ksh, or bash) that accepts sh file redirection.
Secure Shell (SSH) on the remote host	To communicate between the Veritas InfoScale Operations Manager host and remote UNIX hosts, Veritas InfoScale 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 146. ■ SSH is set up properly. See "SSH configuration requirements for agentless discovery" on page 144. ■ 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 136.

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 InfoScale 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 InfoScale Operations Manager Control Host that performs discovery.
Windows Management Instrumentation (WMI)	WMI is installed as part of the Windows operating system. Ensure that the WMI service is enabled on the Veritas InfoScale 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 InfoScale 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 InfoScale 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

See "How agentless discovery of a Windows host works" on page 137.

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 agentless hosts.

See "About agentless discovery of remote hosts" on page 135.

See "Prerequisites for agentless configuration" on page 136.

Commands that require the root access for agentless discovery of UNIX hosts

Veritas InfoScale 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 InfoScale 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)

Table 7-5 Commands that require root access for agentless discovery *(continued)*

Resource	Operating system	Command	Purpose	Requirement[1]
EMC PowerPath	AIX, Linux, and Solaris	AIX: /usr/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 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
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 136.

See "Requirements for agentless discovery of UNIX hosts" on page 138.

Using the privilege control software with agentless discovery of UNIX hosts

Veritas InfoScale 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 InfoScale Operations Manager requires a root user account.

See "Commands that require the root access for agentless discovery of UNIX hosts" on page 141.

To discover that information, you can configure Veritas InfoScale 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 InfoScale 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. Veritas 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 147. See "Adding the managed hosts to Management Server using an agentless configuration" on page 151.

See "Requirements for agentless discovery of UNIX hosts" on page 138.

See "How agentless discovery of a UNIX or Linux host works" on page 136.

See "About Veritas InfoScale Operations Manager" on page 15.

SSH configuration requirements for agentless discovery

Veritas InfoScale 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 `PermitRootLogin` parameter to **yes**.
SSH allows access for the user account that you use for discovery	■ `AllowUsers` If you use this parameter, ensure that it allows the user account that you use for agentless discovery. ■ `DenyUsers` If you use this parameter, ensure that it does not deny the user account that you use for agentless discovery. ■ `AllowGroups` If you use this parameter, ensure that it allows the group to which the user account belongs. ■ `DenyGroups` 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 135.

See "About agentless discovery of remote hosts" on page 135.

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 146.

See "Installing OpenSSH on Linux" on page 146.

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 146.

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 146.

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 if the managed host package is already installed on that host. If the managed host package is not installed on the host, you can install the managed host package on the remote host and then add the host to Management Server.

Note: Veritas InfoScale 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 InfoScale Operations Manager does not display any error messages when you perform this task.

Note: Adding a managed host to multiple management servers is not supported.

Following are the prerequisites for adding the managed hosts to Management Server:

- Before you add a managed agent host to the Management Server, make sure that the host can communicate with the Management Server. This prerequisite is also applicable in cases where you want to install the managed host package on the host before adding it to Management Server.
- The time difference between the system clocks on the Management Server and managed host should not be more than 90 minutes.

- For installing the host package while adding a Linux host, ensure that the PasswordAuthentication field is set to yes in the `/etc/ssh/sshd_config` file on the host.

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 host to Management Server using an agent configuration

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 148.
4. In the **Result** panel, click **Ok**.

   You can view the status of **Add Hosts** task for each host in the **Recent Tasks** panel.

See "Adding the managed hosts to Management Server using an agentless configuration" on page 151.

See "Adding managed hosts to Management Server using the Auto Configure (gendeploy.pl) script" on page 157.

See "Upgrading managed host using the console" on page 74.

See "Refreshing the details of the managed host" on page 160.

See "Removing managed hosts from the Management Server domain" on page 161.

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	Click to manually specify more than one host to add.

Table 7-8 Add agent hosts panel options for agent configuration *(continued)*

Field	Description
Clone	Click to add a new entry and copy the details of the selected managed host into the new row. Once the information is copied in to a new row, you can edit the information, if required. You can use this option if you have multiple hosts with similar host names, user names, and passwords.

Import	Click to import the details of the managed hosts from a comma-separated (.csv) file from a specified location. The CSV file must include the ".csv" extension.
	
	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.
	
	You can use the manual host specification and the CSV file simultaneously to add hosts.

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 specify the option to install the managed host package on the host before adding it to Management Server.

Table 7-9

Field	Description
None	Select this option if you do not want to install the managed host package on the host before adding it to Management Server. You can use this option if the managed host package is already installed on the Linux/Unix or Windows hosts.
Install managed host package on Linux/Unix	Select this option to install the managed host package on the Linux/Unix hosts. If the managed host package is not already installed, the latest version that is uploaded in the Veritas InfoScale Operations Manager repository is installed on the managed host. If a lower version of managed host package is already installed, it is upgraded to the latest version that is uploaded in the Veritas InfoScale Operations Manager repository. Use this option if you have only Linux/Unix hosts that you want to add to Management Server.
Use root password	If you select **Install managed host package on Linux/Unix** option, the **Use root password** option is enabled. Select this option if you want to install the host package on a Linux/Unix host as a non-root user. Provide the non-root username, non-root password, and root password for the specified host. You can use this option if the Secure Shell (SSH) access is disabled for the root login on the host where you want to install the host package and perform the Add Host operation.

Table 7-9 *(continued)*

Field	Description
Install managed host package on Windows	Select this option to install the managed host package on the Windows hosts. If the managed host package is not already installed, the latest version that is uploaded in the Veritas InfoScale Operations Manager repository is installed on the managed host. If a lower version of managed host package is already installed, it is upgraded to the latest version that is uploaded in the Veritas InfoScale Operations Manager repository. Use this option if you have only Windows hosts that you want to add to Management Server.
Select Windows Managed Host	Select a Windows managed host which you want to use as a Control Host. This option is enabled only when you select the option **Install managed host package on Windows** and there is at least one Windows managed host in the domain. The Control Host add-on is installed on the specified Windows managed host, if it is not already installed. If there are no compatible Windows hosts in the domain, you need to manually install the managed host package on at least one Windows managed host and add it to the domain.

See "Adding the managed hosts to Management Server using an agent configuration" on page 147.

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 InfoScale 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.

Note: Adding a managed host to multiple management servers is not supported.

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 153.
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 147.

See "Adding managed hosts to Management Server using the Auto Configure (gendeploy.pl) script" on page 157.

See "Upgrading managed host using the console" on page 74.

See "Refreshing the details of the managed host" on page 160.

See "Removing managed hosts from the Management Server domain" on page 161.

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 7-10 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.
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.

Adding Agentless hosts to the Management Server using Profile

You can add an agentless host to the Management Server using **Profile** in Veritas InfoScale Operations Manager 8.0.2.

Before you add a managed agent host to the Management Server, make sure that the managed agent host can communicate with the Management 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 add an agentless host to Management Server using Profile

1. In the Home page of the Management Server console click **Manage Profiles**, then **Add Profile** wizard panel appears. Do the following:
   - Enter the **Profile Name**, **Username** and **Password**.
   - Click **Close**.
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, do the following:
   - Enter the **Host Name**.
   - Select the **Profile Name** which you created in step 1.
   - Enter the **SSH Port** (optional). The default value is 22.
4 Click **Finish**.
5 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 147.

See "Adding managed hosts to Management Server using the Auto Configure (gendeploy.pl) script" on page 157.

See "Upgrading managed host using the console" on page 74.

See "Refreshing the details of the managed host" on page 160.

See "Removing managed hosts from the Management Server domain" on page 161.

Add agentless hosts panel options using Profile

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 7-11 Add agentless hosts using Profile 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.
Control Host	Control Host through which the agentless host is being discovered. Windows agentless hosts can only be discovered by Windows Control Hosts.
Host Name	Enter host name or the IP address that you can use to reach the managed host from Management Server.
Profile Name	Allows you store the credentials for the agentless host.
SSH Port	Enter the Port. **Note:** The default value for the SSH port is 22. This port number is editable.
Advanced	Lets you specify type and location of privilege control software to use on the agentless hosts. 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.

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:

For Unix host

```
Host,User,Password,Port,Software,Softwarelocation
Host,Profile,Port,Software,Softwarelocation
```

Note: Port, Software, Softwarelocation are optional.

For Unix and Windows host

```
Host,User,Password
Host,Profile
```

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.

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 InfoScale 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.

Note: Adding a managed host to multiple management servers is not supported.

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`
       where, *filename* is the name of the script that you specify.
       For example,
       `/opt/VRTSsfmh/bin/gendeploy.pl --out example.pl`
     - 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>`
       where, *filename* is the name of the script that you specify.
       For example, `perl.exe gendeploy.pl --out example.pl`
2. Copy the script generated by `gendeploy.pl` 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 InfoScale 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 147.

See "Adding the managed hosts to Management Server using an agentless configuration" on page 151.

See "Upgrading managed host using the console" on page 74.

