Veritas™ Operations Manager Management Server 5.0 Installation Guide

November 2012

Symantec™

Veritas™ Operations Manager Management Server Installation Guide

Product version: 5.0

Documentation version: 5.0 Rev 4

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

About Symantec Connect

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

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

Documentation

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

doc_feedback@symantec.com

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

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

Contents

Technical Support 4

Chapter 1 Planning your Veritas Operations Manager installation 11

About Veritas Operations Manager 11
About Management Server 12
About the managed host 12
About standalone (unmanaged) host 13
Downloading Veritas Operations Manager 5.0 13
Downloading Management Server files 14
Downloading managed host files 14
Using the product documentation 15
Host considerations for installing Veritas Operations Manager 16
Typical Veritas Operations Manager deployment configurations 16
Centralized management of Veritas Storage Foundation and High Availability hosts 17
Standalone management of Veritas Storage Foundation and High Availability hosts 18
Centralized and standalone management of Veritas Storage Foundation and High Availability hosts 18
Centralized management of hosts not having Storage Foundation and High Availability products 18
Veritas Operations Manager 5.0 installation overview 18
Choosing a Management Server host 19
Choosing managed hosts 20

Chapter 2 System requirements 21

Operating system requirements 21
Third-party required libraries 24
32-bit SNIA Common HBA API required on Windows hosts 24
System resource requirements 25
About space estimation for data logs 26
About the frequency of managed host information discovery 28
Supported hardware 30

Web browser requirements 31
Network and firewall requirements 31

Chapter 3 Installing, upgrading, and uninstalling Veritas Operations Manager 33

Packages included in Veritas Operations Manager 5.0 34
About installing Management Server 34
Installing Management Server on UNIX 35
Installing Management Server on Windows 36
Verifying Management Server installation on UNIX 37
Verifying Management Server installation on Windows 38
Configuring Veritas Operations Manager 5.0 on UNIX and Windows 38
Setting up the Web browser for Veritas Operations Manager 40
About installing host management 41
Installing host management on UNIX 42
Installing host management on Windows 43
About cloning virtual machines 44
About migrating virtual machines 44
Installing host management through Solaris JumpStart 45
Verifying host management installation on UNIX 46
Verifying host management installation on Windows 46
About installing or upgrading Veritas Operations Manager 5.0 add-ons 47
About upgrading Management Server 47
Upgrading Management Server on UNIX 48
Upgrading Management Server on Windows 49
Backing up data on UNIX 51
Backing up data on Windows 52
Restoring backed up data on UNIX 53
Restoring backed up data on Windows 54
About upgrading host management to Veritas Operations Manager 5.0 55
Upgrading managed hosts using the Veritas Operations Manager console 56
Upgrading host management on UNIX using operating system commands 57
Upgrading host management on Windows using the installer package 58
Verifying the version of Management Server in the console 59
Verifying the version of a managed host in the console 60
Uninstalling Management Server on UNIX 60

Uninstalling Management Server on Windows 61
Uninstalling host management on UNIX 61
Uninstalling host management on Windows 62

Chapter 4 Configuring Veritas Operations Manager in a high availability environment 65

About configuring Veritas Operations Manager in high availability environment 66
About configuring a new Veritas Operations Manager installation in high availability environment 66
Prerequisites for configuring Management Server installation in high availability environment 68
Retrieving the virtual host name and the virtual IP address of a host 68
Performing initial configuration of Management Server installation in high availability environment 69
Creating the base service groups in Veritas Cluster Server on UNIX 70
Creating the base service groups in Veritas Cluster Server on Windows 73
Completing the configuration of a Management Server installation in high availability environment 75
About configuring an existing Veritas Operations Manager installation in high availability environment 76
Modifying the default IP address and host name of the existing UNIX-based Management Server for high availability configuration 77
Modifying the default IP address and host name of the existing Windows-based Management Server for high availability configuration 79
About configuring Veritas Operations Manager in high availability and disaster recovery environment 81
Prerequisites for configuring Veritas Operations Manager in the high availability environment for disaster recovery 82
Performing initial configuration of Management Server installation in high availability and disaster recovery environment 83
Creating the base service groups in Veritas Cluster Server for HA-DR configuration 84
Enabling HA-DR configuration 88
Sample configuration: After you create the base service groups in Veritas Operations Manager 89

Sample configuration: After you configure Veritas Operations Manager in high availability environment 90
Sample configuration: After you configure Veritas Operations Manager in high availability environment for disaster recovery 94
About upgrading the high availability configurations 100
Upgrading Management Server in high availability environment 101
About upgrading the high availability and disaster recovery configurations 102
Upgrading Management Server in high availability and disaster recovery environment 102
Removing the high availability configuration 103

Index 105

Chapter 1

Planning your Veritas Operations Manager installation

This chapter includes the following topics:

- About Veritas Operations Manager
- Downloading Veritas Operations Manager 5.0
- Using the product documentation
- Host considerations for installing Veritas Operations Manager
- Typical Veritas Operations Manager deployment configurations
- Veritas Operations Manager 5.0 installation overview
- Choosing a Management Server host
- Choosing managed hosts

About Veritas Operations Manager

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

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

In Veritas Operations Manager, you can establish user credentials such that authorized users can access the product to perform sensitive management tasks, and other users can perform only a basic set of functions.

A typical Veritas Operations Manager deployment consists of the following:

- Management Server
  See "About Management Server" on page 12.
- Managed hosts
  See "About the managed host" on page 12.

For more information on managing security roles and users accounts, see the *Veritas Operations Manager Management Server Administrator's Guide*.

About Management Server

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.

When you install Management Server, the Web server component is installed automatically.

You can use the Web server on Management Server to access the managed hosts in the centrally managed deployment. You log on to the Management Server URL and Web server port 14161 (for example, `https://myhost.example.com:14161`).

See "About Veritas Operations Manager" on page 11.

About the managed host

A typical Veritas Operations Manager deployment consists of Management Server and at least one managed host.

Typically, a managed host is a production server on which you install and run Storage Foundation and High Availability product components. A typical site can have thousands of hosts using some or all of the Storage Foundation and High Availability products. You can also use Veritas Operations Manager to manage hosts on which Storage Foundation, or Storage Foundation and High Availability, are not installed.

In Veritas Operations Manager, Management Server is also configured as a managed host. You can manage Management Server itself as part of a central management domain.

In a centrally managed deployment, the managed hosts relay information about storage network resources and applications to Management Server. Management

Server merges the data it receives from the managed hosts within its database. Using this merged data, the Veritas Operations Manager console can present centralized views and reports.

See "About Veritas Operations Manager" on page 11.

About standalone (unmanaged) host

A standalone (unmanaged) host is a Storage Foundation host that has been configured so it does not belong to a central management domain.

To manage individual Storage Foundation hosts, you can install and use the Java-based Veritas Enterprise Administrator. This console lets you manage hosts using the Storage Foundation products installed on them.

If you want a standalone host to participate in the central management domain, you must update it by installing the Veritas Operations Manager host management package.

Note: You can convert any standalone host to a managed host. However, because Management Server is also a managed host, you cannot configure it to be a standalone host.

See "About Veritas Operations Manager" on page 11.

Downloading Veritas Operations Manager 5.0

Veritas Operations Manager is a free license add-on to Veritas Storage Foundation.

You can download Veritas Operations Manager 5.0 packages from the following URL:

http://go.symantec.com/vom

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

See "Downloading Management Server files" on page 14.

See "Downloading managed host files" on page 14.

Downloading Management Server files

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

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

- Linux:
  - Download file name - `Veritas_Operations_Manager_Management_Server_5.0.0_Linux.zip`
  - Installer file name - `Veritas_Operations_Manager_CMS_5.0_Linux.bin`
- Solaris:
  - Download file name - `Veritas_Operations_Manager_Management_Server_5.0.0_SolSparc.zip`
  - Installer file name - `Veritas_Operations_Manager_CMS_5.0_SolSparc.bin`
- Windows:
  - Download file name - `Veritas_Operations_Manager_Management_Server_5.0.0_Win.zip`
  - Installer file name - `Veritas_Operations_Manager_CMS_5.0_Win.exe`

See "About installing Management Server" on page 34.

See "About upgrading Management Server" on page 47.

Downloading managed host files

To install or upgrade host management, you need to download the `Veritas_Operations_Manager_Managed_Host_Bundle_5.0.0.zip` file that contains the packages for all the supported operating systems for managed hosts. You can unzip the file and install the package on the host.

Note: To upgrade a managed host to Veritas Operations Manager 5.0, you can choose to use the Deployment Management feature.

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

Table 1-1 provides 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 (*xxx* is the build number for the release)
AIX	VRTSsfmh_5.0.*xxx*.0_AIX.bff.Z
HP-UX	■ For HP-UX 11.23 and HP-UX 11.31: VRTSsfmh_5.0.*xxx*.0_HP-UX.tar.gz ■ For HP-UX 11.11 with Storage Foundation 3.5: VRTSsfmh_5.0.*xxx*.0_HP-UX_osr_B.11.11.tar.gz
Linux on x86 or Xeon	VRTSsfmh_5.0.*xxx*.0_Linux.rpm
Linux on PowerPC	VRTSsfmh_5.0.*xxx*.0_Linux_arch_ppc64.rpm
Solaris on SPARC	VRTSsfmh_5.0.*xxx*.0_SunOS_arch_sparc.pkg
Solaris on x86	VRTSsfmh_5.0.*xxx*.0_SunOS_arch_i386.pkg
Windows 32-bit	VRTSsfmh_5.00.*xxx*_Windows_arch_x86.msi
Windows 64-bit	VRTSsfmh_5.00.*xxx*_Windows_arch_x64.msi
Windows IA64	VRTSsfmh_5.00.*xxx*_Windows_arch_IA64.msi

See "About installing host management" on page 41.

See "About upgrading host management to Veritas Operations Manager 5.0" on page 55.

Using the product documentation

The following guides provide information about Veritas Operations Manager:

- *Veritas Operations Manager Management Server Administrator's Guide*
- *Veritas Operations Manager Management Server Getting Started Guide*
- *Veritas Operations Manager Management Server Installation Guide*

For complete host operating system and system resource specifications, as well as any known issues or software limitations in this release, see the *Veritas Operations Manager Release Notes*.

For information about the third-party software that is used in this product, see the *Veritas Operations Manager Management Server Third-Party License Agreements*.

The latest version of the product documentation is available on the SORT Web site at the following URL:

https://sort.symantec.com/documents

For the late breaking news that is related to this release, use the following TechNote:

http://www.symantec.com/docs/TECH189999

Host considerations for installing Veritas Operations Manager

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

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

See "About installing Management Server" on page 34.

See "About installing host management" on page 41.

Typical Veritas Operations Manager deployment configurations

You have several options for deploying Veritas Operations Manager.

If you implement centralized management, a typical full installation of Veritas Operations Manager consists of a single Management Server, multiple managed

hosts, and any number of Web consoles. We recommend this form of management because of the advantages you gain from being able to perform management operations on multiple hosts across the datacenter.

If you implement traditional, single-host management, you have the following options:

- Install a "thick" client, the Java-based VEA console.
- Install a light-weight Web server that relies on a standard Web browser client.

Only the Java console supports single-host management of both 5.*x* and 4.*x* hosts. Only 5.*x* hosts support the light-weight Web server.

Typical deployment scenarios include the following:

- Centralized management of Veritas Storage Foundation and High Availability hosts
  See "Centralized management of Veritas Storage Foundation and High Availability hosts" on page 17.
- Standalone management of Veritas Storage Foundation and High Availability hosts
  See "Standalone management of Veritas Storage Foundation and High Availability hosts" on page 18.
- Centralized and standalone management of Veritas Storage Foundation and High Availability hosts
  See "Centralized and standalone management of Veritas Storage Foundation and High Availability hosts" on page 18.
- Centralized management of hosts not having Storage Foundation and High Availability products
  See "Centralized management of hosts not having Storage Foundation and High Availability products" on page 18.

Centralized management of Veritas Storage Foundation and High Availability hosts

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

Advantages also include the following:

- Aggregated information for reporting
- Performance management across the datacenter

- Monitoring storage utilization across the datacenter
- Administration and analysis of all clusters in an enterprise

See "Typical Veritas Operations Manager deployment configurations" on page 16.

Standalone management of Veritas Storage Foundation and High Availability hosts

In this deployment scenario, you can use the Java-based Veritas Enterprise Administrator(VEA) console to perform traditional, single-host management for the Veritas Storage Foundation and High Availability hosts.

Unlike centralized management options, connections to multiple hosts are not concurrent and are independent of each other. In this scenario, you cannot easily aggregate information from multiple hosts across the datacenter .

See "Typical Veritas Operations Manager deployment configurations" on page 16.

Centralized and standalone management of Veritas Storage Foundation and High Availability hosts

In this deployment scenario, you centrally manage only your Veritas Storage Foundation and High Availability 5.*x*, or later, hosts on all supported platforms. You can manage your Storage Foundation 4.*x* hosts on UNIX individually using the Java-based Veritas Enterprise Administrator (VEA) console. Programmatically-aggregated information from multiple hosts is available in the Veritas Operations Manager console, from 5.x managed hosts only.

See "Typical Veritas Operations Manager deployment configurations" on page 16.

Centralized management of hosts not having Storage Foundation and High Availability products

In this deployment scenario, you centrally manage those hosts, which do not have Storage Foundation and High Availability products installed on them.

See "Typical Veritas Operations Manager deployment configurations" on page 16.

Veritas Operations Manager 5.0 installation overview

Installing Veritas Operations Manager involves the following:

- Reviewing the Veritas Operations Manager architecture and typical deployment configurations

See "Typical Veritas Operations Manager deployment configurations" on page 16.

- Verifying that you have met system requirements
  See "Operating system requirements" on page 21.
  See "System resource requirements" on page 25.
  See "Supported hardware" on page 30.
  See "Web browser requirements" on page 31.
  See "Network and firewall requirements" on page 31.
- Installing and configuring the Veritas Operations Manager Management Server
  See "About installing Management Server" on page 34.
  See "Configuring Veritas Operations Manager 5.0 on UNIX and Windows" on page 38.
- Installing Veritas Operations Manager host management on the hosts that will be centrally managed
  See "About installing host management" on page 41.

Choosing a Management Server host

Management Server is the central point for collecting and managing the information that managed hosts relay back to it.

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 21.
  See "32-bit SNIA Common HBA API required on Windows hosts" on page 24.
  See "System resource requirements" on page 25.
  See "Supported hardware" on page 30.
  See "Web browser requirements" on page 31.
  See "Network and firewall requirements" on page 31.
- The host should provide data security and space for a growing database as Management Server discovers new managed hosts and monitors network events. Ideally, the host should have RAID-protected storage and the capacity to grow its file systems.
- Clients that connect to Management Server using the Veritas Operations Manager console (Web browser) must be able to access the host.

Choosing managed hosts

A typical Veritas Operations Manager deployment consists of a Management Server and at least one managed host. The managed host has a Veritas Operations Manager agent that collects component-pertinent status information from network resources, such as hardware and applications, and relays that information to Management Server.

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

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

Note: Agentless discovery is not supported on hosts that have Storage Foundation or Veritas Storage Foundation and High Availability installed.

The types of managed hosts are as follows:

- Hosts with Storage Foundation 3.5 on HP-UX
- Hosts with Veritas Storage Foundation and High Availability 4.*x* on UNIX
- Hosts with Veritas Storage Foundation and High Availability 5.*x*, or later, on all supported platforms
- Hosts that do not have Storage Foundation, or Veritas Storage Foundation and High Availability installed on the supported platforms

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

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

See "Operating system requirements" on page 21.

Chapter 2

System requirements

This chapter includes the following topics:

- Operating system requirements
- Third-party required libraries
- System resource requirements
- Supported hardware
- Web browser requirements
- Network and firewall requirements

Operating system requirements

Table 2-1 provides an overview of Veritas Operations Manager operating system requirements for Management Server:

Table 2-1 Veritas Operations Manager operating system requirements for Management Server

Operating system supported	Notes
Red Hat Enterprise Linux 5.0 Red Hat Enterprise Linux 5.1 Update 1 Red Hat Enterprise Linux 5.2 Red Hat Enterprise Linux 5.3 Red Hat Enterprise Linux 5.4 Red Hat Enterprise Linux 5.5 Red Hat Enterprise Linux 5.6 Red Hat Enterprise Linux 5.7 Red Hat Enterprise Linux 5.8 Red Hat Enterprise Linux 6 Red Hat Enterprise Linux 6.1 Red Hat Enterprise Linux 6.2	x86 64-bit is the supported architecture. 32-bit `glibc` and `libgcc` packages must be installed. `Korn shell (KSH)` must be installed.
SUSE Linux Enterprise Server 9 SUSE Linux Enterprise Server 10 SUSE Linux Enterprise Server 11	x86 64-bit is the supported architecture.
Solaris 10	SPARC is the supported architecture. **Note:** Veritas Operations Manager 5.0 is the last major version of the product to support Solaris as a platform for Management Server. Symantec recommends that you deploy Veritas Operations Manager 5.0 Management Server on Linux or Windows to simplify the upgrade process to upcoming Veritas Operations Manager 6.*x* versions.
Windows 2003 Windows 2008 Windows 2008 R2	x86 64-bit is the supported architecture.

Table 2-2 provides an overview of Veritas Operations Manager operating system requirements for managed hosts:

Table 2-2 Veritas Operations Manager operating system requirements for managed hosts having Storage Foundation or Storage Foundation and High Availability products

Operating system supported	Notes
AIX 5.2 AIX 5.3 AIX 6.1 (only for hosts with Storage Foundation 5.0 MP3, or later) AIX 7.1 (only for Storage Foundation 5.1 SP1 PR1 hosts)	On AIX hosts, the xlC runtime environment must be version 8.0, or later. Use the `lslpp -lc | grep xlC.rte` command to verify the version of the xlC runtime environment.
HP-UX 11.11 (only for Storage Foundation 3.5 hosts)	PA RISC is the supported architecture.
HP-UX 11.23 HP-UX 11.31	
Red Hat Enterprise Linux 4.0 Red Hat Enterprise Linux 5.0 Update 2 (only for hosts with Storage Foundation 5.0 MP3, or later) Red Hat Enterprise Linux 6 Red Hat Enterprise Linux 6.1	On Red Hat Enterprise Linux 4.0, Storage Foundation 5.0 is supported on 64-bit Xeon, x86. 32-bit `glibc` and `libgcc` packages must be installed.
SUSE Linux Enterprise Server 9 SUSE Linux Enterprise Server 10 (only for hosts with Storage Foundation 5.0 MP3, or later) SUSE Linux Enterprise Server 11 (only for hosts with Storage Foundation 5.0 MP3, or later)	On SUSE Linux Enterprise Server 9, Storage Foundation 5.0 is supported on 64-bit Xeon, x86, and PowerPC; Storage Foundation 4.1 is supported on x86 and Xeon (32- and 64-bit).
Solaris 8 Solaris 9 Solaris 10 Solaris 11	
Windows Server 2003 Windows Server 2008 Windows 2008 R2	Supported on x86, x64, and IA64.

Veritas Operations Manager operating system requirements for the managed hosts that do not have Storage Foundation or Storage Foundation and High Availability products:

- AIX 5.2, or later
- HP-UX 11.23, or later
- Red Hat Enterprise Linux 4.*x*, or later
- SUSE Linux Enterprise Server 9, or later
- Solaris 9
- Solaris 10
- Solaris 11
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

For the most complete, up-to-date platform support documentation for Storage Foundation (UNIX) and Storage Foundation HA for Windows, visit the Symantec Technical Support website:

www.symantec.com/techsupp/

See "System resource requirements" on page 25.

Third-party required libraries

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

- 32-bit SNIA Common HBA API required on Windows hosts

32-bit SNIA Common HBA API required on Windows hosts

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

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

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

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

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

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

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

System resource requirements

The amount of memory and disk space that Veritas Operations Manager requires are listed in this section. The requirements are in addition to the resources that other software applications running on the host use.

For Management Server:

- CPU required: Dual processor for every 1000 managed hosts.
- Memory required:
  - 4GB for every 1000 managed hosts.
  - Add 4GB of memory if Management Server is used for the deep discovery of enclosures using the Storage Insight Add-on.
  - Add 4GB of memory if Management Server is used for the discovery of virtualization infrastructure.
- Disk space required: 15GB of disk space for every 1000 managed hosts.

For a managed host:

- CPU required: 1 <5%
- Virtual memory required: 1GB
- Disk space required: 2GB

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

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

- Disk space required: 15GB of disk space for agentless discovery of every 1000 managed hosts.

Read the following Symantec Technical Support TechNotes for the latest information on updates, patches, and software issues regarding this release:

http://www.symantec.com/docs/TECH189999

See "About the frequency of managed host information discovery" on page 28.

See "Operating system requirements" on page 21.

About space estimation for data logs

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

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

Table 2-3 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, DMP (path, controller, enclosure), volume, disk and file system are stored on the managed host. The data logs for VMware host, VxDMP (path, controller, enclosure) are stored on the Control Host. For storage array (port, controller, enclosure), data log for 1 day is stored on the discovery host, where as all the other logs are stored on Management Server.

Table 2-3 Space estimation for data logs

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, 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

Table 2-3 Space estimation for data logs *(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
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
VxVM 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
VxVM Disk	100	4	1 minute	6 hours	2348	23
	100	4	5 minutes	1 day	1898	19
	100	4	2 hours	1 month	2347	23
	100	4	1 day	1 year	2379	23
Storage array - Array port	32	2	30 minutes	1 day	304	9
	32	4	2 hours	1 month	751	23
	32	4	1 day	1 year	761	24

Table 2-3 Space estimation for data logs *(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
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

Note: If Veritas Operations Manager is configured in high availability environment, storage array port, controller, and enclosure logs are saved on a shared disk. If Control Host Add-on 5.0 is installed on Management Server, then, VMware ESX server and virtual machines logs are saved on a shared disk.

About the frequency of managed host information discovery

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

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

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

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

See "System resource requirements" on page 25.

Supported hardware

The following TechNotes contain the Hardware Compatibility List (HCL) for Veritas Operations Manager 5.0 and Storage Foundation products on UNIX:

- Storage Foundation 5.0 for UNIX:
  http://www.symantec.com/business/support/index?page=content&id=TECH47620
- Storage Foundation 5.1 for UNIX:
  http://www.symantec.com/business/support/index?page=content&id=TECH74012
- Storage Foundation 6.0 for UNIX:
  http://www.symantec.com/business/support/index?page=content&id=TECH170013

The following TechNotes contain the Hardware Compatibility List (HCL) for Veritas Operations Manager 5.0 and Storage Foundation products on Windows:

- Storage Foundation 5.0 for Windows:
  http://www.symantec.com/business/support/index?page=content&id=TECH50141
- Storage Foundation 5.1 for Windows:
  http://www.symantec.com/business/support/index?page=content&id=TECH59118
- Storage Foundation 6.0 for Windows:
  http://www.symantec.com/business/support/index?page=content&id=TECH152806

See "Operating system requirements" on page 21.

See "System resource requirements" on page 25.

Web browser requirements

The Veritas Operations Manager console is a graphical user interface that displays reports and other information for users of the Storage Foundation products through a standard Web browser.

The Web browsers that the Veritas Operations Manager console supports are:

- Internet Explorer versions 6.*x* to 9.*x*
- Firefox 3.*x*, or later

Additional considerations for supported Web browsers:

- Your browser must support JavaScript 1.2, or later.
- If you use pop-up blockers (including Yahoo Toolbar or Google Toolbar), either disable them or configure them to accept pop-ups from the Veritas Operations Manager Web server to which you connect.
- For Internet Explorer 6.0 on Windows 2003 (Server and Advanced Server), set the default intranet zone security level to Medium, or lower.
- For Internet Explorer, when popup-blocker is turned on, make sure that the filter level is set to Medium or lower.
- For Internet Explorer, ensure that the site is incuded in the list of trusted sites. If you cannot add the site to the list of trusted sites, enable the Binary and script Behaviors option in security settings.
- You must install Adobe Flash plug-in version 10, or later.

Use the following criteria to identify the kind of system you need to run the Web console:

- The Web console host must be able to access Veritas Operations Manager Management Server.
- Veritas Operations Manager must support the Web browser.

See "Operating system requirements" on page 21.

See "System resource requirements" on page 25.

Network and firewall requirements

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

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

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

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

Veritas Operations Manager uses the default ports as shown in Table 2-4 to transfer information.

Table 2-4 Default ports in a Veritas Operations Manager installation

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

See "Operating system requirements" on page 21.

See "System resource requirements" on page 25.

Chapter 3

Installing, upgrading, and uninstalling Veritas Operations Manager

This chapter includes the following topics:

- Packages included in Veritas Operations Manager 5.0
- About installing Management Server
- Verifying Management Server installation on UNIX
- Verifying Management Server installation on Windows
- Configuring Veritas Operations Manager 5.0 on UNIX and Windows
- Setting up the Web browser for Veritas Operations Manager
- About installing host management
- Installing host management through Solaris JumpStart
- Verifying host management installation on UNIX
- Verifying host management installation on Windows
- About installing or upgrading Veritas Operations Manager 5.0 add-ons
- About upgrading Management Server
- Backing up data on UNIX
- Backing up data on Windows
- Restoring backed up data on UNIX

- Restoring backed up data on Windows
- About upgrading host management to Veritas Operations Manager 5.0
- Verifying the version of Management Server in the console
- Verifying the version of a managed host in the console
- Uninstalling Management Server on UNIX
- Uninstalling Management Server on Windows
- Uninstalling host management on UNIX
- Uninstalling host management on Windows

Packages included in Veritas Operations Manager 5.0

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

Table 3-1 Software packages

Package name	Description
VRTSsfmcs	Veritas Operations Manager package that is required on Management Server
VRTSsfmh	Veritas Operations Manager package that is required on the managed host

See "Downloading Veritas Operations Manager 5.0" on page 13.

About installing Management Server

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

- A Linux host
- A Solaris host
- A Windows host

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

See "Operating system requirements" on page 21.

See "Choosing a Management Server host" on page 19.

See "Installing Management Server on UNIX" on page 35.

See "Installing Management Server on Windows" on page 36.

Installing Management Server on UNIX

You can install the Veritas Operations Manager Management Server on a Linux host or a Solaris host using a `.bin` file. The `.bin` file installs the `VRTSsfmcs` and the `VRTSsfmh` packages on the target host.

Note: On a Solaris host, you can install Management Server on both global and non-global zones.

To install Veritas Operations Manager Management Server on UNIX

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

   See "Operating system requirements" on page 21.

   See "Choosing a Management Server host" on page 19.

2. Download and unzip the installation file.

   See "Downloading Veritas Operations Manager 5.0" on page 13.