See "Refreshing the details of the managed host" on page 160.

See "Removing managed hosts from the Management Server domain" on page 161.

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 160.

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 143.

See "Adding the managed hosts to Management Server using an agentless configuration" on page 151.

Edit agentless host panel options

Use this wizard panel to edit the details of configured agentless hosts.

Table 7-12 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 159.

See "Adding managed hosts to Management Server using the Auto Configure (gendeploy.pl) script" on page 157.

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 ?.

See "Adding the managed hosts to Management Server using an agentless configuration" on page 151.

See "Adding managed hosts to Management Server using the Auto Configure (gendeploy.pl) script" on page 157.

See "Removing managed hosts from the Management Server domain" on page 161.

See "Verifying the version of a managed host in the console" on page 78.

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 147.

See "Adding the managed hosts to Management Server using an agentless configuration" on page 151.

See "Adding managed hosts to Management Server using the Auto Configure (gendeploy.pl) script" on page 157.

See "Refreshing the details of the managed host" on page 160.

Chapter 8

Setting up user access

This chapter includes the following topics:

- About managing authentication brokers and authentication domains in the Veritas InfoScale Operations Manager domain
- Adding 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
- Configuring LDAP using CLI
- Configuring Single Sign-On in Veritas InfoScale Operations Manager
- Enabling the authentication domain
- Disabling the authentication domain
- About predefined roles in Veritas InfoScale Operations Manager
- About Organizations, objects, and roles in Veritas InfoScale 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 InfoScale Operations Manager console
- Example: Managing user access in Veritas InfoScale Operations Manager using Organizations and existing user groups

About managing authentication brokers and authentication domains in the Veritas InfoScale Operations Manager domain

An authentication broker is an intermediate registration and certification authority that can authenticate clients including users or services.

In Veritas InfoScale 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 InfoScale Operations Manager.

Veritas InfoScale Operations Manager supports the authentication mechanism that is configured in the operating system, including Pluggable Authentication Modules (PAM), Network Information Service (NIS), or NIS+. In addition to the native operating system authentication, Veritas InfoScale Operations Manager supports Lightweight Directory Access Protocol (LDAP) and Active Directory (AD).

Veritas InfoScale 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 InfoScale 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 "Adding Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server" on page 165.

See "Unconfiguring Lightweight Directory Access Protocol or Active Directory configuration from the authentication broker" on page 170.

See "Assigning permissions to user groups for a perspective" on page 181.

Adding Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server

You can add 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 add is in the enabled state.

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

To add LDAP or AD-based authentication

1. In the Home page on the Management Server console, click **Settings**.
2. Do one of the following:
   - Click **Add LDAP/AD**.
   - Click **Security**. In the **Brokers & Domains** tab, click **Add LDAP/AD**.
3. In the **Add LDAP/AD** wizard panel, enter the details, and click **Next**.

   See "Add LDAP/AD panel options" on page 166.
4. In the **Add LDAP/AD** wizard panel, enter a domain name, specify the search base, and click **Finish**.

   See "Add LDAP/AD panel options to specify the domain name" on page 168.
5. In the **Add LDAP/AD** panel that confirms that you have added the LDAP or AD-based authentication, click **OK**.

See "About managing authentication brokers and authentication domains in the Veritas InfoScale Operations Manager domain" on page 164.

See "Unconfiguring Lightweight Directory Access Protocol or Active Directory configuration from the authentication broker" on page 170.

Add LDAP/AD panel options

Use this wizard panel to add LDAP or AD-based authentication on the primary authentication broker.

Table 8-1 Add LDAP/AD panel 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 Add LDAP/AD panel 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: ■ *username@domainname.com* ■ *domainname\username* For example, You can provide the DN as Administrator@enterprise.*domainname*.com ENTERPRISE\Administrator For RFC 2307 compliant LDAP servers, specify complete bind DN. For example, **cn=Manager,dc=vss,dc=veritas,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 Add LDAP/AD panel 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 InfoScale 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 "Adding Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server" on page 165.

Add 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 Add LDAP/AD panel 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 Add LDAP/AD panel 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: ou=HR,ou=People,dc=veritas,dc=com |-sampleuser ou=Engg,ou=People,dc=veritas,dc=com |-Eng1 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=veritas,dc=com**

See "Adding Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server" on page 165.

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 InfoScale Operations Manager domain" on page 164.

See "Viewing the details of the authentication broker and the domains associated with the broker" on page 257.

See "Adding Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server" on page 165.

Configuring LDAP using CLI

InfoScale Operations Manager leverages existing user groups that are present in the Lightweight Directory Access Protocol (LDAP) or the Active Directory (AD) configuration of your environment. Alternatively, it uses the native authentication mechanism of a Windows or a UNIX system. You can use the Management Server console to configure LDAP and assign permissions to user groups. However, to perform this task, your user group must be assigned the Admin role from the perspective. When you apply InfoScale Operations Manager patch 7.4.2.200, users other than administrators also can perform the following tasks using the command line interface (CLI):

- Configuring LDAP in InfoScale Operations Manager
- Unconfiguring an existing LDAP configuration
- Changing user permissions in InfoScale Operations Manager
- Changing the password for the bind user from the existing LDAP configuration in InfoScale Operations Manager

For details on the syntax and usage of the command-line options, log on to the CMS, and run the following command: `# /opt/VRTSsfmcs/webgui/jre/bin/java -cp /opt/VRTSsfmcs/webgui/tomcat/lib/vom_shared.jar vrts.vom.shared.util.ConfigLdap help`

Important: Follow these guidelines when you use the command-line options for this utility:

- The utility should be run from the master node only.
- File name and paths should not include spaces. Otherwise, you might encounter errors, especially on Windows systems.
- User input options that are specified in the CLI prompts are case sensitive. You must enter a string exactly as displayed in response to the prompt.

Configuring an LDAP domain

To confirure an LDAP domain

1. Log on to the CMS.
2. To configure a LDAP domain, run the following command:`# /opt/VRTSsfmcs/webgui/jre/bin/java -cp /opt/VRTSsfmcs/webgui/tomcat/lib/vom_shared.jar vrts.vom.shared.util.ConfigLdap configure`

   The utility prompts you to choose whether you want to only configure the LDAP domain or only assign permissions to the user groups.
3. Enter Yes to only configure the LDAP domain but not assign permissions.

   Note: Alternatively, you can enter No and later run the vrts.vom.shared.util.ConfigLdap configure utility only to assign permissions for a user group.
4. Enter the name of the LDAP server that you want to configure.

5. Enter the port for the LDAP server.

   The default port for LDAP without SSL certificates is 389 and for LDAP with SSL certificates is 636.

6. Enter the name of the bind user or the DNS name.
7. Enter a password for the bind user account.
8. (Optional) Enter the path of the SSL certificate. Press Enter to skip this step.
9. Enter the username of the user on the LDAP or the AD server.

   This name is used to determine the default search base.

10. Enter a numeric or an alphabetical LDAP domain configuration name.

    Note: Alphanumeric characters are not supported.

11. Enter the search base.

    The LDAP domain is discovered and enabled.

12. When prompted, enter Yes to add permission to a user group in the added LDAP domain. Enter No to skip this step.
13. Restart the Web service to reflect the configuration changes on the browser-based CMS interface.

Assigning permissions to a user group

You can assign administrator permissions to the user groups in an existing or a newly configured LDAP domain.

Note: To assign the Guest or the Operator role to a user group on a perspective, you must log in as an administrator using the browser-based CMS user interface.

To assign permissions to a user group

1. Log in to the CMS as an administrator.
2. To assign permissions, run the following command:#

   ```
   /opt/VRTSsfmcs/webgui/jre/bin/java -cp
   /opt/VRTSsfmcs/webgui/tomcat/lib/vom_shared.jar
   vrts.vom.shared.util.ConfigLdap configure
   ```

   The system prompts you to choose whether you want to only configure the LDAP domain or only assign permissions to the user groups.

3. Enter No to only assign permissions for a user group.
4. At the prompt, enter Yes to add permissions to a user group in an existing LDAP domain.
5. Enter the name of the LDAP server that you want to configure.
6. Enter the LDAP or the AD domain that corresponds to the user group to which you want to assign permissions.
7. Enter the name of the user group to which you want to assign permissions.
8. Enter one or more perspectives on which you want to assign the permission to the user group: SERVER, AVAILABILITY, STORAGE, VIRTUALIZATION, and INFRA.

   Note: This input is case sensitive. Ensure that your input matches exactly with the input options specified at the prompt.

9. Enter Admin to assign the administrator permissions to the user group on the selected perspective.

   Note: This input is case sensitive. The system checks and removes any old permissions that are assigned to the specified user group.

10. When prompted, enter Yes to continue assigning permissions to other groups in the same LDAP domain, or enter No to exit.

    On successful completion, the newly assigned permissions are visible on the browser-based CMS user interface.