3. Open an operating system console.

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

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

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

   - On a Linux host:

     `./Veritas_Operations_Manager_CMS_5.0_Linux.bin`

   - On a Solaris host:

     `./Veritas_Operations_Manager_CMS_5.0_SolSparc.bin`

   If you see the error `Permission Denied`, change the permissions for the `.bin` file so that it can be run. Enter one of the following:

   - On a Linux host:

     `chmod +x Veritas_Operations_Manager_CMS_5.0_Linux.bin`

   - On a Solaris host:

     `chmod +x Veritas_Operations_Manager_CMS_5.0_SolSparc.bin`

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

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

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

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

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

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

8 Verify that the packages are installed and the processes are started.

See "Verifying Management Server installation on UNIX" on page 37.

9 Configure Veritas Operations Manager.

See "Configuring Veritas Operations Manager 5.0 on UNIX and Windows" on page 38.

Installing Management Server on Windows

You can install the Veritas Operations Manager Management Server on a Windows host using the `Veritas_Operations_Manager_CMS_5.0_Win.exe` file.

To install Veritas Operations Manager Management Server on Windows

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

See "Operating system requirements" on page 21.

See "Choosing a Management Server host" on page 19.

2 On the host where you plan to install Management Server, log on as a user with administrator privileges.

3 Download and unzip the installation file.

See "Downloading Veritas Operations Manager 5.0" on page 13.

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

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

6 To launch the installer, run the `Veritas_Operations_Manager_CMS_5.0_Win.exe` file.

7 To proceed with the Management Server installation, accept the End User License Agreement.

8 Click **Install** and follow through the installation process.

9 After the installation is complete, click **Finish**.

The Web browser is launched to configure Veritas Operations Manager.

10 Configure Veritas Operations Manager.

See "Configuring Veritas Operations Manager 5.0 on UNIX and Windows" on page 38.

11 Verify that Management Server is installed and the required services are started.

See "Verifying Management Server installation on Windows" on page 38.

Verifying Management Server installation on UNIX

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 UNIX

1 On the host where you installed Management Server, check whether the `VRTSsfmcs` package is installed. Enter one of the following:

- On a Linux host: **`rpm -q VRTSsfmcs`**
- On a Solaris host: **`pkginfo -l VRTSsfmcs`**

2 Check whether the `VRTSsfmh` package is installed. Enter one of the following:

- On a Linux host: **`rpm -q VRTSsfmh`**
- On a Solaris host: **`pkginfo -l VRTSsfmh`**

3 Check whether the `xprtld` process is started. Enter the following:

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

4 Check whether the `vxdclid` process is started. Enter the following:

```
ps -ef | grep vxdclid
```

See "Verifying the version of Management Server in the console" on page 59.

Verifying Management Server installation on Windows

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

To verify Management Server installation on Windows

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

See "Verifying the version of Management Server in the console" on page 59.

Configuring Veritas Operations Manager 5.0 on UNIX and Windows

If you are installing Management Server on a UNIX host, messages similar to the following are displayed after successful installation of Management Server:

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

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

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

Use the URL displayed in the message to configure Veritas Operations Manager.

Note: You can configure the Veritas Operations Manager in either IPv4 mode or in the mixed mode (IPv4 and IPv6). For mixed mode, Management Server need to be configured using only IPv4 address. Management Server configuration using IPv6 address is not supported.

If you are installing Management Server on a Windows host, the Web browser is automatically launched with the URL to configure Veritas Operations Manager. For Internet Explorer 7.0, or later, on Windows Server 2008, or Firefox 3.0, or later, if the Web page does not get displayed, you have to set up the Web browser.

See "Setting up the Web browser for Veritas Operations Manager" on page 40.

During the configuration, you are prompted to specify a location to store the Veritas Operations Manager database. You can accept the default location or specify your own.

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

To configure Veritas Operations Manager on UNIX and Windows

1. Do the following tasks to launch the Web browser. If you are configuring Veritas Operations Manager on a Windows host, skip this step.
   - On a host that has a network connection to the Management Server host, open a Web browser.
   - In the Web browser's address field, type the following URL and press **Enter**:
     https://*hostname*:5634/
     where *hostname* is the Management Server's host name, fully-qualified host name, or IP address. This is applicable for IPv4 mode. For dual mode (IPv4 and IPv6 mode) configuration, you can give only the host name. For example: **https://myhost.example.com:5634/**
     For the dual mode of Management Server, the IPv6 address and the hostname entries of the managed hosts should be present in Management Server's `/etc/hosts` file. 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 user name and password.
3. In the **Server Setting** page, check and modify the **Server Name**, if required.
4. Check and modify the **Server Address**, if required.
5. In the **Database Setting** page, check the default **Database location** and modify it, if required.

   The default database directory is `/var/opt/VRTSsfmcs/db` on UNIX, `%ALLUSERSPROFILE%\Application Data\Symantec\VRTSsfmcs\db` on Windows 2003, and `%ALLUSERSPROFILE%\Symantec\VRTSsfmcs\db` on Windows 2008/2008 R2.
6. Click **Next**.
7. In the **Analytics Setting** page, select **Enable Analytics Gathering** to allow Symantec to gather data on your Veritas Operations Manager usage.

8 Do one of the following:

- To change settings, click **Back**,
- To start the configuration, click **Finish**.

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

```
Configuration successful

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

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

See "Installing Management Server on UNIX" on page 35.

See "Installing Management Server on Windows" on page 36.

See "About configuring Veritas Operations Manager in high availability environment" on page 66.

Setting up the Web browser for Veritas Operations Manager

If you use Internet Explorer 7.0, or later, on Windows Server 2008, or Firefox 3.0, or later, the Web pages for configuring and launching Veritas Operations Manager are not displayed. You need to set up the Web browser to display the Web pages. For Internet Explorer 7.0, or later, on Windows Server 2008, if the Web pages are not automatically displayed, add each Web site to the **Trusted Sites** list. On Firefox 3.0, or later, if a security exception is displayed, add the exception to the Web browser to override how Firefox identifies the sites.

To set up Internet Explorer 7.0, or later, on Windows Server 2008 for Veritas Operations Manager

1 In Internet Explorer, select **Tools** > **Internet Options**.

2 Select the **Security** tab.

3 Click **Sites** to add the following Web sites:

- **https://*hostname*:5634/**—URL to configure Veritas Operations Manager
- **https://*hostname*:14161/**—URL to launch Veritas Operations Manager

where, *hostname* is the name of the Management Server host.

To set up Firefox 3.0, or later, for Veritas Operations Manager

1. On the security exception page that is displayed when you attempt to open an Veritas Operations Manager Web page, click the **Or you can add an exception** link.
2. Click **Add Exception**.

   For Firefox 3.6.*x*, or later, the users should first click the **I Understand the Risks** button before they click the **Add Exception** button.
3. In the **Add Security Exception** dialog, verify that the location is one of the following:

   - **https://*hostname*:5634/**—URL to configure Veritas Operations Manager
   - **https://*hostname*:14161/**—URL to launch Veritas Operations Manager

   where, *hostname* is the name of the Management Server host.
4. Click **Get Certificate**.
5. Select the **Permanently store this exception** check box.
6. Click **Confirm Security Exception**.

   The Web page is now displayed.

See "Configuring Veritas Operations Manager 5.0 on UNIX and Windows" on page 38.

About installing host management

You must install the `VRTSsfmh` package on a host so you can manage it using Veritas Operations Manager Management Server.

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 Veritas Operations Manager console, or the `gendeploy.pl` script.

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

See "Operating system requirements" on page 21.

See " Choosing managed hosts" on page 20.

See "About cloning virtual machines" on page 44.

See "About migrating virtual machines" on page 44.

Installing host management on UNIX

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

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

To install Veritas Operations Manager host management on a UNIX host

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

   See "Operating system requirements" on page 21.

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

   See "Downloading Veritas Operations Manager 5.0" on page 13.

3. Open an operating system console.
4. On the host where you plan to install host management, log on as root.
5. Change directory to the location where you unzipped the installation files bundle.

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

   See "Downloading managed host files" on page 14.

6. At the command prompt, enter one of the following commands to install the package:

   - For AIX, enter the following:
     `installp -ac -d VRTSsfmh_5.0.xxx.0_AIX.bff VRTSsfmh`
     where, ***xxx*** is the build number for the release.
   - For HP-UX, enter the following:
     `swinstall -s $PWD VRTSsfmh`
   - For Linux on x86 or Xeon, enter the following:
     `rpm -ivh VRTSsfmh_5.0.xxx.0_Linux.rpm`
     where, ***xxx*** is the build number for the release.
   - For Linux on PowerPC, enter the following:
     `rpm -ivh VRTSsfmh_5.0.xxx.0_Linux_arch_ppc64.rpm`
     where, ***xxx*** is the build number for the release.
   - For Solaris versions prior to version 11 on SPARC, enter the following:
     `pkgadd -d VRTSsfmh_5.0.xxx.0_SunOS_arch_sparc.pkg`

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

- For Solaris versions prior to version 11 on x86, enter the following:
  pkgadd -d VRTSsfmh_5.0.*xxx*.0_SunOS_arch_i386.pkg
  where, ***xxx*** is the build number for the release.
- For Solaris 11 on SPARC, enter the following:
  pkg install --accept -g VRTSsfmh_5.0.*xxx*.0_SunOS_arch_sparc.p5p VRTSsfmh
  where, ***xxx*** is the build number for the release.
- For Solaris 11 on x86, enter the following:
  pkg install --accept -g VRTSsfmh_5.0.*xxx*.0_SunOS_arch_i386.p5p VRTSsfmh
  where, ***xxx*** is the build number for the release.

7 Verify that the `VRTSsfmh` package is installed and the required processes have started.

See "Verifying host management installation on UNIX" on page 46.

See "About installing host management" on page 41.

Installing host management on Windows

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

To install Veritas Operations Manager host management on a Windows host

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

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

See "Operating system requirements" on page 21.

See " Choosing managed hosts" on page 20.

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

See "Downloading managed host files" on page 14.

4 From the directory to which you unzipped the installation files bundle, do one of the following:

- On a 32-bit host, run `VRTSsfmh_5.00.xxx_Windows_arch_x86.msi`
- On a 64-bit host, run `VRTSsfmh_5.00.xxx_Windows_arch_x64.msi`
- On a IA64 host, run `VRTSsfmh_5.00.xxx_Windows_arch_IA64.msi`

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

5 On the Welcome screen of the InstallShield Wizard, click **Next**.

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

7 Click **Finish** to exit the InstallShield Wizard.

8 Verify that the host management program is installed and the required service has started.

See "Verifying host management installation on Windows" on page 46.

See "About installing host management" on page 41.

About cloning virtual machines

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

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

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

See "About installing host management" on page 41.

About migrating virtual machines

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

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

On some virtualization technologies such as LPAR or LDOM, the MAC address of the host changes when it is migrated. You need to ensure that Veritas Operations Manager uses the same identifier for a managed host even when it is migrated.

For this purpose, you need to ensure that the host id of the virtual machine does not change after migration. In most of the virtualization technologies, host id of the virtual machine remains the same after migration.

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

See "About installing host management" on page 41.

Installing host management through Solaris JumpStart

You can install host management and add a 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. The script that is generated by `gendeploy.pl` can be included in the finalized stages of the Solaris JumpStart installation process.

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

- 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 the *Veritas Operations Manager Management Server Administrator's Guide* for more information on adding hosts to a Management Server domain.

Verifying host management installation on UNIX

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

To verify host management installation on UNIX

1. On the host where you installed host management, 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 HP-UX, enter the following:
     `swlist VRTSsfmh`
   - On Linux, enter the following:
     `rpm -q VRTSsfmh`
   - On Solaris, enter the following:
     `pkginfo -l VRTSsfmh`
2. Check whether the `xprtld` process is started. Enter the following:
   `ps -ef | grep xprtld`
3. Check whether the `vxdclid` process is started. Enter the following:
   `ps -ef | grep vxdclid`

See "Verifying the version of a managed host in the console" on page 60.

See "Installing host management on UNIX" on page 42.

Verifying host management installation on Windows

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

To verify host management installation on Windows

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

See "Verifying the version of a managed host in the console" on page 60.

See "Installing host management on Windows" on page 43.

About installing or upgrading Veritas Operations Manager 5.0 add-ons

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

Add-ons are installed on Management Server and are deployed from there on the managed hosts. Some add-ons are installed on Management Server during Management Server installation.

If you have upgraded to Veritas Operations Manager Management Server 5.0 from a previous version of Veritas Operations Manager, you may need to upgrade the add-ons. The previous version of the add-on may not be supported with Veritas Operations Manager 5.0.

For more information on the versions of the add-ons that are supported in Veritas Operations Manager 5.0, see the *Veritas Operations Manager Hardware and Software Compatibility List (HSCL)*.

You can download the latest available add-ons to Management Server from the following URL:

http://www.symantec.com/sfm_addons

For more information on deploying add-ons, see the *Veritas Operations Manager Management Server Administrator's Guide*.

About upgrading Management Server

To upgrade your existing Management Server installation to Veritas Operations Manager 5.0, you have to download and install the required packages. You can upgrade to Veritas Operations Manager 5.0 from version 3.1, or from version 4.*x*.

Note: To upgrade to Veritas Operations Manager 5.0 from version 2.*x* or from version 3.0, you need to first upgrade to version 3.1, or version 4.*x*. Then, you can upgrade to version 5.0.

You can upgrade Management Server on Linux, Solaris, and Windows hosts.

See "Downloading Veritas Operations Manager 5.0" on page 13.

See "Upgrading Management Server on UNIX" on page 48.

See "Upgrading Management Server on Windows" on page 49.

See "Backing up data on UNIX" on page 51.

See "Backing up data on Windows" on page 52.

Upgrading Management Server on UNIX

You can upgrade an existing Management Server on a Linux host or a Solaris host to Veritas Operations Manager 5.0 using a `.bin` file. When you run the `.bin` file, the installer first attempts to upgrade the Veritas Operations Manager database to a temporary location. If the database upgrade is successful, the remaining steps in the upgrade process are carried out. If the database upgrade fails, the previous version of Veritas Operations Manager is restored.

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

See "Backing up data on UNIX" on page 51.

To upgrade Management Server to Veritas Operations Manager 5.0 on UNIX

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 21.

   See "System resource requirements" on page 25.

2. Download and unzip the installation file.

   See "Downloading Veritas Operations Manager 5.0" on page 13.

3. Open an operating system console.
4. On the host where you plan to upgrade Management Server, log on as root.
5. Change directory to the location where you unzipped the `.bin` file.
6. At the command prompt, enter one of the following:

   - On a Linux host:

     `./Veritas_Operations_Manager_CMS_5.0_Linux.bin`

   - On a Solaris host:

     `./Veritas_Operations_Manager_CMS_5.0_SolSparc.bin`

   If you see the error `Permission Denied`, change the permissions for the `.bin` file so that it can be run. Enter one of the following:

   - On a Linux host:

```
chmod +x Veritas_Operations_Manager_CMS_5.0_Linux.bin
```

- On a Solaris host:

```
chmod +x Veritas_Operations_Manager_CMS_5.0_SolSparc.bin
```

7 To accept the End User License Agreement and proceed with the upgrade, 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.

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

```
Veritas Operations Manager is upgraded successfully.
```

10 To verify the upgrade, enter one of the following:

- On a Linux host:

```
rpm -q VRTSsfmcs
```

- On a Solaris host:

```
pkginfo -l VRTSsfmcs
```

Verify that the version for the `VRTSsfmcs` package is displayed as 5.0.

See "Verifying the version of a managed host in the console" on page 60.

See "Upgrading host management on UNIX using operating system commands" on page 57.

Upgrading Management Server on Windows

You can upgrade an existing Management Server on a Windows host to Veritas Operations Manager 5.0 using the `Veritas_Operations_Manager_CMS_5.0_Win.exe` file. When you run the `.exe` file, the installer first attempts to upgrade the Veritas Operations Manager database to a temporary location. If the database upgrade is successful, the remaining steps in the upgrade process are carried out. If the database upgrade fails, the previous version of Veritas Operations Manager is restored.

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

See "Backing up data on Windows" on page 52.

To upgrade Management Server to Veritas Operations Manager 5.0 on Windows

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

   See "Operating system requirements" on page 21.

   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 Operations Manager 5.0" on page 13.

4. Turn off the Windows firewall, or, open ports 5634 and 14161 for TCP/IP communication.
5. Ensure that there is no pending restart from Windows Update. If there is, restart the host before launching the installer.
6. To launch the installer, run the `Veritas_Operations_Manager_CMS_5.0_Win.exe` file.
7. In the message window that recommends that you back up data before the upgrade, do one of the following:

   - Click **Yes** to continue with the upgrade.
   - Click **No** to stop the upgrade. You can choose this option to stop the upgrade and back up data for the previous version of Veritas Operations Manager.
     See "Backing up data on Windows" on page 52.

8. To upgrade Management Server, click **Upgrade**.
9. If you do not have sufficient disk space in your current database directory to create the temporary files, you are prompted to provide the path for a temporary working area having enough disk space. Provide the complete path of a temporary working area.

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

   (2 * *DB size*) + (10% of *DB size*) + 150 MB

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

10. After the upgrade is complete, you will see the message **Upgrade Completed Successfully**.

11 Click **Finish** to close the installer.

12 To verify the upgrade, open the **Add or Remove Programs** panel.

13 To verify that the version has changed to 5.0, click the support information link under the **Veritas Operations Manager for Windows** program in the currently installed programs list.

See "Verifying the version of Management Server in the console" on page 59.

See "Upgrading host management on Windows using the installer package" on page 58.

Backing up data on UNIX

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

Before you upgrade Management Server, Symantec recommends that you back up the data. To take a backup of the existing configuration, you need to first extract a backup script, and then, run the backup script.

On UNIX, the backup script can back up an existing Management Server in high-availability configuration.

Note: The backup script does not back up the data that is related to the add-ons.

To back up Veritas Operations Manager data on UNIX

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

2 ■ In case of upgrade from versions prior to 4.*x*, do the following:
Use the `.bin` file that you downloaded for installing the version 5.0 Management Server to extract the backup script. You need to perform the extract step only once to obtain the backup script.

To extract the backup script, run the following command:

■ On Linux:

```
./Veritas_Operations_Manager_CMS_5.0_Linux.bin --x-backup
```

■ On Solaris:

```
./Veritas_Operations_Manager_CMS_5.0_SolSparc.bin --x-backup
```

The command extracts a Perl script named `vom_bkup.pl`.

- In case of upgrade from 4.*x*, you can access the `vom_bkup.pl` script from the following location:
  `/opt/VRTSsfmcs/config/adm/`

3 To take the backup, run the perl 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`.

The backup script can also be used to restore the backup. To restore the data using the backup script, the backup must be taken using the backup script for version 5.0.

See "Restoring backed up data on UNIX" on page 53.

See "Upgrading Management Server on UNIX" on page 48.

Backing up data on Windows

You can regularly back up the Veritas Operations Manager Management Server data to prevent data loss in the event of a failure. Veritas Operations Manager 5.0 provides a script that you can use to back up and restore data.

Before you upgrade Management Server, Symantec recommends that you back up the data.

On Windows, the backup script can back up an existing Management Server in high-availability configuration. However, you cannot use the backup script to restore the high-availability configuration. This feature is currently not supported.

Note: The backup script does not back up the data that is related to the add-ons.

To back up Veritas Operations Manager data on Windows

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

2 - In case of upgrade from versions lower than 4.1, do the following:
    - Download and unzip the installation file.
      See "Downloading Veritas Operations Manager 5.0" on page 13.
    - To launch the installer, run the `Veritas_Operations_Manager_CMS_5.0_Win.exe` file.

- In the message window that recommends that you back up data before the upgrade, click **No** to stop the upgrade.

You need to perform this step only when you are taking backup for the first time. You do not need to launch the installer again after you have extracted the `vom_bkup.pl` script.

- In case of upgrade from 4.1, you can access the `vom_bkup.pl` script from the following location:

  installdir`\VRTSsfmcs\config\adm`

3 To take the backup, run the following command at the command prompt:

`"`*installdir*`\VRTSsfmh\bin\perl" ./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`

The backup script can also be used to restore the backup. To restore the data using the backup script, the backup must be taken using the backup script for version 5.0.

See "Restoring backed up data on Windows" on page 54.

See "Upgrading Management Server on Windows" on page 49.

Restoring backed up data on UNIX

After you have backed up the Veritas Operations Manager data, you can use the `vom_bkup.pl` backup script to restore the data as and when required. You can also restore the data if the upgrade process fails after the packages are upgraded.

Note: You can restore a backup with the Veritas Operations Manager 5.0 backup script, only if the backup was taken using the same script. You cannot use the version 5.0 backup script to restore a backup that was taken using a script of an earlier version of Veritas Operations Manager.

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

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

To restore the Veritas Operations Manager data on UNIX

- Run the following command to restore the data:

  ```
  ./vom_bkup.pl --restore dir
  ```

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

See "Backing up data on UNIX" on page 51.

See "About installing Management Server" on page 34.

See "About installing or upgrading Veritas Operations Manager 5.0 add-ons" on page 47.

See "Configuring Veritas Operations Manager 5.0 on UNIX and Windows" on page 38.

Restoring backed up data on Windows

After you have backed up the Veritas Operations Manager data, you can use the `vom_bkup.pl` backup script to restore the data as and when required. You can also restore the data if the upgrade process fails after the packages are upgraded.

Note: You can restore a backup with the Veritas Operations Manager 5.0 backup script, only if the backup was taken using the same script. You cannot use the version 5.0 backup script to restore a backup that was taken using a script of an earlier version of Veritas Operations Manager.

Note: You cannot restore the data that you backed up on a Windows-based Management Server in high-availability environment. This feature is currently not supported. To restore the backed up data, contact Symantec Technical Support.

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

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

To restore the Veritas Operations Manager data on Windows

- 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.

See "Backing up data on Windows" on page 52.

See "About installing Management Server" on page 34.

See "About installing or upgrading Veritas Operations Manager 5.0 add-ons" on page 47.

See "Configuring Veritas Operations Manager 5.0 on UNIX and Windows" on page 38.

About upgrading host management to Veritas Operations Manager 5.0

You can upgrade managed hosts in your Management Server domain to Veritas Operations Manager 5.0 to make them compatible with the 5.0 Management Server. You can upgrade both the UNIX-based and the Windows-based managed hosts. You can upgrade to Veritas Operations Manager 5.0 from the following:

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

Note: You must upgrade Management Server to 5.0 before you upgrade the managed hosts in its domain to 5.0.

You can choose one of the following methods to upgrade a managed host to Veritas Operations Manager 5.0:

- Upgrade the managed host using the **Settings** > **Deployment** tab in the Veritas Operations Manager console.
  See "Upgrading managed hosts using the Veritas Operations Manager console" on page 56.
  For more information on deploying packages, see the *Veritas Operations Manager Management Server Administrator's Guide*.
- Upgrade the managed host using operating system commands.
  See "Upgrading host management on UNIX using operating system commands" on page 57.
  See "Upgrading host management on Windows using the installer package" on page 58.

Upgrading managed hosts using the Veritas Operations Manager console

You can upgrade multiple managed hosts using the Veritas Operations Manager 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.

For more information on uploading packages to the repository, see the *Veritas Operations Manager Management Server Administrator's Guide*.

To upgrade managed hosts using the Veritas Operations Manager console

1. In the Veritas Operations Manager console, click **Settings** > **Deployment.**
2. In the **Deployment Management** view, do one of the following:
   - Select the `VRTSsfmh` package, and click **Actions** > **Install**.
   - Right-click on the `VRTSsfmh` package. From the submenu, select **Install**.

3 In the **Install Solution** 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.

4 Click **Install.**

5 Verify the managed host version in the console.

See "Verifying the version of a managed host in the console" on page 60.

Upgrading host management on UNIX using operating system commands

You can upgrade an existing managed host on UNIX to Veritas Operations Manager 5.0 by upgrading the `VRTSsfmh` package on it.

To upgrade managed host to Veritas Operations Manager 5.0 on UNIX

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

See "Operating system requirements" on page 21.

See "System resource requirements" on page 25.

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

See "Downloading Veritas Operations Manager 5.0" on page 13.

3 Open an operating system console.

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

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

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

See "Downloading managed host files" on page 14.

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_5.0.`*`xxx`*`.0_AIX.bff VRTSsfmh`

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

- For HP-UX, enter the following:
  `swinstall -s $PWD VRTSsfmh`
- For Linux on x86 or Xeon, enter the following:
  `rpm -U VRTSsfmh_5.0.xxx.0_Linux.rpm`
  where, *xxx* is the build number for the release.
- For Linux on PowerPC, enter the following:
  `rpm -U VRTSsfmh_5.0.xxx.0_Linux_arch_ppc64.rpm`
  where, *xxx* is the build number for the release.
- For Solaris versions earlier than version 11 on SPARC, enter the following:
  `pkgadd -d VRTSsfmh_5.0.xxx.0_SunOS_arch_sparc.pkg -a /opt/VRTSsfmh/etc/VRTSsfmhadmin VRTSsfmh`
  where, *xxx* is the build number for the release.
- For Solaris versions earlier than version 11 on x86, enter the following:
  `pkgadd -d VRTSsfmh_5.0.xxx.0_SunOS_arch_i386.pkg -a /opt/VRTSsfmh/etc/VRTSsfmhadmin VRTSsfmh`
  where, *xxx* is the build number for the release.
- For Solaris 11, enter the following:
  `pkg update --accept -g VRTSsfmh.p5p package path  VRTSsfmh`

8 To verify that the package has been upgraded and the version has changed to 5.0, enter one of the following at the command prompt:

- On AIX, enter the following:
  `lslpp -l VRTSsfmh`
- On HP-UX, enter the following:
  `swlist VRTSsfmh`
- On Linux, enter the following:
  `rpm -q VRTSsfmh`
- On Solaris, enter the following:
  `pkginfo -l VRTSsfmh`

See "Verifying the version of a managed host in the console" on page 60.

Upgrading host management on Windows using the installer package

You can upgrade an existing managed host on Windows to Veritas Operations Manager 5.0 by upgrading the `.msi` package on it.

To upgrade managed host to Veritas Operations Manager 5.0 on Windows

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

   See "Downloading Veritas Operations Manager 5.0" on page 13.
3. From the directory to which you unzipped the installation files bundle, do one of the following:
   - On a 32-bit host, run `VRTSsfmh_5.00.xxx_Windows_arch_x86.msi`
   - On a 64-bit host, run `VRTSsfmh_5.00.xxx_Windows_arch_x64.msi`
   - On a IA64 host, run `VRTSsfmh_5.00.xxx_Windows_arch_IA64.msi`

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

   See "Downloading managed host files" on page 14.
4. On the Welcome screen of the InstallShield Wizard, click **Next**.
5. On the Ready to Install the Program screen, click **Install** to start the upgrade.
6. Click **Finish** to exit the InstallShield Wizard.
7. To verify the upgrade, open the **Add or Remove Programs** panel.
8. To verify that the version has changed to 5.0, click the support information link under the **Veritas Operations Manager for Windows (Host Component)** program in the currently installed programs list.

See "Verifying the version of a managed host in the console" on page 60.

Verifying the version of Management Server in the console

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

To verify the version of Management Server in the console

1. In the header, at the top of the Veritas Operations Manager console, click **About**.

   The Management Server version is displayed.
2. To close the window, click **OK**.

See "Verifying Management Server installation on UNIX" on page 37.

See "Verifying Management Server installation on Windows" on page 38.

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 Veritas Operations Manager console.

To verify the version of a managed host in the console

1. In the Veritas Operations Manager console, click **Settings** > **Host**.
2. In the **Host** view that is displayed, verify the managed host version in the **MH Version** column.

See "Verifying host management installation on UNIX" on page 46.

See "Verifying host management installation on Windows" on page 46.

Uninstalling Management Server on UNIX

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

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

To uninstall Veritas Operations Manager Management Server on UNIX

1. Open an operating system console.
2. On the Management Server host, log on as root.
3. To remove the `VRTSsfmcs` package, enter one of the following:
   - On a Linux host: **`rpm -e VRTSsfmcs`**
   - On a Solaris host: **`pkgrm VRTSsfmcs`**
4. To remove the `VRTSsfmh` package, enter one of the following:
   - On a Linux host: **`rpm -e VRTSsfmh`**
   - On a Solaris host: **`pkgrm VRTSsfmh`**

See "About installing Management Server" on page 34.

Uninstalling Management Server on Windows

You can uninstall Veritas Operations Manager Management Server from a Windows host. When you uninstall Management Server, all data on managed hosts is also removed. If you reinstall Management Server on the host, you have to add the hosts again to the Management Server domain.

To uninstall Veritas Operations Manager Management Server on Windows

1. Log on to the target host as a user with administrator privileges.
2. On the Windows Control Panel, click **Add or Remove Programs**.
3. From the list of installed programs, select **Veritas Operations Manager for Windows**.
4. Click **Remove**.
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 34.

Uninstalling host management on UNIX

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

Note: Before you uninstall the host, remove it from the Management Server domain. In the Veritas Operations Manager console, select **Settings** > **Host**. Select a host and right-click on it to display the shortcut menu. From the shortcut menu, select **Remove Host(s)**.

To uninstall Veritas Operations Manager host management on UNIX

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

See "About installing host management" on page 41.

Uninstalling host management on Windows

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

Note: Before you uninstall the host, remove it from the Management Server domain. In the Veritas Operations Manager console, select **Settings** > **Host**. Select a host and right-click on it to display the shortcut menu. From the shortcut menu, select **Remove Host(s)**.

To uninstall Veritas Operations Manager host management on Windows

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

See "About installing host management" on page 41.

Chapter 4

Configuring Veritas Operations Manager in a high availability environment

This chapter includes the following topics:

- About configuring Veritas Operations Manager in high availability environment
- About configuring a new Veritas Operations Manager installation in high availability environment
- About configuring an existing Veritas Operations Manager installation in high availability environment
- About configuring Veritas Operations Manager in high availability and disaster recovery environment
- Sample configuration: After you create the base service groups in Veritas Operations Manager
- Sample configuration: After you configure Veritas Operations Manager in high availability environment
- Sample configuration: After you configure Veritas Operations Manager in high availability environment for disaster recovery
- About upgrading the high availability configurations
- About upgrading the high availability and disaster recovery configurations

- Removing the high availability configuration

About configuring Veritas Operations Manager in high availability environment

Configuring Veritas Operations Manager in high availability environment enhances the efficiency of Veritas Operations Manager as an operational tool for storage administrators. This configuration improves the availability of the applications and the services that Veritas Operations Manager provides.

Note: You can configure Veritas Operations Manager in high availability environment only in the failover mode.

For the Veritas Operations Manager HA configuration, you must use a two-node VCS cluster in which Storage Foundation HA 5.*x*, or later, is installed. Before you configure Veritas Operations Manager in high availability environment, you must ensure that Node1 that you configure as Management Server and Node2 that you add as managed host to Node1 are part of the same domain.

After you configure Veritas Operations Manager in high availability environment, you can enable the disaster recovery feature on the Veritas Operations Manager-HA setup.

See "About configuring a new Veritas Operations Manager installation in high availability environment" on page 66.

See "About configuring an existing Veritas Operations Manager installation in high availability environment" on page 76.

See "About configuring Veritas Operations Manager in high availability and disaster recovery environment" on page 81.

See "Removing the high availability configuration" on page 103.

See "About upgrading the high availability configurations" on page 100.

See "About upgrading the high availability and disaster recovery configurations" on page 102.

About configuring a new Veritas Operations Manager installation in high availability environment

In Veritas Operations Manager, you can configure both UNIX and Windows Management Servers in the high availability environment. You can configure

Windows Management Server with versions Windows 2008 (64-bit) and Windows 2008 R2 in the high availability environment.

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

Note: To avoid losing the data, do not use this method to configure high availability environment on an existing Management Server.

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

To configure a new Veritas Operations Manager 5.0 installation in high availability environment

1. Ensure the prerequisites for configuring a new Management Server installation in high availability environment

   See "Prerequisites for configuring Management Server installation in high availability environment" on page 68.

2. Retrieve the virtual host name and the virtual IP address of a host

   See "Retrieving the virtual host name and the virtual IP address of a host" on page 68.

3. Perform initial configuration of Management Server installation in high availability environment

   See "Performing initial configuration of Management Server installation in high availability environment" on page 69.

4. Create the base service groups in VCS to ensure failover

   See "Creating the base service groups in Veritas Cluster Server on UNIX" on page 70.

   See "Creating the base service groups in Veritas Cluster Server on Windows" on page 73.

5. Complete the configuration of a Management Server installation in high availability environment

   See "Completing the configuration of a Management Server installation in high availability environment" on page 75.

See "About configuring an existing Veritas Operations Manager installation in high availability environment" on page 76.

See "About configuring Veritas Operations Manager in high availability and disaster recovery environment" on page 81.

Prerequisites for configuring Management Server installation in high availability environment

Following are some prerequisites for configuring a Veritas Operations Manager 5.0 installation in high availability environment:

- Installing Storage Foundation HA 5.*x*, or later, on Node1 and Node2 as part of preparing Management Server for high availability configuration. Both node 1 and node 2 should be in the same cluster.
- Creating a Volume Manager Cluster Dynamic disk group and a volume for the data.

See "About configuring a new Veritas Operations Manager installation in high availability environment" on page 66.

See "About configuring an existing Veritas Operations Manager installation in high availability environment" on page 76.

Retrieving the virtual host name and the virtual IP address of a host

You need to retrieve the virtual host name and the virtual IP address on Node1 before you configure the Management Server in high availability environment.

To retrieve the virtual host name and the virtual IP address on Node1

- To retrieve the virtual host name and the virtual IP address on Node1 on which you have installed VCS cluster with Veritas Storage Foundation and High Availability 5.*x*, or later, run the following command:
  - For the node on Linux:

    ```
    ifconfig eth0:0 My_host_1's virtual IP Address netmask subnet mask up
    ```

  - For the node on Solaris:

    ```
    ifconfig hme0:1 plumb
    ifconfig hme0:1 My_host_1's virtual IP Address netmask subnet mask up
    ```

  Where, My_host_1 is the host name of Node1.

Note: for Veritas Storage Foundation and High Availability for Windows (SFW HA), Symantec recommends that you use a Lanman resource to associate the virtual IP address with the virtual server name. For more information on Lanman resource, see the *Veritas Cluster Server Bundled Agents Reference Guide*.

See "About configuring a new Veritas Operations Manager installation in high availability environment" on page 66.

See "About configuring an existing Veritas Operations Manager installation in high availability environment" on page 76.

Performing initial configuration of Management Server installation in high availability environment

You need to configure Management Server on Node1 and then add Node2 as a managed host to the configured Management Server that is configured on Node 1.

To configure Management Server on Node1

1 You need to configure Node1 as Management Server in standalone mode.

- To configure a new Management Server installation in high availability environment, 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.
- To configure an existing Management Server installation in high availability environment, 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 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. For Veritas Storage Foundation and High Availability for Window setup, enter the virtual IP address that is used in the SFM_Services_IP resource.

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.

When you modify the default database path, do not enter the clustered disk group path that you have created for the SFM_SStore_DG resource.

4 In the Analytics Setting page, select **Enable Analytics Gathering** to allow Symantec to gather data on your Veritas Operations Manager usage. Click **Finish**.

5 In the next panel, view the status of the tasks that are performed. Click **Launch Web Console** to log on to Management Server on Node1.

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

- Use the Veritas Operations Manager Web console to add Node2 as a managed host to the configured Management Server on Node1. Make sure that the storage objects that are associated with Node2 are accessible after you add it as a managed host.

See "About configuring a new Veritas Operations Manager installation in high availability environment" on page 66.

See "About configuring an existing Veritas Operations Manager installation in high availability environment" on page 76.

Creating the base service groups in Veritas Cluster Server on UNIX

To ensure the failover, you need to create the base service groups in Veritas Cluster Server and link those base service groups and resource types.

To create the base service groups in Veritas Cluster Server to ensure failover

1 In the Veritas Operations Manager console, select **Manage > Clusters**. Select any one cluster, and click **Actions > Create Service Group**.

2 If the selected cluster is in read only mode, the **Open Configuration** wizard appears. In the **Open Configuration** wizard, click **Next**.

3 In the **Create Service Group** panel, provide service group **Name** as **SFM_SStore**. Select the **Type** as **Failover**.

4 In the **Configure SystemList** panel, select Node1 and Node2 from the Available Systems list, and move them to the Systems in Priority Order list. Click **Finish**.

5 Repeat steps 1 to 4 again to create the **SFM_Services** service group.

6 Select **Manage > Service Groups**. You can see both the service groups listed there.

7 Select the **SFM_SStore** service group and click **Actions Edit > Resources > Add/Modify Resources**.

8 In the **Configure Resources** panel, enter the **Name** of the resource. Select **Type** and click **Add**.

9 After the resource is added to the **Resource List**, select the **Enabled** and **Critical** check boxes in the table. Select **Edit**.

10 In **Edit Attributes** panel, enter values of attributes.

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

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

11 Repeat steps 7 to 10 for the **SFM_Services** service group.

12 For the resources that you can create on the SFM_Services service group for a UNIX 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 to be monitored. For example, if you use eth0:1 device for virtual IP, then use eth0 as device name.
SFM_Services_NIC	NIC	**Device**: Name of the NIC to be monitored. For example, if you use eth0:1 device for virtual IP, then use eth0 as device name. The procedure in this topic uses the following: ■ eth0 as NIC for Linux Management Server. ■ bge0/hme0 as NIC for Solaris Management Server.

Resource name	Resource type	Attributes
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 that is specified for failover. In Veritas Operations Manager, you can specify only Veritas File System (VxFS). ■ **FsckOpt**: File check option (fsckpt = -n or -y).

To link the base service groups and resource types

1. Select **Manage > Service Groups**. Select the **SFM_Services** service group. Click **Actions > Edit > Link**.
2. In the **Link Service Group** panel, **SFM_Services** is displayed as **Parent Group**. Select **SFM_SStore** as **Child Group**. Select the following:

Relationship	Online Local
Dependency Type	Hard

3. Click **Finish**.
4. In the Service Groups view, click on the **SFM_Services** service group.
5. Click **Resources** tab. From the **Resource Associations** table, select **SFM_Service_IP** resource.
6. Select the **Actions > Link/Unlink Resources**.
7. In **Resource Dependencies** panel, link the resources as follows:
   - Set **Select Parent** as **SFM_Services_IP**.
   - Set **Select Child** as **SFM_Services_NIC**.
   - Click **Link**.
   - Verify the dependency in the **Dependencies** table.
8. Click **Finish**.

See "Creating the base service groups in Veritas Cluster Server on Windows" on page 73.

See "About configuring a new Veritas Operations Manager installation in high availability environment" on page 66.

See "About configuring an existing Veritas Operations Manager installation in high availability environment" on page 76.

Creating the base service groups in Veritas Cluster Server on Windows

To ensure the failover, you need to create the base service groups in Veritas Cluster Server and link those base service groups and resource types.

To create the base service groups in Veritas Cluster Server to ensure failover

1. In the Veritas Operations Manager console, select **Manage > Clusters**. Select any one cluster, and click on **Actions > Create Service Group**.
2. If the selected cluster is in read only mode, the **Open Configuration** wizard appears. In the **Open Configuration** wizard, click **Next**.
3. In the **Create Service Group** panel, provide service group **Name** as **SFM_SStore**. Select the **Type** as **Failover**.
4. In the **Configure SystemList** panel, select Node1 and Node2 from the Available Systems list, and move them to the Systems in Priority Order list. Click **Finish**.
5. Repeat steps 1 to 4 again to create the **SFM_Services** service group.
6. Select **Manage > Service Groups**. You can see both the service groups listed there.
7. Select the **SFM_SStore** service group and click **Actions Edit > Resources > Add/Modify Resources**.
8. In the **Configure Resources** panel, enter the **Name** of the resource. Select **Type** and click **Add**.
9. In **Edit Attributes** panel, enter values of attributes.

   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	Disk group that is specified for the failover. **Note:** You must create a clustered disk group.

10 After the resource is added to the **Resource List**, select the **Enabled** and **Critical** check boxes in the table. Select **Edit**.

11 Repeat steps 7 to 10 for the **SFM_Services** service group.

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

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

To link the base service groups and resource types

1 Select **Manage > Service Groups**. Select the **SFM_Services** service group. Click **Actions > Edit > Link**.

2 In the **Link Service Group** panel, **SFM_Services** is displayed as **Parent Group**. Select **SFM_SStore** as **Child Group**. Select the following:

Relationship	Online Local
Dependency Type	Hard

3 Click **Finish**.

4 In the Service Groups view, click on the **SFM_Services** service group.

5 Click **Resources** tab. From the **Resource Associations** table, select **SFM_Service_IP** resource.

6 Select the **Actions > Link/Unlink Resources**.

7 In **Resource Dependencies** panel, link the resources as follows::

- Set **Select Parent** as **SFM_Services_IP**.
- Set **Select Child** as **SFM_Services_NIC**.
- Click **Link**.
- Verify the dependencies in the **Dependencies** table.

8 Click **Finish**.

See "Creating the base service groups in Veritas Cluster Server on UNIX" on page 70.

See "About configuring a new Veritas Operations Manager installation in high availability environment" on page 66.

See "About configuring an existing Veritas Operations Manager installation in high availability environment" on page 76.

Completing the configuration of a Management Server installation in high availability environment

After you create the base service groups and link the base service groups with the resource types, you need to perform certain steps to complete the configuration in high availability environment.

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

1 Open a Web browser, and launch the following URL:

https://My_virtual-host:5634

where, My_virtual-host is the virtual host name of Node1.

You must ensure that you have appropriate privileges to log on to this host.

2 In the panel that displays the message **Click Next to configure CS as a Cluster Node**, click **Next**.

3 In the next panel, which displays the steps that you must do to configure Management Server as a cluster node, click **Start**.

4 In the panel, that displays the steps that you must do to configure Management Server in high availability environment, click **Next**.

5 In the panel, that displays the details of the service group for the HA configuration for your review, click **Next**.

6 View the status of the tasks that are performed as part of Veritas Operations Manager HA configuration and do one of the following:

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

See "About configuring a new Veritas Operations Manager installation in high availability environment" on page 66.

See "About configuring an existing Veritas Operations Manager installation in high availability environment" on page 76.

About configuring an existing Veritas Operations Manager installation in high availability environment

In Veritas Operations Manager, you can configure the existing UNIX or Windows Management Servers in the high availability environment.

Note: Before you configure an existing Veritas Operations Manager installation in high availability environment, you must install Veritas Cluster Server cluster with Storage Foundation HA 5.*x*, or later, on the hosts that you want to designate as Node1 and Node2.

Following is an overview of the steps that are involved in the process of configuring an exisitng Veritas Operations Manager 5.0 installation in high availability environment:

To configure an existing Veritas Operations Manager 5.0 installation in high availability environment

1. Ensure the prerequisites for configuring a new Management Server installation in high availability environment

   See "Prerequisites for configuring Management Server installation in high availability environment" on page 68.

2. Modify the virtual host name and the virtual IP address of Management server

   See "Modifying the default IP address and host name of the existing UNIX-based Management Server for high availability configuration" on page 77.

   See "Modifying the default IP address and host name of the existing Windows-based Management Server for high availability configuration" on page 79.

3. Perform initial configuration of Management Server installation in high availability environment

   See "Performing initial configuration of Management Server installation in high availability environment" on page 69.

4. Create the base service groups in VCS to ensure failover

   See "Creating the base service groups in Veritas Cluster Server on Windows" on page 73.

5. Complete the configuration of a Management Server installation in high availability environment

   See "Completing the configuration of a Management Server installation in high availability environment" on page 75.

See "About configuring a new Veritas Operations Manager installation in high availability environment" on page 66.

See "About configuring Veritas Operations Manager in high availability and disaster recovery environment" on page 81.

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

Before you start the configuration of an existing UNIX-based Management Server in high availability, you need to perform following operations:

- Modify the default IP address and host name of the existing Windows-based Management Server.

- Change all occurrences of the host name and the IP address of Node1 to virtual host name and virtual IP address in the files on the system.

Following host names are used in the examples of the procedure:

Host name of Node1	My_host_1
Host name of Node2	My_host_2
Virtual host name	My_virtual_host
Virtual host IP	My_virtual_host_IP

To modify the default host name and the IP address of Node1 (for UNIX Management Server)

1. To change the original host name of Node1 (My_host_1) to virtual host name (My_virtual_host), run the `hostname virtual_hostname` command. For example, use `hostname My_virtual_host`
2. To bring up the virtual host name and the virtual IP address on Node1 on which you have installed Veritas Cluster Server cluster with Veritas Storage Foundation and High Availability, run the following command:
   - For the node on Linux:
     ```
     ifconfig eth0:0 My_virtual_host_IP netmask subnet mask up
     ```
   - For the node on Solaris:
     ```
     ifconfig hme0:1 plumb
     ifconfig hme0:1 My_virtual_host_IP netmask subnet mask up
     ```

To modify the default host names and the IP addresses in the files

1. Change the host name and the IP address of Node1 to virtual host name and virtual IP address in the files on your system.
2. Stop all the VCS processes on Node1 and Node2. Run the following command on each host.

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

3 On Node 1, you need to change all occurrences of the original host names (My_host_1) to the virtual host names (My_virtual_host) in the files. Modify the required entries in the following files from the locations that are mentioned against each of them:

`llttab`	`/etc/llttab`
`llthosts`	`/etc/llthosts`
`sysname`	`/etc/VRTSvcs/conf/sysname`
`main.cf`	`/etc/VRTSvcs/conf/config/main.cf`

4 On Node2, you need to change all occurrences of Node1 host names to the virtual host name in the files. Modify the required entries in the following files from the locations that are mentioned against each of them:

`llthosts`	`/etc/llthosts`
`main.cf`	`/etc/VRTSvcs/conf/config/main.cf`

5 Start all the VCS processes on Node1 and Node2. Run the following command on each host.