Unconfiguring an existing LDAP configuration

Perform the following steps to unconfigure an existing LDAP configuration:

To unconfigure an existing LDAP configuration

1. Log on to the CMS as an administrator.
2. Run the following command:`# /opt/VRTSsfmcs/webgui/jre/bin/java -cp /opt/VRTSsfmcs/webgui/tomcat/lib/vom_shared.jar vrts.vom.shared.util.ConfigLdap unconfigure`

3 Enter the name of the existing LDAP or the AD configuration that you want to unconfigure.

4 Restart the Web service to reflect the configuration changes on the browser-based CMS interface.

Changing the password for a bind user

You can change the password for an existing bind user account using the changepass command. While using this command, ensure that except for the password, you provide the exact details of the existing

To change the password for a bind user

1 Log on to the CMS as an administrator.

2 Run the following command:`# /opt/VRTSsfmcs/webgui/jre/bin/java -cp /opt/VRTSsfmcs/webgui/tomcat/lib/vom_shared.jar vrts.vom.shared.util.ConfigLdap changepass`

3 Enter the existing LDAP server name.

4 Enter the port for the LDAP server.

The default port for LDAP without SSL certificates is 389 and for LDAP with SSL certificates is 636.

5 Enter the name of the bind user or the DNS name.

6 Enter a new password for the bind user account.

(Optional) Enter the path of the SSL certificate. Press Enter to skip this step.

7 Enter the username of the user on the LDAP or the AD server.

This name is used to determine the default search base.

8 Enter a numeric or an alphabetical LDAP domain configuration name.

Note: Note: Alphanumeric characters are not supported.

9 Enter the search base.

Configuring Single Sign-On in Veritas InfoScale Operations Manager

Veritas InfoScale Operations Manager provides Single Sign-On (SSO) services for Veritas InfoScale Operations Manager users. SSO is based on SAML protocol and

supporting Shibboleth, ADFS Identity Provider (IDP). SAML enables SSO, a term that means you can sign in once, and those same credentials can be reused to sign into other applications or vice versa.

Identity Provider: Performs authentication and passes the user's identity and authorization level to the service provider.

Service Provider: Trusts the identity provider and authorizes the given user to access the requested resource. In this case, Veritas InfoScale Operations Manager application works as a service provider.

To enable SSO in Veritas InfoScale Operations Manager

1. Download IDP metadata and save in the .xml format.

   Note: As Veritas InfoScale Operations Manager supports Shibboleth and ADFS, you can download either one of the IDP based on your requirement.

IDP	URL
Shibboleth	a. Open the IDP metadata using the following URL in browser: `https://<idp-hostname>/idp/shibboleth` b. Copy the content in .xml file format.
ADFS	a. Open the IDP metadata using this following URL in browser: `https://<idp-hostname>/FederationMetadata/2007-06/FederationMetadata.xml` b. ADFS metadata file gets downloaded use that as a IDP metadata file.

2. Sign in to Veritas InfoScale Operations Manager CMS.
3. Select **Settings** icon from the right-side top corner.
4. In the Setting tab, select and click **Management Server.**

5 On the Management Server page, in the **Single sign-on using SAML** pane, setup the IDP settings with the following values:

(a) Click **Browse** to locate the IDP metadata xml file from your local system and click **Upload** to upload the located xml file.

Note: Ensure that you are uploading the xml file that is downloaded from the URL as mentioned in the first step of this procedure.

(b) Enter the **IDP** URL. For example: `https://idp-hostname/idp/shibboleth`

(c) Enter **Domain Name**. For example: ssoDomian.test

(d) Click **Save Settings**.

Note: To disable Single sign-on, clear **Enable Single sign-on Authentication** checkbox and click **Save Settings**. To delete Single sign-on settings, click **Delete Settings**, in the confirmation message; click **Yes** to delete and **No** to cancel the operation.

---

6 Restart Veritas InfoScale Operations Manager Web server. Use the following command for the different platforms:

OS	Command
Linux CMS	`/opt/VRTSsfmcs/bin/vomsc --restart web`
Win CMS	`InstalledDrive/Program Files/Veritas/VRTSsfmcs/bin/vomsc --restart web`

If the Web server start-up fails, check xml file uploaded at the location.

OS	Location
Linux	`/var/opt/VRTSsfmcs/conf/IdpMetadata.xml`
Win	`InstallDrive/ProgramData/Symantec/VRTSsfmcs/conf/IdpMetadata.xml`

Ensure that the metadata is in proper xml format which contains only xml tags.

7 Get the Veritas InfoScale Operations Manager metadata from URL, **https://<*CMS-Name*>:14161/vom/saml2/service-provider-metadata/one**, and do the following:

a. Enter Veritas InfoScale Operations Manager metadata URL in browser and press enter, one xml file gets downloaded. (Example: `saml-one-metadata.xml`).

b. Provide the downloaded Veritas InfoScale Operations Manager application xml file to IDP administrator to configure IDP for SSO. On successful configuration of IDP, you receive a confirmation from the administrator.

Following are the properties for ADFS to send to VIOM application:

LDAP attributes	Outgoing claim types
Is-Member-Of-DL	memberOf
Display-Name	displayName
SAM-Account-Name	sAMAccountName
User-Principal-Name	Name ID

Once the IDP and SP (Veritas InfoScale Operations Manager) metadata is generated then you need to configure user group information.

8 Follow the steps to configure user group:

a. Sign in to Veritas InfoScale Operations Manager CMS without SSO.

b. Go to Settings > Security > Permissions tab.

c. Select **Perspective** from the drop-down list.

d. Select **User group**, and provide domain name and user group name, and click **OK**.

e. Select role and click **Add**.

9 When you have done all the configurations, do the following:

a. On login page, click **Login with SSO**.

The browser redirects to login page of identity provider.

b. Enter the credentials like username and password.

Once authenticated, The Veritas InfoScale Operations Manager dashboard console appears.

Enabling the authentication domain

Using the Management Server console, you can enable the authentication domains that are associated with an authentication broker, LDAP, or AD. You must enable an authentication domain to do the following:

- Display the authentication domain on the Veritas InfoScale Operations Manager login page.
- To assign permissions to the user groups for the perspectives.

To enable the authentication domain

1. In the Management Server console, click **Settings**.
2. Click **Security.**
3. In the **Brokers & Domains** tab, right-click the domain and select **Enable**.
4. In the **Enable Domains** wizard panel, review the domain name and type, and click **OK**.

See "About managing authentication brokers and authentication domains in the Veritas InfoScale Operations Manager domain" on page 164.

See "Viewing the details of the authentication broker and the domains associated with the broker" on page 257.

See "Adding Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server" on page 165.

See "Unconfiguring Lightweight Directory Access Protocol or Active Directory configuration from the authentication broker" on page 170.

See "Disabling the authentication domain" on page 178.

Disabling the authentication domain

Using the Management Server console, you can disable the authentication domain that is associated with an authentication broker, AD, or LDAP. When you disable a domain, it is not displayed on the Veritas InfoScale Operations Manager login page and you cannot assign permissions to the user groups for the perspectives.

To disable the authentication domain

1. In the Management Server console, click **Settings**.
2. Click **Security.**

3 In the **Brokers & Domains** tab, right-click the domain and select **Disable**.

4 In the **Disable Domains** wizard panel, review the domain name and type, and click **OK**.

See "About managing authentication brokers and authentication domains in the Veritas InfoScale Operations Manager domain" on page 164.

See "Viewing the details of the authentication broker and the domains associated with the broker" on page 257.

See "Adding Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server" on page 165.

See "Unconfiguring Lightweight Directory Access Protocol or Active Directory configuration from the authentication broker" on page 170.

See "Enabling the authentication domain" on page 178.

About predefined roles in Veritas InfoScale Operations Manager

Veritas InfoScale Operations Manager has three predefined roles: Admin, Operator, and Guest. Veritas InfoScale 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 "Assigning permissions to user groups for a perspective" on page 181.

About Organizations, objects, and roles in Veritas InfoScale Operations Manager

Organization is a collection of objects in a perspective that can be secured and managed as a group. Organizations can be created in all perspectives except in

the **Management Server** perspective. 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 InfoScale Operations Manager 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

Table 8-4 Objects within an Organization *(continued)*

Perspective	Object
Virtualization	Virtualization servers

See "About predefined roles in Veritas InfoScale Operations Manager" on page 179.

See "Assigning permissions to user groups for a perspective" on page 181.

Assigning permissions to user groups for a perspective

Veritas InfoScale 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 InfoScale Operations Manager" on page 179.

8 In the **Success** panel click **OK**.

See "Modifying permissions assigned to user groups for a perspective" on page 182.

See "Deleting permissions assigned to user groups on a perspective" on page 183.

Modifying permissions assigned to user groups for a perspective

Veritas InfoScale 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 InfoScale Operations Manager" on page 179.

See "Deleting permissions assigned to user groups on a perspective" on page 183.

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 InfoScale Operations Manager" on page 179.

See "Modifying permissions assigned to user groups for a perspective" on page 182.