```
/opt/VRTSvcs/bin/hastart
```

6 Restart Node1, run the following command:

```
service network restart
```

7 Log on to Node1 using the virtual host name (My_virtual_host).

See "Modifying the default IP address and host name of the existing Windows-based Management Server for high availability configuration" on page 79.

See "About configuring an existing Veritas Operations Manager installation in high availability environment" on page 76.

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

Before you start the configuration of an existing Windows-based Management Server in high availability, you need to perform following operations:

- Modify the default IP address and host name of the existing Windows-based Management Server.

- Change all occurrences of the host name and the IP address of Node1 to virtual host name and virtual IP address in the files on the system.

To modify the default host names and the IP addresses in the files

1. Stop all the VCS processes on Node1 and Node2. Do the following steps on each host:
   - Select **Start > Run**. In the **Run** dialog box, type `services.msc`.
   - In the **Services** window, stop the Veritas high availability engine service.
2. On Node 1, you need to change all occurrences of the original host names to the virtual host names in the files. Modify the required entries in the following files from the locations that are mentioned against each of them:

`llttab.txt`	C:\Program Files\Veritas\comms\llt\
`llthosts.txt`	C:\Program Files\Veritas\comms\llt\
`sysname`	C:\Program Files\Veritas\cluster server\conf
`main.cf`	C:\Program Files\Veritas\cluster server\conf\config\

3. On Node2, you need to change all occurrences of Node1 host names to the virtual host name in the files. Modify the required entries in the following files from the locations that are mentioned against each of them:

`llthosts.txt`	C:\Program Files\Veritas\comms\llt\
`main.cf`	C:\Program Files\Veritas\cluster server\conf\config\

4. On Windows Management Server, modify the required entries in the following files from the locations that are mentioned against each of them:

`llthosts.txt`	C:\Program Files\Veritas\comms\llt\
`main.cf`	C:\Program Files\Veritas\cluster server\conf\config\

5. Start all the VCS processes on Node1 and Node2. Do the following on each host.:
   - Select **Start > Run**. In the **Run** dialog box, type `services.msc`.

- In the **Services** window, start the Veritas high availability engine service.

You must perform this task on both Node1 and Node2.

6 Restart Node1.

7 Log on to Node1 using the virtual host name.

See "Modifying the default IP address and host name of the existing UNIX-based Management Server for high availability configuration" on page 77.

See "About configuring an existing Veritas Operations Manager installation in high availability environment" on page 76.

About configuring Veritas Operations Manager in high availability and disaster recovery environment

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

In configuring Veritas Operations Manager in high availability environment for disaster recovery, typically you configure a Veritas Operations Manager HA setup in a remote site along with the Veritas Operations Manager HA setup in your local site and make them act as two nodes. You can also configure a Veritas Operations Manager HA setup with single node Veritas Cluster Server (VCS) clusters.

This topic considers the local Veritas Operations Manager-HA setup as Site A and the remote Veritas Operations Manager- HA setup as Site B.

To configure Veritas Operations Manager 5.0 installation in high availability and disaster recovery environment

1 Ensure the prerequisites for configuring Veritas Operations Manager 5.0 in high availability and disaster recovery environment

See "Prerequisites for configuring Veritas Operations Manager in the high availability environment for disaster recovery" on page 82.

2 Retrieve the virtual host name and the virtual IP address of a host

See "Retrieving the virtual host name and the virtual IP address of a host" on page 68.

3 Perform initial configuration of Management Server installation in high availability and disaster recovery environment

See "Performing initial configuration of Management Server installation in high availability and disaster recovery environment" on page 83.

4 Create the base service groups in VCS for HA-DR configuration

See "Creating the base service groups in Veritas Cluster Server for HA-DR configuration" on page 84.

5 Enable Veritas Operations Manager HA-DR configuration

See "Enabling HA-DR configuration" on page 88.

Prerequisites for configuring Veritas Operations Manager in the high availability environment for disaster recovery

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

- Storage Foundation HA 5.*x*, or later, and VCS cluster are installed on the hosts that you want to designate as Node1 and Node2 in Site A and Node3 and Node4 in Site B. Also, Node1 in Site A and Node3 in Site B are considered as primary nodes.

  For single node HA-DR configuration, you need to designate Node1 in Site A and Node2 in Site B. There are no secondary nodes in case of a single node HA-DR configuration
- Global Cluster Option (GCO) is enabled in VCS in Site A and Site B. For more information on enabling GCO, see *Veritas™ Cluster Server Administrator's Guide*.
- Veritas Volume Replicator (VVR) is configured in Site A and Site B. For more information on configuring VVR, see *Veritas™ Cluster Server Agents for Veritas™ Volume Replicator Configuration Guide*.
- All the nodes on which you want to configure Veritas Operations Manager in the high availability environment must report synchronized Universal Time Clock (UTC/UC) time.
- You must specify the database location. You can either use the default database location `/var/opt/VTRSsfmcs/db` or specify another location. If you specify the location other than the default database location, you must make sure that it is not part of the shared file system that is used for failover. Later, the Veritas Operations Manager HA 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, SFM_Services_IP, and SFM_SStore_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.

See "About configuring Veritas Operations Manager in high availability and disaster recovery environment" on page 81.

See "About configuring a new Veritas Operations Manager installation in high availability environment" on page 66.

See "About configuring an existing Veritas Operations Manager installation in high availability environment" on page 76.

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

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

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

1. Install Management Server on the nodes Node1 and Node2 in Site A and Node3 and Node4 in Site B.

   In case of a single node HA-DR configuration, install Management Server on Node1 in Site A and Node2 in Site B.

2. Before configuring On Node1, configure Management Server in high availability environment using the virtual host and virtual IP.

   Add Node2 in Site A and Node3 and Node4 in Site B as managed hosts to Management Server. In case of a single node HA-DR configuration, add Node2 in Site B as a managed host.

   See "Performing initial configuration of Management Server installation in high availability environment" on page 69.

3. Add the virtual host name and the virtual IP addresses of Node1 in the `/etc/hosts` file of Node3. Similarly, add the virtual host name and the virtual IP addresses of Node3 in the `/etc/hosts` file of Node1.

   In case of a single node HA-DR configuration, add the virtual host name and the virtual IP addresses of Node1 in the `/etc/hosts` file of Node2. Similarly, add the virtual host name and the virtual IP addresses of Node2 in the `/etc/hosts` file of Node1.

Note: Adding entries to `/etc/hosts` is not a recommended procedure. Use VCS DNS resource to update the host name and IP mapping.

See "About configuring Veritas Operations Manager in high availability and disaster recovery environment" on page 81.

Creating the base service groups in Veritas Cluster Server for HA-DR configuration

To ensure the failover, you need to create the base service groups in Veritas Cluster Server and link those base service groups and resource types for HA-DR configuration.

To create the base service groups in Veritas Cluster Server to ensure failover

1. In the Veritas Operations Manager console, select **Manage > Clusters**. Select any one cluster, and click on **Actions > Create Service Group**.

2. If the selected cluster is in read only mode, the **Open Configuration** wizard appears. In the **Open Configuration** wizard, click **Next**.

3 In the **Create Service Group** panel, provide service group **Name** as **SFM_SStore**. Select the **Type** as **Failover**.

4 In the **Configure SystemList** panel, select Node1 and Node2 from the Available Systems list, and move them to the Systems in Priority Order list. Click **Finish**.

5 Repeat steps 1 to 4 again to create the **SFM_Services** service group.

6 Select **Manage > Service Groups**. You can see both the service groups listed there.

7 Select the **SFM_SStore** service group and click **Actions Edit > Resources > Add/Modify Resources**.

8 In the **Configure Resources** panel, enter the **Name** of the resource. Select **Type** and click **Add**.

9 After the resource is added to the **Resource List**, select the **Enabled** and **Critical** checkboxes in the table. Select **Edit**.

10 In **Edit Attributes** panel, enter values of attributes.

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

Resource name	Resource type	Attributes
SFM_SStore_DG	Disk group	Disk group that is specified for the failover.
SFM_SStore_IP	IP	Virtual IP, which is used to configure Node1 in Site A.
SFM_SStore_NIC	NIC	Resource that is created on an interface on which original IP address and virtual IP address are configured. **Device**: Name of the NIC to be monitored. For example, if you use eth0:1 device for virtual IP, then use eth0 as device name. The procedure in this topic uses the following: ■ eth0 as NIC for Linux Management Server. ■ bge0/hme0 as NIC for Solaris Management Server.

Resource name	Resource type	Attributes
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.

11 Repeat steps 7 to 10 for the **SFM_Services** service group.

12 For the resources that you can create on the SFM_Services service group for a UNIX 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 to be monitored. For example, if you use eth0:1 device for virtual IP, then use eth0 as device name.
SFM_Services_NIC	NIC	**Device**: Name of the NIC to be monitored. For example, if you use eth0:1 device for virtual IP, then use eth0 as device name. The procedure in this topic uses the following: ■ eth0 as NIC for Linux Management Server. ■ bge0/hme0 as NIC for Solaris Management Server.
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 that is specified for failover. In Veritas Operations Manager, you can specify only Veritas File System (VxFS). ■ **FsckOpt**: File check option (fsckpt = -n or -y).
SFM_Services_RVGPrimary	RVG Primary	Contains the RVG resource name that is to be used for replication.

To link the base service groups and resource types

1. Select **Manage > Service Groups**. Select the **SFM_Services** service group. Click **Actions > Edit > Link**.
2. In the **Link Service Group** panel, **SFM_Services** is displayed as **Parent Group**. Select **SFM_SStore** as **Child Group**. Select the following:

Relationship	Online Local
Dependency Type	Hard

3. Click **Finish**.
4. In the Service Groups view, click on the **SFM_Services** service group.
5. Click **Resources** tab. From the **Resource Associations** table, select **SFM_Service_IP** resource.
6. Select the **Actions > Link/Unlink Resources**.
7. In **Resource Dependencies** panel, link the resources as follows:
   - Set **Select Parent** as **SFM_Services_IP**.
   - Set **Select Child** as **SFM_Services_NIC**.
   - Click **Link**.
   - Verify the dependency in the **Dependencies** table.
8. Repeat steps 5 to 7 for other resources. For selecting parent and child dependencies, refer to the following table:

Parent	Child
SFM_SStore_RVG	SFM_SStore_DG
SFM_SStore_RVG	SFM_SStore_IP
SFM_SStore_IP	SFM_SStore_NIC
SFM_Services_Mount	SFM_Services_RVGPrimary

9. Click **Finish**.

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_IP, SFM_SStore_NIC, SFM_SStore_Diskgroup are online and rest of the resources are offline. Also, you must configure SFM_Services service group as Global.

For performing these tasks related to the service groups and resources, you need to have Veritas Operations Manager Add-on for Veritas Cluster Server Administration enabled on the Management Server. For more information, see *Veritas Operations Manager Management Server Add-ons User's Guide*.

See "About configuring Veritas Operations Manager in high availability and disaster recovery environment" on page 81.

Enabling HA-DR configuration

To enable Veritas Operations Manager HA-DR configuration for two node configuration

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