Restricting users or user groups from accessing the Veritas InfoScale 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
- 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@exampledomain.com:user
firstname2_lastname2@exampledomain.com:user
alpha_usergroup@exampledomain.com:group
beta_usergroup@exampledomain.com:group
```

Place the file at the following location:

- For Linux-based Management Server: /var/opt/VRTSsfmcs/conf/
- For Windows-based Management Server (2019/2022): C:\ProgramData\Symantec\VRTSsfmcs\conf\

Precede a comment in the `.esmwebdeny` file with "#".

See "Adding Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server" on page 165.

See "Assigning permissions to user groups for a perspective" on page 181.

See "Deleting permissions assigned to user groups on a perspective" on page 183.

Example: Managing user access in Veritas InfoScale 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.
- 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 InfoScale Operations Manager Management Server User Guide*.

In this example, we use the following names:

Domain	alpha.veritasdomain.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 InfoScale 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.

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.veritasdomain.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 **exampledomain.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.

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 "Adding Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server" on page 165.

See "About predefined roles in Veritas InfoScale Operations Manager" on page 179.

See "Assigning permissions to user groups for a perspective" on page 181.

Chapter 9

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 InfoScale 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 260.

See "Configuring SMTP settings for email notifications" on page 242.

See "Configuring SNMP trap settings for alert notifications" on page 243.

Creating rules in the Management Server perspective

In the Management Server console, you can create rules to trigger various actions based on alert conditions.

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

For more information on applying rules to specific Organizations, see *Veritas InfoScale Operations Manager 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 192.
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 193.
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 193.
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 194.
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 195.

See "Deleting rules in the Management Server perspective" on page 199.

See "Enabling rules in the Management Server perspective" on page 200.

See "Disabling rules in the Management Server perspective" on page 200.

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.
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.

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.

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.
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 243.
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)

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.

Table 9-4 Create Rule - Enter name and description options *(continued)*

Field	Description
Enable	Clear to disable the rule. An enabled rule monitors alerts for the defined conditions.

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 196.
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 197.
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 197.

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 198.

9 In the **Edit Rule - Result** panel, verify that the rule has been successfully created, and click **OK**.

See "Deleting rules in the Management Server perspective" on page 199.

See "Enabling rules in the Management Server perspective" on page 200.

See "Disabling rules in the Management Server perspective" on page 200.

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 195.

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 195.

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 243.
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.
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 195.

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.

Table 9-8 Edit Rule - Description *(continued)*

Field	Description
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 195.

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 199.
6. In the **Delete Rule - Result** panel, click **OK**.

See "Editing rules in the Management Server perspective" on page 195.

See "Enabling rules in the Management Server perspective" on page 200.

See "Disabling rules in the Management Server perspective" on page 200.

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 199.

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 200.
6. In the **Enable Rule - Result** panel, click **OK**.

See "Disabling rules in the Management Server perspective" on page 200.

See "Editing rules in the Management Server perspective" on page 195.

See "Deleting rules in the Management Server perspective" on page 199.

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 200.

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 201.
6. In the **Disable Rule - Result** panel, click **OK**.

See "Enabling rules in the Management Server perspective" on page 200.

See "Editing rules in the Management Server perspective" on page 195.

See "Deleting rules in the Management Server perspective" on page 199.

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 200.

About faults and risks

Veritas InfoScale 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 258.

See "Viewing faults in the Management Server perspective " on page 258.

See "Suppressing a fault definition in the Management Server perspective" on page 204.

See "Restoring a suppressed fault definition in the Management Server perspective" on page 205.

See "Suppressing faults in the Management Server perspective" on page 202.

See "Restoring a suppressed fault in the Management Server perspective" on page 203.

Suppressing faults in the Management Server perspective

Using the Management Server console, you can suppress one or more faults in Veritas InfoScale 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 202.

See "Viewing faults in the Management Server perspective " on page 258.

See "Restoring a suppressed fault in the Management Server perspective" on page 203.

Suppress Faults panel options

Use this panel to suppress the faults in Veritas InfoScale 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.
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 InfoScale 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 202.

Restoring a suppressed fault in the Management Server perspective

You can restore the fault that is suppressed in Veritas InfoScale 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 InfoScale 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 202.

See "Viewing faults in the Management Server perspective " on page 258.

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 InfoScale 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 205.

See "Viewing the faults definitions" on page 258.

See "Restoring a suppressed fault definition in the Management Server perspective" on page 205.

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 InfoScale 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 InfoScale 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 204.

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 InfoScale 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 204.

See "Viewing the faults definitions" on page 258.

Chapter 10

Setting up virtualization environment discovery

This chapter includes the following topics:

- About the virtualization technologies supported
- About Control Hosts in Veritas InfoScale Operations Manager
- Requirements for discovering vCenter and ESX servers using Veritas InfoScale Operations Manager
- About near real-time discovery of VMware events
- Setting up near real-time discovery of VMware events
- Configuration settings for VMware vCenter discovery
- 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
- Adding a virtualization server
- 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 InfoScale 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 InfoScale 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 InfoScale 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 InfoScale Operations Manager Management Server domain, provides storage mapping discovery.

For Kernel-based Virtual Machine (KVM) discovery, Veritas InfoScale 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 InfoScale 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 217.

See "Requirements for discovering logical partitions" on page 219.

See "Requirements for Microsoft Hyper-V virtualization discovery" on page 220.

See "Requirements for Kernel-based Virtual Machine (KVM) virtualization discovery" on page 220.

About Control Hosts in Veritas InfoScale Operations Manager

Veritas InfoScale Operations Manager uses Control Hosts as a discovery mechanism. In Veritas InfoScale 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 InfoScale Operations Manager Management Server or a managed host that reports to Management Server.

Information on VMware Virtualization Infrastructure (vSphere)

In Veritas InfoScale Operations Manager, you can configure Veritas InfoScale 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 InfoScale Operations Manager, you must download the Control Host Add-on from the Veritas 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 vCenter Servers 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 InfoScale Operations Manager creates a user named 'vomuser' with the administrative privileges.

Ensure that the Control Hosts can communicate with 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.

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 Linux 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 using agentless method.

See “About agentless discovery using the Control Host” on page 135.

See “About the virtualization technologies supported” on page 208.

See “Requirements for discovering vCenter and ESX servers using Veritas InfoScale Operations Manager” on page 210.

Requirements for discovering vCenter and ESX servers using Veritas InfoScale Operations Manager

The following are the requirements for discovering VMware Infrastructure using Veritas InfoScale 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 InfoScale Operations Manager to discover.

About near real-time discovery of VMware events

With near real-time discovery of VMware events, any change in the state of a virtual machine (for example, VM powered on) and changes occurring at the vCenter Server infrastructure-level (for example, VM created) in the Management Server domain are updated in the Veritas InfoScale Operations Manager database in near real-time.

The near real-time discovery of VMware infrastructure enables the partial discovery of ESX servers managed under a vCenter Server. For example, if an SNMP trap is received for a virtual machine (VM1) hosted on ESX1, Veritas InfoScale Operations Manager runs the discovery cycle only for ESX1. Other ESX servers under that vCenter Server are not re-discovered. This discovery is triggered by the event notification from the VMware vCenter Server to the Management Server using SNMP traps.

For near real-time discovery, ensure to configure the VMware vCenter Server and the Management Server in the same domain. This discovery is supported for the following events occurring at a VMware vCenter Server-level:

Table 10-1 Supported events for near-real time discovery

Discovered state	Event as shown in VMware vCenter Server	Applicable with the Management Server version
Virtual machine powered on	VM powered on	8.0.2, or later
Virtual machine powered off	VM powered off	8.0.2, or later
Virtual machine Distributed Resource Scheduler (DRS) powered on	DRS VM powered on	8.0.2, or later
Virtual machine suspended	VM suspended	8.0.2, or later

Table 10-1 Supported events for near-real time discovery *(continued)*

Discovered state	Event as shown in VMware vCenter Server	Applicable with the Management Server version
Virtual machine created	VM created	8.0.2, or later
Virtual machine migrated Hot migration: A powered-on virtual machine is migrated from one ESX server to another ESX server.	VM migrated	8.0.2, or later
Virtual machine relocated from one ESX server to another Cold migration: A powered-off virtual machine is migrated from one ESX server to another ESX server.	VM relocating	8.0.2, or later
Virtual machine renamed	VM renamed	8.0.2, or later
Virtual machine migrated to another host by VMware DRS (Distributed Resource Scheduler)	DRS VM migrated	8.0.2, or later

Note: The near real-time update of virtual machines is supported on VMware vCenter Server 7.x.

See "Setting up near real-time discovery of VMware events" on page 212.

See "Configuring the VMware vCenter Server to generate SNMP traps" on page 214.

Setting up near real-time discovery of VMware events

To set up near real-time discovery of VMware events, configure the VMware vCenter Server SNMP settings with the Management Server address as the receiver URL. The Management Server receives the updates when you add the VMware vCenter Server to the Management Server.

The VMware vCenter Server generates SNMP traps for the following events:

- When a virtual machine's state changes - powered on, powered off, and suspended.
- When any other virtual infrastructure-related changes are detected. For example, when a virtual machine is created, migrated, or renamed.

The vCenter Server sends the SNMP 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 InfoScale Operations Manager component of near real-time discovery is `xtrapd`. It runs as a daemon on Linux and as a service on Windows operating system. `xtrapd` detects the SNMP trap that is sent from the VMware vCenter Server, updates the virtual machine records in the Veritas InfoScale 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 discovery of VMware events, complete the following steps:

Table 10-2 Setting up near real-time (NRT) discovery of VMware events

Step	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 214.
Using the Management Server console:		

Table 10-2 Setting up near real-time (NRT) discovery of VMware events *(continued)*

Step	Action	Description
Step 2	Add VMware vCenter Server to Management Server.	When you add a VMware vCenter Server to Management Server, the `xtrapd` daemon on the Management Server starts accepting SNMP traps from the specified VMware vCenter Server. See "Adding a virtualization server" on page 221. **Note:** If you have not configured the VMware vCenter Server before adding it to the Veritas InfoScale Operations Manager domain, a warning message is displayed. It does not affect the vCenter Server discovery. However, near real-time discovery of VMware events is not functional. If you want to enable the discovery, 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 discovery of VMware events is enabled. To disable it, you need to remove the Management Server as the SNMP receiver in the VMware vCenter Server and refresh vCenter configuration in Veritas InfoScale Operations Manager Management Server.

See "About near real-time discovery of VMware events" on page 211.

Configuring the VMware vCenter Server to generate SNMP traps

Provide the following information to configure the vCenter Server to generate SNMP traps:

- Using the vCenter Server console, configure the Management Server as the SNMP trap receiver.

  In the Home page of vSphere Client, select **vCenter Server Settings** and then select SNMP configuration. Enable one of the SNMP receivers and enter the 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 in Veritas InfoScale Operations Manager Management Server. **Note:** For a Windows Management Server configured in high availability (HA) environment, provide the virtual IP address of the Management Server HA setup.
Community String	Provide community string. SNMP versions v1 and v2 are supported.

- Configure alarm for generating SNMP traps when a virtual machine state changes or any virtual infrastructure-related change occurs.
  It includes adding alarm to monitor the changes related to virtual machine state and vCenter Server infrastructure, and then adding the appropriate action (for example, send a notification trap).
  - 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:

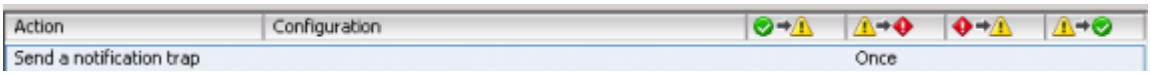
Field	Description
Alarm Name	Provide the name of the alarm.
Description	Provide additional information about the alarm.
Alarm Type	Select Virtual Machines in the **Monitor** drop-down list. Select **Monitor for specific events occurring on this object, for example, VM powered On** option. Ensure that **Enable this alarm** check box is selected.

  - In the **Triggers** tab, add the required triggers to monitor the states of the virtual machine. For example, VM created, VM migrated, VM powered on, VM powered off, VM suspended, DRS VM powered on (for clustered

environment with DRS enabled) and so on. The values of the fields are as follows:

For the following value of an event...	Select the following status...
VM powered on	Unset
VM powered off	Unset
DRS VM powered on	Unset
VM suspended	Unset
VM created	Unset
VM migrated	Unset
VM relocating	Unset
VM renamed	Unset
DRS VM migrated	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 discovery of VMware events" on page 211.

Configuration settings for VMware vCenter discovery

To change the number of vCenter Servers and the ESX servers that are configured for the periodic vCenter discovery, you need to edit the following values in the `virtualization.conf` file. The file is created during the installation of Control Host.

- vc_max_processes
- esx_batchsize
- ds_browse_batchsize

- datastore_browse

Where:

`vc_max_processes`: The number of processes that are created for the discovery of the vCenter Servers. One process per vCenter Server is created for the discovery.

`esx_batchsize`: The maximum number of ESX/ESXi servers that gets discovered in a batch. Default value of this parameter is 300. If there are more than 300 ESX/ESXi servers in a vCenter, discovery of such vCenter creates batches of ESX/ESXi servers and discovers them.

`ds_browse_batchsize`: The number of datastores that gets discovered on a vCenter in parallel. Default value of this configuration parameter is 25. This configuration parameter works only if datastore_browse is set to 1.

`datastore_browse`: This flag indicates if datastores need to be browsed for discovering the details of virtual disks. Default value of this configuration parameter is 0 which means datastore browse is skipped. In case datastore browse is required, set this parameter to 1.

The `virtualization.conf` file is located at:

- On Linux Control Host: `/var/opt/VRTSsfmh`
- On Windows Control Host: `%ALLUSERSPROFILE%\Symantec\VRTSsfmh\`

See "About near real-time discovery of VMware events" on page 211.

See "Setting up near real-time discovery of VMware events" on page 212.

See "Configuring the VMware vCenter Server to generate SNMP traps" on page 214.

Requirements for discovering the Solaris zones

The following are the requirements for discovering Solaris zones in Veritas InfoScale Operations Manager:

- Install the `VRTSsfmh` package on one or more traditional hosts that contains Global Zones. This helps Veritas InfoScale Operations Manager discover non-global-zones that are configured on the Global Zones.
- Ensure that the managed hosts with the Solaris 11 operating system contain non-Global Zones.
- Ensure that the managed hosts with the Solaris 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 208.

See "Requirements for the zlogin utility on non-Global Zones" on page 218.

See "Requirements for devices exported to non-Global Zones" on page 218.

See "Requirements for file systems exported to non-Global Zones" on page 218.

Requirements for the zlogin utility on non-Global Zones

Veritas InfoScale 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 217.

Requirements for devices exported to non-Global Zones

Veritas InfoScale 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 InfoScale 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 217.

Requirements for file systems exported to non-Global Zones

Veritas InfoScale 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 InfoScale 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 217.

Requirements for discovering Solaris Logical domains

The following are the requirements for discovering Solaris LDoms using Veritas InfoScale Operations Manager:

- Install the `VRTSsfmh` package on one or more traditional hosts with the Solaris operating system on which you want Veritas InfoScale 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 208.

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 InfoScale 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 InfoScale Operations Manager as agents.
- You must have at least hmcoperator role in HMC to perform these tasks.

Note: The Veritas InfoScale 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 208.

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 208.

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 208.

Adding a virtualization server

In Veritas InfoScale Operations Manager, you must add the virtualization servers to let a Control Host discover the virtual servers. You can add the virtualization servers 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 add a virtualization server, 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 add a virtualization server in Veritas InfoScale Operations Manager

1. In the Home page on the Management Server console, click **Settings**.
2. Do one of the following:
   - Click **Add Virtualization Server**
   - Click **Virtualization**, and then click **Add Virtualization Server**.
   - Click **Virtualization**, right-click **Data Center** and select **Add Virtualization Server**.
3. In the **Add Virtualization Server** wizard panel, enter the details, and click **Next**.

   See “Add Virtualization Server panel options” on page 222.
4. In the **Select option** wizard panel, select the method for virtualization discovery of the servers, and click **Finish**.

   See “Add Virtualization Server panel options” on page 223.
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 224.

See "Refreshing a virtualization discovery configuration" on page 226.

See "Removing a virtualization discovery configuration" on page 227.

Add Virtualization Server panel options

Use this wizard panel to add a virtualization server for discovery in Veritas InfoScale Operations Manager.