```
/opt/VRTSsfmh/bin/xprtlc  \

                  -u vxss://Virtual hostname of Site A:14545/sfm_admin/sfm_domain/vx\
                  -d debug=1 \
                  -d setup=1 \
                  -d mh=site B Node_1,site B Node_2 \
                  -l https://Virtual hostname of Site A:5634/admin/cgi-bin/cs_hadr_config.pl
```

To enable Veritas Operations Manager HA-DR configuration for single node configuration

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

```
/opt/VRTSsfmh/bin/xprtlc  \
                  -u vxss://Virtual hostname of Site A:14545/sfm_admin/sfm_domain/vx\
                  -d debug=1 \
                  -d setup=1 \
                  -d mh=site B Node_1\
                  -l https://Virtual hostname of Site A:5634/admin/cgi-bin/cs_hadr_config.pl
```

See "About configuring Veritas Operations Manager in high availability and disaster recovery environment" on page 81.

Sample configuration: After you create the base service groups in Veritas Operations Manager

The following is an example of Veritas Operations Manager configuration after you create the base service groups (SFM_Services and SFM_SStore):

Note: The following example uses the names London for Node1 and Paris for Node2.

```
group SFM_SStore (
        SystemList = { London = 0, Paris = 1 }
        AutoStartList = { London, Paris }
        )

        DiskGroup SFM_SStore_DG (
                DiskGroup = hadg
                )

        // resource dependency tree
        //
        //      group SFM_SStore
        //      {
        //      DiskGroup SFM_SStore_DG
        //      }


group SFM_Services (
        SystemList = { London = 0, Paris = 1 }
        AutoStartList = { London, Paris }
        )

        IP SFM_Services_IP (
                Device @London = eth0
                Device @Paris = eth0
                Address = "IP_Address"
                NetMask = "Netmask"
                )

        Mount SFM_Services_MOUNT (
                MountPoint = "/hafs"
                BlockDevice = "/dev/vx/dsk/hadg/havol"
                FSType = vxfs
```

```
        FsckOpt = "-n"
        )

NIC SFM_Services_NIC (
        Device @London = eth0
        Device @Paris = eth0
        )


requires group SFM_SStore online local hard
SFM_Services_IP requires SFM_Services_NIC


// resource dependency tree
//
//      group SFM_Services
//      {
//      IP SFM_Services_IP
//          {
//          NIC SFM_Services_NIC
//          }
//      Mount SFM_Services_MOUNT
//          {
//      }
```

See "About configuring a new Veritas Operations Manager installation in high availability environment" on page 66.

See "About configuring Veritas Operations Manager in high availability and disaster recovery environment" on page 81.

See "Sample configuration: After you configure Veritas Operations Manager in high availability environment" on page 90.

Sample configuration: After you configure Veritas Operations Manager in high availability environment

The following is an example of Veritas Operations Manager configuration after you configure it in high availability environment:

Note: The following example uses the names London for Node1 and Paris for Node2.

```
group SFM_SStore (
        SystemList = { London = 0, Paris = 1 }
        AutoStartList = { London, Paris }
        )

        DiskGroup SFM_SStore_DG (
                DiskGroup = hadg
                )



        // resource dependency tree
        //
        //      group SFM_SStore
        //      {
        //      DiskGroup SFM_SStore_DG
        //      }


group SFM_Services (
        SystemList = { London = 0, Paris = 1 }
        AutoStartList = { London, Paris }
        )

        Application SFM_Services_DB (
                User = root
                StartProgram = "/opt/VRTSsfmcs/config/vcs/db/online"
                StopProgram = "/opt/VRTSsfmcs/config/vcs/db/offline"
                MonitorProgram = "/opt/VRTSsfmcs/config/vcs/db/monitor"
                )

        Application SFM_Services_SECD (
                User = root
                StartProgram = "/opt/VRTSsfmcs/config/vcs/secd/online.sh"
                StopProgram = "/opt/VRTSsfmcs/config/vcs/secd/offline.sh"
                CleanProgram = "/opt/VRTSsfmcs/config/vcs/secd/clean.sh"
                MonitorProgram = "/opt/VRTSsfmcs/config/vcs/secd/monitor.sh"
                )

        Application SFM_Services_WEB (
                User = root
                StartProgram = "/opt/VRTSsfmcs/config/vcs/gui/online.sh"
                StopProgram = "/opt/VRTSsfmcs/config/vcs/gui/offline.sh"
```

```
        CleanProgram = "/opt/VRTSsfmcs/config/vcs/gui/clean.sh"
        MonitorProgram = "/opt/VRTSsfmcs/config/vcs/gui/monitor.sh"
        )

Application SFM_Services_XPRTLDD (
        User = root
        StartProgram = "/opt/VRTSsfmcs/config/vcs/xprtld_domain/online.sh"
        StopProgram = "/opt/VRTSsfmcs/config/vcs/xprtld_domain/offline.sh"
        MonitorProgram = "/opt/VRTSsfmcs/config/vcs/xprtld_domain/monitor.sh"
        )

IP SFM_Services_IP (
        Device @London = eth0
        Device @Paris = eth0
        Address = "IP_Address"
        NetMask = "Netmask"
        )

Mount SFM_Services_MOUNT (
        MountPoint = "/hafs"
        BlockDevice = "/dev/vx/dsk/hadg/havol"
        FSType = vxfs
        FsckOpt = "-n"
        )

NIC SFM_Services_NIC (
        Device @London = eth0
        Device @Paris = eth0
        )


requires group SFM_SStore online local hard
SFM_Services_DB requires SFM_Services_IP
SFM_Services_DB requires SFM_Services_MOUNT
SFM_Services_SECD requires SFM_Services_DB
SFM_Services_WEB requires SFM_Services_SECD
SFM_Services_XPRTLDD requires SFM_Services_DB
SFM_Services_IP requires SFM_Services_NIC


// resource dependency tree
//
//      group SFM_Services
```

```
        //      {
        //      Application SFM_Services_WEB
        //          {
        //          Application SFM_Services_SECD
        //              {
        //              Application SFM_Services_DB
        //                  {
        //                  IP SFM_Services_IP
        //                      {
        //                      NIC SFM_Services_NIC
        //                      }
        //                  Mount SFM_Services_MOUNT
        //                  }
        //              }
        //          }
        //      Application SFM_Services_XPRTLDD
        //          {
        //          Application SFM_Services_DB
        //              {
        //              IP SFM_Services_IP
        //                  {
        //                  NIC SFM_Services_NIC
        //                  }
        //              Mount SFM_Services_MOUNT
        //              }
        //          }
        //      }


group SFM_Xprtld (
        SystemList = { London = 0, Paris = 1 }
        Parallel = 1
        AutoStartList = { London, Paris }
        )

        Application SFM_Services_XPRTLDS (
                User = root
                StartProgram = "/opt/VRTSsfmcs/config/vcs/xprtld_standalone/online.sh"
                StopProgram = "/opt/VRTSsfmcs/config/vcs/xprtld_standalone/offline.sh"
                MonitorProgram = "/opt/VRTSsfmcs/config/vcs/xprtld_standalone/monitor.sh"
                )

        // resource dependency tree
```

```
        //
        //      group SFM_Xprtld
        //      {
        //      Application SFM_Services_XPRTLDS
        //      }
```

See "About configuring a new Veritas Operations Manager installation in high availability environment" on page 66.

See "About configuring Veritas Operations Manager in high availability and disaster recovery environment" on page 81.

See "Sample configuration: After you create the base service groups in Veritas Operations Manager " on page 89.

Sample configuration: After you configure Veritas Operations Manager in high availability environment for disaster recovery

The following is an example of Veritas Operations Manager configuration after you configure it in high availability environment for disaster recovery:

```
include "types.cf"
include "VVRTypes.cf"

cluster USA_gco_cluster (
        UserNames = { admin = IppJ }
        ClusterAddress = "IP_Address"
        Administrators = { admin }
        HacliUserLevel = COMMANDROOT
        )

cluster India_gco_cluster (
        ClusterAddress = "IP_Address"
        )

heartbeat Icmp (
        ClusterList = { rhel5_cmsha }
        Arguments @rhel5_cmsha = { "IP_Address" }
        )

system Chicago (
        )
```

```
system Washington (
        )

group ClusterService (
        SystemList = { Chicago = 0, Washington = 1 }
        AutoStartList = { Chicago, Washington }
        OnlineRetryLimit = 3
        OnlineRetryInterval = 120
        )

        Application wac (
                StartProgram = "/opt/VRTSvcs/bin/wacstart"
                StopProgram = "/opt/VRTSvcs/bin/wacstop"
                MonitorProcesses = { "/opt/VRTSvcs/bin/wac" }
                RestartLimit = 3
                )

        IP gcoip (
                Device @Chicago = eth0
                Device @Washington = eth2
                Address = "IP_Address"
                NetMask = "Netmask"
                )

        NIC csgnic (
                Device @Chicago = eth0
                Device @Washington = eth2
                )

        gcoip requires csgnic
        wac requires gcoip


        // resource dependency tree
        //
        //      group ClusterService
        //      {
        //      Application wac
        //          {
        //          IP gcoip
        //              {
        //              NIC csgnic
```

```
        //              }
        //          }
        //      }


group SFM_SStore (
        SystemList = { Washington = 0, Chicago = 1 }
        AutoStartList = { Washington }
        )

        DiskGroup SFM_SStore_DG (
                Critical = 0
                DiskGroup = hadg
                )

        IP SFM_SStore_IP (
                Critical = 0
                Device @Washington = eth2
                Device @Chicago = eth0
                Address = "IP_Address"
                )

        Proxy SFM_SStore_PROXY (
                TargetResName = csgnic
                )

        RVG SFM_SStore_RVG (
                RVG = rvg
                DiskGroup = hadg
                )

        SFM_SStore_IP requires SFM_SStore_PROXY
        SFM_SStore_RVG requires SFM_SStore_DG
        SFM_SStore_RVG requires SFM_SStore_IP


        // resource dependency tree
        //
        //      group SFM_SStore
        //      {
        //      RVG SFM_SStore_RVG
        //          {
        //          DiskGroup SFM_SStore_DG
```

```
        //          IP SFM_SStore_IP
        //              {
        //              Proxy SFM_SStore_PROXY
        //              }
        //          }
        //      }


group SFM_Services (
        SystemList = { Washington = 0, Chicago = 1 }
        ClusterList = { suse_cmsha_dr = 0, rhel5_cmsha = 1 }
        Authority = 1
        AutoStartList = { Washington }
        ClusterFailOverPolicy = Auto
        )