Table 10-3 Add 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.
Control host	Select the name of the control host from the drop-down list: ■ In case of VMware configuration, Veritas InfoScale 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 InfoScale 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.

Table 10-3 Add Virtualization Server panel options *(continued)*

Field	Description
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 "Adding a virtualization server" on page 221.

Add Virtualization Server panel options

Use this wizard panel to choose a method to enable the virtualization discovery configuration of servers.

Table 10-4 Add Virtualization Server panel options

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 "Adding a virtualization server" on page 221.

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 InfoScale 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 224.
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 225.
6. In the **Result** panel, view the progress of the configuration, click **OK**.

See "Refreshing a virtualization discovery configuration" on page 226.

See "Removing a virtualization discovery configuration" on page 227.

Edit Configuration panel options

Use this wizard panel to edit the virtualization server discovery that you have configured in Veritas InfoScale Operations Manager.

Table 10-5 Virtualization configuration panel options for editing configurations

Field	Description
Configuration Type	Displays the configuration type.

Table 10-5 Virtualization configuration panel options for editing configurations *(continued)*

Field	Description
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 InfoScale 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.
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 224.

Edit Configuration panel options for method selection

Use this wizard panel to choose a method to edit the virtualization discovery configuration of servers.

Table 10-6 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.

Table 10-6 Virtualization configuration panel options for method selection *(continued)*

Field	Description
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 224.

Refreshing a virtualization discovery configuration

Using the Management Server console, you can refresh the virtualization server that Veritas InfoScale 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 "Adding a virtualization server" on page 221.

See "Editing a virtualization discovery configuration" on page 224.

See "Removing a virtualization discovery configuration" on page 227.

Refreshing an ESX Server discovery

Using the Management Server console, you can refresh the discovery of one or more ESX servers that are configured under a selected VMware vCenter Server.

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

To refresh the discovery of an ESX server

1. In the Home page on the Management Server console, click **Settings**.
2. Click **Virtualization**.
3. Under the **Virtualization Configurations** tab, you can view the details of virtualization configuration. For example, the name of the virtualization server (vCenter Server) used in the configuration, its type, associated control host and other parameters. Select the desired virtualization configuration.
4. The **Configured Virtualization Servers** tab lists the ESX servers managed under the vCenter Server that is part of the selected virtualization configuration.
5. Right-click the required ESX server and click **Refresh.** Press Ctrl or Shift for the selection of multiple ESX servers.
6. In the **Refresh Virtualization Server** wizard panel, click **Refresh**.
7. In the **Result** panel, click **OK**.

See "Adding a virtualization server" on page 221.

See "About the virtualization technologies supported" on page 208.

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 "Editing a virtualization discovery configuration" on page 224.

See "Refreshing a virtualization discovery configuration" on page 226.

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 InfoScale Operations Manager 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 8.0.2.

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**.

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 InfoScale Operations Manager 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**.

Chapter 11

Deploying hot fixes, packages, and patches

This chapter includes the following topics:

- About deploying Veritas InfoScale 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 InfoScale Operations Manager hot fix or package to the repository
- Installing a Veritas InfoScale Operations Manager hot fix, package, or patch
- Removing a hot fix, package, or patch from the repository
- Canceling deployment request for a hot fix, package, or patch
- Installing a Veritas InfoScale Operations Manager hot fix on a specific managed host

About deploying Veritas InfoScale Operations Manager hot fixes

You can download and install hot fixes for Veritas InfoScale Operations Manager in one of the following ways:

- Download from Veritas Services and Operations Readiness Tools (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 Storage Foundation High Availability hot fixes, you need to install the Patch Installer add-on. For more information on deploying Storage Foundation High Availability hot fixes using the Patch Installer add-on, refer to *Veritas InfoScale Operations Manager Add-ons User Guide*.

See "About deploying Veritas InfoScale Operations Manager add-ons" on page 109.

See "About deploying maintenance release packages and patches" on page 231.

See "Downloading a Veritas InfoScale Operations Manager add-on" on page 110.

See "Uploading a Veritas InfoScale Operations Manager hot fix or package to the repository" on page 233.

See "Installing a Veritas InfoScale Operations Manager hot fix, package, or patch" on page 234.

About deploying maintenance release packages and patches

You can download and install the maintenance release packages and patches for Veritas InfoScale Operations Manager that are **VOM Deployable** in one of the following ways.

- Download from Veritas Services and 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 InfoScale Operations Manager are available in tape archive (tar.gz) format, Storage Foundation archive (`.sfa`) format, or compress (.zip) format.

See "About deploying Veritas InfoScale Operations Manager add-ons" on page 109.

See "Downloading a Veritas InfoScale Operations Manager add-on" on page 110.

See "Uploading a Veritas InfoScale Operations Manager hot fix or package to the repository" on page 233.

See "Installing a Veritas InfoScale Operations Manager hot fix, package, or patch" on page 234.

About deploying base release packages

You can download and install the base release packages for Veritas InfoScale Operations Manager that are **VOM Deployable** in one of the following ways.

- Download from Veritas Services and 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 InfoScale Operations Manager add-ons" on page 109.

See "Downloading a Veritas InfoScale Operations Manager add-on" on page 110.

See "Uploading a Veritas InfoScale Operations Manager hot fix or package to the repository" on page 233.

See "Installing a Veritas InfoScale Operations Manager hot fix, package, or patch" on page 234.

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 InfoScale Operations Manager, Storage Foundation, and 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 InfoScale Operations Manager hot fix or package to the repository" on page 233.

See "Installing a Veritas InfoScale Operations Manager hot fix, package, or patch" on page 234.

Uploading a Veritas InfoScale 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 InfoScale 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.

4 Click **Upload** to upload to the repository.

5 Click **Close**.

See "Installing a Veritas InfoScale Operations Manager hot fix, package, or patch" on page 234.

See "Removing a Veritas InfoScale Operations Manager add-on from the repository" on page 115.

See "Uninstalling a Veritas InfoScale Operations Manager add-on" on page 114.

Installing a Veritas InfoScale Operations Manager hot fix, package, or patch

Using the Management Server console, you can install a Veritas InfoScale 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 InfoScale 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 234.
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 235.
7. In the **Result** panel, click **OK**

See "Uninstalling a Veritas InfoScale Operations Manager add-on" on page 114.

See "Removing a Veritas InfoScale Operations Manager add-on from the repository" on page 115.

See "Canceling deployment request for a Veritas InfoScale Operations Manager add-on" on page 116.

See "Viewing the details of an add-on, hot fix, package, or patch on SORT website" on page 256.

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 Veritas Download center
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 Veritas Download center
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 InfoScale Operations Manager hot fix, package, or patch" on page 234.

See "Upgrading managed host using the console" on page 74.

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 InfoScale 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 InfoScale Operations Manager hot fix, package, or patch" on page 234.

See "Upgrading managed host using the console" on page 74.

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 116.

See "Refreshing the repository" on page 121.

See "Installing a Veritas InfoScale Operations Manager add-on" on page 112.

See "Installing a Veritas InfoScale Operations Manager hot fix, package, or patch" on page 234.

See "Uninstalling a Veritas InfoScale Operations Manager add-on" on page 114.

Canceling deployment request for a hot fix, package, or patch

Using the Management Server console, you can cancel the deployment request for a Veritas InfoScale 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 117.

See "Installing a Veritas InfoScale Operations Manager add-on" on page 112.

See "Installing a Veritas InfoScale Operations Manager hot fix, package, or patch" on page 234.

See "Uninstalling a Veritas InfoScale Operations Manager add-on" on page 114.

Installing a Veritas InfoScale Operations Manager hot fix on a specific managed host

Using the Management Server console, you can install the Veritas InfoScale Operations Manager hot fix on the selected managed host. If the hot fix is already installed on the selected host, then Veritas InfoScale 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 InfoScale 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 118.

6. In the **Install - Result** panel, click **OK**.

See "About deploying Veritas InfoScale Operations Manager add-ons" on page 109.

Chapter 12

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
- Configuring two-factor authentication (2FA)
- 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
- Forwarding audit logs

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 242.
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 243.
Configuring proxy settings	You can download the information on the patch and the price tiers for Storage Foundation and High Availability products from the Veritas Services and 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 245.