        Application SFM_Services_DB (
                User = root
                StartProgram = "/opt/VRTSsfmcs/config/vcs/db/online"
                StopProgram = "/opt/VRTSsfmcs/config/vcs/db/offline"
                MonitorProgram = "/opt/VRTSsfmcs/config/vcs/db/monitor"
                )

        Application SFM_Services_SECD (
                User = root
                StartProgram = "/opt/VRTSsfmcs/config/vcs/secd/online.sh"
                StopProgram = "/opt/VRTSsfmcs/config/vcs/secd/offline.sh"
                CleanProgram = "/opt/VRTSsfmcs/config/vcs/secd/clean.sh"
                MonitorProgram = "/opt/VRTSsfmcs/config/vcs/secd/monitor.sh"
                )

        Application SFM_Services_WEB (
                User = root
                StartProgram = "/opt/VRTSsfmcs/config/vcs/gui/online.sh"
                StopProgram = "/opt/VRTSsfmcs/config/vcs/gui/offline.sh"
                CleanProgram = "/opt/VRTSsfmcs/config/vcs/gui/clean.sh"
                MonitorProgram = "/opt/VRTSsfmcs/config/vcs/gui/monitor.sh"
                )

        Application SFM_Services_XPRTLDD (
                User = root
                StartProgram = "/opt/VRTSsfmcs/config/vcs/xprtld_domain/online.sh"
                StopProgram = "/opt/VRTSsfmcs/config/vcs/xprtld_domain/offline.sh"
```

```
        MonitorProgram = "/opt/VRTSsfmcs/config/vcs/xprtld_domain/monitor.sh"
        )

IP SFM_Services_IP (
        Critical = 0
        Device @Washington = eth2
        Device @Chicago = eth0
        Address = "IP_Address"
        )

Mount SFM_Services_Mount (
        Critical = 0
        MountPoint = "/hafs"
        BlockDevice = "/dev/vx/dsk/hadg/havol"
        FSType = vxfs
        FsckOpt = "-y"
        )

NIC SFM_Services_NIC (
        Critical = 0
        Device @Washington = eth2
        Device @Chicago = eth0
        )

RVGPrimary SFM_Services_RVGPRIMARY (
        RvgResourceName = rvg
        )

requires group SFM_SStore online local hard
SFM_Services_DB requires SFM_Services_IP
SFM_Services_DB requires SFM_Services_Mount
SFM_Services_IP requires SFM_Services_NIC
SFM_Services_Mount requires SFM_Services_RVGPRIMARY
SFM_Services_SECD requires SFM_Services_DB
SFM_Services_WEB requires SFM_Services_SECD
SFM_Services_XPRTLDD requires SFM_Services_DB


// resource dependency tree
//
//      group SFM_Services
//      {
//      Application SFM_Services_WEB
```

```
        //          {
        //          Application SFM_Services_SECD
        //              {
        //              Application SFM_Services_DB
        //                  {
        //                  IP SFM_Services_IP
        //                      {
        //                      NIC SFM_Services_NIC
        //                      }
        //                  Mount SFM_Services_Mount
        //                      {
        //                      RVGPrimary SFM_Services_RVGPRIMARY
        //                      }
        //                  }
        //              }
        //          }
        //      Application SFM_Services_XPRTLDD
        //          {
        //          Application SFM_Services_DB
        //              {
        //              IP SFM_Services_IP
        //                  {
        //                  NIC SFM_Services_NIC
        //                  }
        //              Mount SFM_Services_Mount
        //                  {
        //                  RVGPrimary SFM_Services_RVGPRIMARY
        //                  }
        //              }
        //          }
        //      }


group SFM_Xprtld (
        SystemList = { Washington = 0, Chicago = 1 }
        Parallel = 1
        AutoStartList = { Washington, Chicago }
        )

        Application SFM_Services_XPRTLDS (
                User = root
                StartProgram = "/opt/VRTSsfmcs/config/vcs/xprtld_standalone/online.sh"
                StopProgram = "/opt/VRTSsfmcs/config/vcs/xprtld_standalone/offline.sh"
```

```
        MonitorProgram = "/opt/VRTSsfmcs/config/vcs/xprtld_standalone/monitor.sh"
        )



// resource dependency tree
//
//      group SFM_Xprtld
//      {
//      Application SFM_Services_XPRTLDS
//      }
```

See "About configuring a new Veritas Operations Manager installation in high availability environment" on page 66.

See "About configuring Veritas Operations Manager in high availability and disaster recovery environment" on page 81.

See "Sample configuration: After you configure Veritas Operations Manager in high availability environment" on page 90.

About upgrading the high availability configurations

You can upgrade Veritas Operations Manager 3.1, or 4.*x*, UNIX-based, or Windows-based Management Server that is configured in the high availability (HA) environment to version 5.0. To upgrade, you can download and use the installer for Management Server.

See "Downloading Veritas Operations Manager 5.0" on page 13.

After the upgrade, you can use the HA environment on the upgraded Veritas Operations Manager 5.0 Management Server.

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

See "Upgrading Management Server in high availability environment" on page 101.

See "About configuring Veritas Operations Manager in high availability environment" on page 66.

Upgrading Management Server in high availability environment

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

- The SFM_Services, the SFM_SStore, and the SFM_Xprtld service groups should be online on one of the nodes of Veritas Operations Manager in the high availability environment, which is the active node.
- Symantec recommends that you take a backup of the Management Server data.
  See "Backing up data on UNIX" on page 51.
  See "Backing up data on Windows" on page 52.

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

To upgrade Management Server in high availability environment to 5.0

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

   See "Upgrading Management Server on UNIX" on page 48.

   See "Upgrading Management Server on Windows" on page 49.

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

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.

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

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 100.

See "Upgrading Management Server in high availability and disaster recovery environment" on page 102.

About upgrading the high availability and disaster recovery configurations

You can upgrade Veritas Operations Manager 3.1, or 4.*x*, UNIX-based Management Server that is configured in the high availability and disaster recovery (HA-DR) environment to version 5.0. To upgrade, you can download and use the installer for Management Server.

See "Downloading Veritas Operations Manager 5.0" on page 13.

After the upgrade, you can use the HA-DR environments on the upgraded Veritas Operations Manager 5.0 Management Server.

See "Upgrading Management Server in high availability and disaster recovery environment" on page 102.

See "About configuring Veritas Operations Manager in high availability environment" on page 66.

Upgrading Management Server in high availability and disaster recovery environment

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

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

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

To upgrade Management Server in high availability environment to 5.0

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

   See "Upgrading Management Server on UNIX" on page 48.

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

   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.

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

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 and disaster recovery configurations" on page 102.

See "Upgrading Management Server in high availability environment" on page 101.

Removing the high availability configuration

To remove the high availability configuration from Veritas Operations Manager, you need to launch the **https://hostname:5634** URL.

Note: In Veritas Operations Manager 5.0, you cannot remove the Veritas Operations Manager HA-DR environment that is configured in the remote site.

The procedure uses the following host names:

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

To remove the high availability configuration from Veritas Operations Manager

1. Launch the following URL from a Web browser:

   https://My_Virtual-host_1:5634

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

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

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

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

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

   - On Node1and Node2, remove the `sfm_ha` directory from the mount location of the file system.
   - On both the nodes, check for the `VRTSsfmcs.pre_clus` file on the location *var/opt/.VRTSsfmcs.pre_clus/*. If the `VRTSsfmcs.pre_clus` file exist on any of the nodes, remove the file.

4. In the next panel, view the status of the tasks that are performed as part of removing the Veritas Operations Manager HA configuration and do the following:

   - Click the link that is displayed on the panel to log on to Management Server from which the HA configuration is removed.
   - Click **Quit** to quit the configuration dialog.

See "About configuring Veritas Operations Manager in high availability environment" on page 66.

See "About configuring an existing Veritas Operations Manager installation in high availability environment" on page 76.

Index

A

ActiveX 31

B

backing up Veritas Operations Manager
  on UNIX 51
  on Windows 52
browsers 31

C

configuring
  existing Management Server installation in HA environment 76
  Firefox 40
  Internet Explorer 40
  Management Server 38
  Management Server in HA- DR environment 81
  new Management Server installation in HA environment 66
  Web browsers 40

D

deploying
  Veritas Operations Manager 16
domains
  multiple 31
downloading
  managed host files 14
  Management Server files 14
  Veritas Operations Manager 13

F

firewalls
  ports 31

G

gendeploy.pl 45

H

HA configuration
  completing the configuration 75
  creating base service groups on UNIX 70
  creating base service groups on Windows 73
  modify default IP address and host name on UNIX 77
  modify default IP address and host name on Windows 79
  performing initial configuration of Management Server 69
  prerequisites 68
  retrieving virtual host name and virtual IP address 68
HA-DR configuration 81
  creating base service groups 84
  enabling configuration 88
  performing initial configuration 83
  prerequisites 82

I

installation resources
  Veritas Operations Manager 16
installing
  host management through Solaris JumpStart 45
  managed host 41
  managed host on UNIX 42
  managed host on Windows 43
  Management Server 34
  Management Server on UNIX 35
  Management Server on Windows 36
Intranet zone security level 31

J

JavaScript 31
JScript 31

M

managed host
  installation files for UNIX 42

managed host *(continued)*
installation files for Windows 43
installing 41
installing on UNIX 42
installing on Windows 43
installing through Solaris JumpStart 45
package 34
types 12
uninstalling on UNIX 61
uninstalling on Windows 62
upgrading 55
upgrading on UNIX 57
upgrading on Windows 58
verifying installation on UNIX 46
verifying installation on Windows 46
managed hosts
upgrade using VOM console 56
verifying version using the console 60
Management Server
configuring 38
configuring a new installation in HA environment 66
configuring an existing installation in HA environment 76
installation files for UNIX 35
installation files for Windows 36
installing 34
installing on UNIX 35
installing on Windows 36
package 34
uninstalling on UNIX 60
uninstalling on Windows 61
upgrading 47
upgrading in HA DR environment 102
upgrading in HA environment 101
upgrading on UNIX 48
upgrading on Windows 49
verifying installation on UNIX 37
verifying installation on Windows 38
verifying version using the console 59
Management Server HA-DR
configuring 81

N

network requirements 31

P

pop-up blockers 31
ports
firewalls 31

R

resolv.conf 31
resources
installation
Veritas Operations Manager 16
restoring Veritas Operations Manager
on UNIX 53
on Windows 54

S

security level 31
Solaris JumpStart installation 45
space estimation
data logs 26
SSL 31
standalone management
defined 13

T

TCP 31
toolbars 31

U

UC 16
UDP 31
uninstalling
managed host on UNIX 61
managed host on Windows 62
Management Server on UNIX 60
Management Server on Windows 61
upgrading
disaster recovery 102
HA 100
HA-DR 102
managed host 55
managed host on UNIX 57
managed host on Windows 58
managed host using installer package 58
managed host using operating system commands 57
managed hosts using console 56
Management Server 47
Management Server in HA DR environment 102
Management Server in HA environment 101
Management Server on UNIX 48

upgrading *(continued)*
Management Server on Windows 49
Veritas Operations Manager add-ons 47
UTC 16

V

VEA
deployment 18
verifying
managed host installation on UNIX 46
managed host installation on Windows 46
managed host version using the console 60
Management Server installation on UNIX 37
Management Server installation on Windows 38
Management Server version using console 59
Veritas Enterprise Administrator.. *See* VEA
Veritas Operations Manager
about 11
backing up on UNIX 51
backing up on Windows 52
choosing managed hosts 20
choosing Management Server hosts 19
choosing Web console hosts 31
configuring Management Server 38
deployment configurations 16
downloading 13
downloading managed host files 14
downloading Management Server files 14
installation resources 16
installing managed host on UNIX 42
installing managed host on Windows 43
installing Management Server on UNIX 35
installing Management Server on Windows 36
managed host component 12
Management Server component 12
packages 34
restoring on UNIX 53
restoring on Windows 54
uninstalling 61
upgrading managed host on UNIX 57
upgrading managed host on Windows 58
upgrading Management Server in HA DR environment 102
upgrading Management Server in HA environment 101
upgrading Management Server on UNIX 48
upgrading Management Server on Windows 49
URL 13
Web server component 12
Veritas Operations Manager Add-ons
downloading 47
installing 47
upgrading 47
Veritas Operations Manager deployment
centralized and standalone management 18
centralized management 17
centralized management of Non-SF hosts 18
standalone management 18
Veritas Operations Manager HA
configuring a new installation 66
configuring an existing installation 76
configuring for disaster recovery 81
removing configuration 103
upgrading 100
Veritas Operations Manager in HA environment 66
Veritas_Operations_Manager_CMS_5.0_Linux.bin 14
Veritas_Operations_Manager_CMS_5.0_SolSparc.bin 14
Veritas_Operations_Manager_CMS_5.0_Win.exe 14
Veritas_Operations_Manager_Managed_Host_Bundle_5.0.0.zip 14
virtual machines
cloning 44
migrating 44
VRTSsfmcs package 34
VRTSsfmh package 34, 41–42, 57
VRTSsfmh_5.00.0xxx_Windows_arch_IA64.msi 58
VRTSsfmh_5.00.0xxx_Windows_arch_x64.msi 58
VRTSsfmh_5.00.0xxx_Windows_arch_x86.msi 58

W

Web browsers
About 31
configuring 40
Web console 31
Web server
overview 12