Configuring two-factor authentication	You can enable or disable the two-factor authentication (2FA) to protect user accounts from getting compromised. A combination of user's login credentials and a six-digit PIN is used for two-factor authentication. The users are authenticated to access the Management Console only on successful validation of the combination of user's login credentials and the PIN. **Note:** Only the root level users or the administrators can enable or disable the two-factor authentication. See "Configuring two-factor authentication (2FA)" on page 246.

Table 12-1 Management Server settings *(continued)*

Task	Description
Analytics gathering settings	Veritas InfoScale Operations Manager provides statistical information such as the frequency of use of particular features or views of the Veritas InfoScale Operations Manager user interface in your organization to help analyze product usage. You can allow Veritas to analyze this data by enabling the analytics gathering feature on Management Server
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 246.
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 247.
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**.
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 248.
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 Management Server settings" on page 261.

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 239.

See "Viewing the Management Server settings" on page 261.

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 InfoScale 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 239.

See "Viewing the Management Server settings" on page 261.

Configuring SNMPv3 settings

Using the Management Server console in Veritas InfoScale Operations Manager, you can configure SNMPv3 settings.

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

Prerequisites for configuring SNMPv3 settings are as follows:

- Install Python 3.5.
- Install PySNMP.
  To install PySNMP through pip run the following command:
  ```
  pip install pysnmp
  ```
  To install PySNMP off-line, the following packages must be downloaded and installed for PySNMP to be operational:
  - PyASN1 - https://pypi.python.org/pypi/pyasn1
  - PySNMP - https://pypi.python.org/pypi/pysnmp/
  - PyCryptodomex - https://pypi.python.org/pypi/pycryptodomex/

To configure SNMPv3 settings for SNMP traps

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 **SNMPv3 settings** check the SNMPv3 checkbox.
4. Enter the **User Name**.
5. For authentication check the **Authentication** checkbox and do the following:
   - Select the **Authentication Protocol** from the drop-down.
   - Enter the **Authentication Password**.
6. For encryption check the **Privacy** Checkbox and do the following:
   - Select the **Privacy Protocol** from the drop-down.
   - Enter the **Privacy Password**.
7. Enter the path for python executable.
8. Click **Save Settings**.
9. To delete the settings click **Delete Settings**.

Table 12-2 SNMPv3 Settings

Input parameters	Security level applied		What it does
	Authentication	**Encryption**	
User Name	User Name	No	Uses a username match for authentication.
User Name, Authentication Protocol, Authentication Password	MD5 or SHA	No	Provides authentication based on MD5 or SHA algorithms.
User Name, Authentication Protocol, Authentication Password Privacy Protocol, Privacy Password	MD5 or SHA	AES/DES 56-bit encryption	Provides authentication based on the MD5 or SHA algorithms. In addition to authentication it also provides AES/DES 56-bit encryption.

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 239.

See "Viewing the Management Server settings" on page 261.

Configuring two-factor authentication (2FA)

You can enable or disable the two-factor authentication (2FA) to protect user accounts from getting compromised. A combination of user's login credentials and a six-digit PIN is used for two-factor authentication.

To enable or disable two-factor authentication

1. Log into Operations Manager with the administrator role.
2. On the Management Server console, click **Settings** > **Management Server**.
3. In the **Server settings** tab, configure the SMTP settings to receive email notifications or the OTP for resetting the six-digit PIN.
4. In the **Two factor authentication** pane, select the **Enable Two Factor Authentication** check box to enable it. Optionally clear the check box to disable the two-factor authentication.
5. Click **Save Settings**.

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 InfoScale 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 239.

See "Viewing the Management Server settings" on page 261.

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 InfoScale 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 239.

See "Viewing the Management Server settings" on page 261.

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 InfoScale Operations Manager 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 239.

See "Viewing the Management Server settings" on page 261.

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 239.

See "Viewing the Management Server settings" on page 261.

See "Viewing audit information for Management Server" on page 262.

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 InfoScale 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 239.

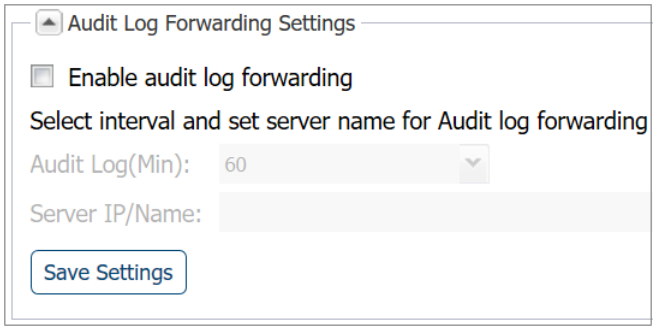
Forwarding audit logs

An audit log includes records of user actions on the CMS, like signing in, signing out, refreshing a host, creating volumes, and so on. This release introduces the Audit Log Forwarding feature, which lets you add the audit logs at specific intervals to the `/var/log/messages/syslog` file on the local server or on a remote server. You can enable or disable this scheduled activity from the **Settings** perspective of a VIOM Management Server. You can optionally specify the IP address or the name of a specific server where you want these logs to be forwarded.

Note: This feature is applicable to VIOM management servers on Linux only.

To access audit log forwarding settings

1. On the VIOM management console, open the **Settings** perspective.
2. Click **Management Server**; the **Server settings** tab appears by default.
3. Scroll down to locate the **Audit Log Forwarding Settings** section.



By default, audit log forwarding is disabled.

To enable audit log forwarding

1. Select the **Enable audit log forwarding** check box.
2. Use the **Audit Log(Min)** drop-down list to select the time intervals at which to forward the latest audit logs.

   At each scheduled interval, the audit logs that are collected since the last instance are added to `/var/log/messages/syslog`.
3. (Optional) To forward the audit logs to a different server, enter the appropriate server name or IP address in the **Server IP/Name** text box.

   Note: When you specify a server name or IP address, the `/etc/rsyslog.conf` file gets updated with the that value. The audit logs are then added to the `/var/log/messages/syslog` file on both, the CMS and the specified server.

4. Click **Save Settings**.

   An information message confirms that the change is saved.

To disable audit log forwarding

1. Deselect **Enable audit log forwarding**.
2. Click **Save Settings**.

   An information message confirms that the change is saved.

Chapter 13

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 InfoScale Operations Manager. This information about an object is in addition to the details that Veritas InfoScale 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 InfoScale 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 InfoScale Operations Manager User Guide*.

See "Viewing the list of extended attributes" on page 262.

See "Adding an extended attribute" on page 252.

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 InfoScale 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 "Modifying an extended attribute" on page 253.

See "Viewing the list of extended attributes" on page 262.

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 "Adding an extended attribute" on page 252.

See "Viewing the list of extended attributes" on page 262.

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 252.

See "Modifying an extended attribute" on page 253.

See "Viewing the list of extended attributes" on page 262.

Chapter 14

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 InfoScale Operations Manager add-on" on page 112.

See "Installing a Veritas InfoScale Operations Manager hot fix, package, or patch" on page 234.

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 160.

See "Removing managed hosts from the Management Server domain" on page 161.

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 InfoScale Operations Manager domain" on page 164.

See "Adding Lightweight Directory Access Protocol or Active Directory-based authentication on Management Server" on page 165.

See "Unconfiguring Lightweight Directory Access Protocol or Active Directory configuration from the authentication broker" on page 170.

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 201.

See "Suppressing faults in the Management Server perspective" on page 202.

See "Restoring a suppressed fault in the Management Server perspective" on page 203.

Viewing the faults definitions

You can view a comprehensive list of all the fault definitions that Veritas InfoScale 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 InfoScale 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 201.

See "Suppressing a fault definition in the Management Server perspective" on page 204.

See "Restoring a suppressed fault definition in the Management Server perspective" on page 205.

Viewing details of alert logs

Using the Management Server console, you can quickly ascertain the condition of all resources in the Veritas InfoScale 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 189.

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 "Editing rules in the Management Server perspective" on page 195.

See "Enabling rules in the Management Server perspective" on page 200.

See "Disabling rules in the Management Server perspective" on page 200.

See "Deleting rules in the Management Server perspective" on page 199.

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 239.

See "Viewing the Management Server settings" on page 261.

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 239.

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 "Adding an extended attribute" on page 252.

See "Modifying an extended attribute" on page 253.

See "Deleting an extended attribute" on page 253.

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 248.

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 246.

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 InfoScale 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.

Appendix A

Troubleshooting

This appendix includes the following topics:

- Management Server (MS)
- Managed host (MH)

Management Server (MS)

Veritas InfoScale 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`

Veritas InfoScale Operations Manager services running on Management Server for Windows

- Veritas InfoScale Operations Manager Authentication Service
- Veritas InfoScale Operations Manager Service
- Veritas Storage Foundation Messaging Service
- Veritas InfoScale Operations Manager Database Service
- Veritas InfoScale Operations Manager SNMP Trap Service

Commands to start and stop the Veritas InfoScale 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}
```

Commands to start and stop the Veritas InfoScale 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}
```

Management Server log file locations on Linux

- General: `/var/opt/VRTSsfmcs/logs`
- Database installation and upgrade logs:`/var/VRTSsfmcs/config_db`
- Installer log file:`/var/opt/VRTSsfmh/logs/install_sfm.log`
- DB engine log: `var/opt/VRTSsfmcs/db/data/SFMdb3.dblog`

Management Server log file locations on Windows

- General: `C:\ProgramData\Symantec\VRTSsfmcs\logs`
- General: `C:\ProgramData\Symantec\VRTSsfmh\logs`
- Database configuration and upgrade logs:`C:\ProgramData\Symantec\VRTSsfmcs\config_db`
- Installer log file: `C:\Program Files\Veritas\VRTSsfmcs\install.log`
- DB engine log: `C:\ProgramData\Symantec\VRTSsfmcs\logs\SFMdb3.dblog`

Managed host (MH)

Veritas InfoScale Operations Manager processes running on managed host on Unix/Linux

- `/opt/VRTSsfmh/bin/xprtld`
- `/opt/VRTSsfmh/bin/sfmh-discovery.pl`
- `/opt/VRTSsfmh/bin/vxdclid`

Veritas InfoScale 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.

Commands to start and stop Veritas InfoScale 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>`

Managed host log files

- UNIX/Linux: `/var/opt/VRTSsfmh/logs`
- Windows: `C:\ProgramData\Symantec\VRTSsfmh\logs`

Agentless driver log files

The agentless driver log files are stored at the Control Host at the following location:

- UNIX/Linux : `/var/opt/VRTSsfmh/`*`hostname`*`/log`
- Windows: C:\ProgramData\Symantec\VRTSsfmh\AGENTLESS*hostname*\log

where, *hostname* is the name of the agentless host.

Gathering information for troubleshooting

Use the `vomgather.pl` script to gather logs for troubleshooting issues on Veritas InfoScale 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 124
Active Directory removing 170
ActiveX 33
add-on
  canceling deployment request 116
  disabling 121
  downloading 110
  enabling 120
  installing 112
  removing 115
  uninstalling 114
adding
  virtualization server 221
advance authorization settings 248
agentless discovery
  about 128
  Commands that require the root access 141
  control hosts 135
  Linux 136
  prerequisites 136
  privilege control software for UNIX hosts 143
  remote hosts 135
  requirements for deep array discovery 140
  requirements for UNIX hosts 138
  requirements for Windows hosts 140
  SSH configuration requirements 144
  supported features 132
  UNIX 136
  Windows 137
alert log retention period 246
alerts and rules 189
array management capabilities 135
audit information 262
authentication broker
  managing 164
  viewing 257
authentication domains
  enabling 178
authentication domains *(continued)*
  managing 164
  viewing 257

B

backing up Veritas InfoScale Operations Manager
  on Linux 68–69
  on Windows 71–72
browsers 33

C

configuring
  Control Host 209
  existing Management Server in HA environment 90
  Management Server 43
  Management Server HA 82
  Management Server in HADR environment 98
  new Management Server installation in HA environment 82
Configuring Management Server settings
  advance authorization 248
  report scheduling 248
Control Host 135
  discover VMware Virtualization Infrastructure 209

D

deep array discovery 140
deploying
  add-ons 109
  hot fixes 230
  package 232
  packages or patches 231
  Veritas InfoScale Operations Manager 20
disable performance metering
  VMware vCenter server 228
disabling authentication domains 178
domains 33
downloading
  managed host files 17

downloading *(continued)*
Management Server files 17
Veritas InfoScale Operations Manager 16
DR
one-to-one 93
DR configuration
creating base service groups 96, 101
enabling configuration 98, 104
performing initial configuration 95, 100
prerequisites 94

E

enabling authentication domains 178
extended attribute
adding 252
deleting 253
modifying 253
using 251

F

fault definition
restoring 205
suppressing 204
faults
restoring 203
suppressing 202
viewing 258
faults and risks 201
fibre channel switch capabilities 135
firewalls ports
ports 33

G

gendeploy.pl 57

H

HA configuration 82
completing the configuration 89
creating base service groups 85
modify default IP address and host name 92
performing initial configuration 84
prerequisites for existing MS 91
prerequisites for new MS 83
HA-DR configuration
prerequisites 99
HADR configuration 98
host discovery 128
See also agentless discovery of hosts
host discovery *(continued)*
about 128
supported features 132
hot fix
cancel deployment request 237
deploying 230
install on specific host 238
installing 234
removing 236
uploading 233

I

installation resources 19
installing
host management through Solaris JumpStart 57
managed host 54
managed host on UNIX 55
managed host on Windows 56
Management Server 39
Management Server on Linux 40
Management Server on Windows 41
Intranet zone security level 33
IPV 36

J

JavaScript 33
JScript 33

L

LDAP
adding authentication 165
removing 170
LDom discovery
prerequisites 219
requirements 219

M

managed host
add using gendeploy.pl 157
installation files for UNIX 55
installation files for Windows 56
installing 54
installing on UNIX 55
installing on Windows 56
installing through Solaris JumpStart 57
package 39
removing 161
uninstalling on UNIX 79

managed host *(continued)*
uninstalling on Windows 80
upgrading 74
upgrading on UNIX 75
upgrading on Windows 76
verifying installation on UNIX 59
verifying installation on Windows 59
managed hosts
refresh host details 160
upgrade using console 74
verifying version using the console 78
Management Server
advance authorization settings 261
alert log retention period settings 246
analytics gathering 261
configuring 43
configuring a new installation in HA environment 82
configuring an existing installation in HA environment 90
configuring HA 82
configuring HADR 98
configuring proxy server 245
configuring settings 239
configuring SNMP trap 243
database retention policy 261
editing agentless hosts 159
installation files for Linux 40
installation files for Windows 41
installing 39
installing on Linux 40
installing on Windows 41
LDAP based authentication 165
package 39
proxy settings 261
remove managed host 161
report subscription settings 261
SMTP settings 261
SMTP settings for email 242
SNMP trap settings 261
task log retention period settings 246
uninstalling on Linux 78
uninstalling on Windows 79
upgrading 60
upgrading in HA DR environment 106
upgrading in HA environment 105
upgrading on Linux 61
upgrading on Windows 63
verifying installation on Linux 42
Management Server *(continued)*
verifying installation on Windows 43
verifying version using the console 77
Web server settings 247
web server settings 261

N

network requirements 33

O

OpenSSH
about 146
installing on AIX 146
installing on Linux 146
operating system requirements 23
organization 179

P

package
base release 232
cancel deployment request 237
deploying 232
installing 234
removing 236
uploading 233
packages or patches
deploying 231
maintenance release 231
patch
cancel deployment request 237
installing 234
removing 236
uploading 233
performance metering
disable for VMware vCenter server 228
permissions
assigning for perspective 181
deleting on perspective 183
modifying for perspective 182
perspective
assigning permissions 181
deleting permissions 183
modifying permissions 182
policy checks
enabling or disabling signatures for data center 249
exporting signatures 264
pop-up blockers 33

Proxy server requirements 36
proxy server settings 245

R

removing
    Active Directory 170
    LDAP 170
report scheduling 248
resolv.conf 33
restoring Veritas InfoScale Operations Manager
    on Linux 70
    on Windows 72
roles 179
rules
    about 189
    creating 191
    deleting 199
    disabling 200
    editing 195
    enabling 200

S

security level 33
signatures
    exporting 264
signatures for data center
    enabling or disabling 249
SNMP trap settings 243
Solaris JumpStart installation 57
solaris zones discovery
    prerequisites 217
    requirements 217
space estimation data logs 27
SSL 33
system resource requirements 25

T

task information for the data center 263
task log retention period 246
TCP 33
toolbars 33

U

UC 19
UDP 33
uninstalling
    add-on 114
    managed host on UNIX 79
uninstalling *(continued)*
    managed host on Windows 80
    Management Server on Linux 78
    Management Server on Windows 79
upgrading
    HA 104
    HA-DR 106
    managed host 74
    managed host on UNIX 75
    managed host on Windows 76
    managed host using installer package 76
    managed host using operating system commands 75
    managed hosts using console 74
    Management Server 60
    Management Server in HA DR environment 106
    Management Server in HA environment 105
    Management Server on Linux 61
    Management Server on Windows 63
upload
    add-on 111
user
    restricting 183
user group permissions
    assigning for perspective 181
    deleting on perspective 183
    modifying for perspective 182
    restricting 183
UTC 19

V

verifying
    managed host installation on UNIX 59
    managed host installation on Windows 59
    managed host version using the console 78
    Management Server installation on Linux 42
    Management Server installation on Windows 43
    Management Server version using the console 77
Veritas InfoScale Operations Manager
    about 15
    backing up on Linux 68–69
    backing up on Windows 71–72
    choosing managed hosts 22
    choosing Management Server hosts 21
    choosing Web console hosts 33
    configuring HA 82
    configuring HADR 98
    configuring Management Server 43
    deployment configuration 20

Veritas InfoScale Operations Manager *(continued)*
downloading 16
downloading managed host files 17
downloading Management ServeVeritas InfoScale Operations Managerr files 17
installation resources 19
installing managed host on UNIX 55
installing managed host on Windows 56
installing Management Server on Linux 40
installing Management Server on Windows 41
IPV requirements 36
network requirements 33
operating systems 23
organization 179
packages 39
proxy server requirements 36
restoring on Linux 70
restoring on Windows 72
supported hardware 33
system resource requirements 25
uninstalling UNIX managed host 79
upgrading managed host on UNIX 75
upgrading managed host on Windows 76
upgrading Management Server in HA DR environment 106
upgrading Management Server in HA environment 105
upgrading Management Server on Linux 61
upgrading Management Server on Windows 63
URL 16
Veritas InfoScale Operations Manager deployment
centralized management 20
Veritas InfoScale Operations Manager HA
configuring a new installation 82
configuring an existing installation 90
removing configuration 107
upgrading 104
Veritas InfoScale Operations Manager HA-DR
upgrading 106
viewing
alert log 259
authentication broker 257
authentication domains 257
extended attributes 262
virtual machines
cloning 58
migrating 58
virtualization discovery
editing configuration 224
virtualization discovery *(continued)*
refreshing configuration 226
refreshing ESX Server 226
removing configuration 227
virtualization server
adding 221
virtualization technology
kernel-based virtual machine 208
LPAR 208
Microsoft Hyper-V 208
Solaris LDom 208
Solaris zones 208
VMware 208
VMware discovery
near real-time update of virtual machine states 211
prerequisites 210
requirements 210
VRTSsfmcs package 39
VRTSsfmh package 39, 54–55, 75

W

Web browsers requirements 33
Web console 33
Web server
settings 247
web server
CLI command 122
restart 122
Web UI framework
starting and stopping 126