Veritas™ Operations Manager Release Notes

4.1

January 2013

Symantec™

Veritas™ Operations Manager Release Notes

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

Product version: 4.1

Documentation version: 4.1.2

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 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

Contents

Chapter 1

Overview of this release

This chapter includes the following topics:

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 14.
- Managed hosts
  See "About the managed host" on page 14.

For more information on managing security roles and users accounts, see the *Veritas Operations Manager 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 13.

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 13.

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 13.

Coexistence of Veritas Operations Manager and Veritas Operations Manager Advanced

If you plan to install both Veritas Operations Manager and Veritas Operations Manager Advanced on a single host, you need to check the support for coexistence of both the products. Only certain versions of Veritas Operations Manager can be installed with certain versions of Veritas Operations Manager Advanced. The coexistence support also depends on the sequence in which the products are installed.

Table 1-1 describes the coexistence support when Veritas Operations Manager is installed before Veritas Operations Manager Advanced:

Table 1-1 Coexistence support when Veritas Operations Manager is installed first

Veritas Operations Manager version on the host	Supported Veritas Operations Manager Advanced version
4.0, or lower versions	None
4.0 RU1	4.0
4.1	4.0 RU1

Table 1-2 describes the coexistence support when Veritas Operations Manager Advanced is installed before Veritas Operations Manager:

Table 1-2 Coexistence support when Veritas Operations Manager Advanced is installed first

Veritas Operations Manager Advanced version on the host	Supported Veritas Operations Manager version
4.0	4.0 RU1, or later versions
4.0 RU1	4.1

What's new in Veritas Operations Manager 4.1?

This release of Veritas Operations Manager includes the following new features and enhancements.

- Veritas Operations Manager Virtual Business Services Availability Add-on
  See "Veritas Operations Manager Virtual Business Services Availability Add-on" on page 17.
- Ability to manage Symantec ApplicationHA on the virtual entities
  See "Ability to manage Symantec ApplicationHA on the virtual entities" on page 17.
- The new Symantec Performance Value Unit pricing method
  See "The new Symantec Performance Value Unit pricing method" on page 17.
- SORT integration for patches and add-ons information
  See "SORT integration for patches and add-ons information" on page 18.
- User interface enhancements
  See "User interface enhancements" on page 18.
- `vomadm` utility
  See "vomadm utility" on page 18.
- Support for restoring backups of UNIX-based Management Server in high-availability configuration
  See "Support for restoring backups of UNIX-based Management Server in high-availability configuration" on page 19.
- `vomsc restart` command
  See "vomsc restart command" on page 19.
- Support for Red Hat Enterprise Linux 6.1
  See "Support for Red Hat Enterprise Linux 6.1" on page 19.

Veritas Operations Manager Virtual Business Services Availability Add-on

The application entity type of business entity is now referred to as Virtual Business Service (VBS) in Veritas Operations Manager. A VBS provides continuous high availability, and reduces the frequency and duration of service disruptions for the multi-tier business applications that are running on heterogeneous operating systems, and virtualization technologies. A VBS represents the multi-tier applications as a single consolidated entity, and provides support for high availability and disaster recovery.

You can use the Veritas Operations Manager Virtual Business Services Availability Add-on to perform several operations that are related to a VBS. For example, start and stop a VBS, configure service group dependencies for a VBS, and enable fault management. The fault management feature provides better control of fault propagation across multi-tier applications.

Ability to manage Symantec ApplicationHA on the virtual entities

Using the new Veritas Operations Manager Add-on for ApplicationHA Management, you can manage Symantec ApplicationHA in the VMware ESX/ESXi, Linux Kernel Virtual Machine (KVM), IBM AIX Logical Partitions (LPAR), and the Oracle VM Server (OVM) for SPARC (Solaris LDOM) environments. The Add-on for ApplicationHA Management lets you perform the various ApplicationHA operations through the Veritas Operations Manager console, based on your user role in Veritas Operations Manager. The add-on supports the virtual entities on the Windows, Solaris, Linux, and the IBM AIX operating systems.

The new Symantec Performance Value Unit pricing method

From the 4.1 release, Veritas Operations Manager lets you calculate the new pricing unit for the Storage Foundation and High Availability products on your managed hosts, which is called the Symantec Performance Value Unit (SPVU). The SPVU is calculated by considering the processor type, the number of used cores and the operating system on which the host runs. Based on these criteria, a host is assigned a specific SPVU value per core. The price for a product is calculated by multiplying the SPVU values for the cores that the product uses with the total number of cores that are allocated to the physical or virtual hosts. This new pricing method lets you pay for the products optimally, instead of paying for fixed tiers.

SORT integration for patches and add-ons information

The information about the patches and Veritas Operations Manager add-ons is available on SORT Web site. This information is gathered and displayed on Veritas Operations Manager console using the SORT API. You can use this information to decide on the patches or add-ons to be downloaded and installed based on their importance and criticality.

User interface enhancements

The following key user interface enhancements have been introduced in Veritas Operations Manager 4.1:

- New color and font scheme that is consistent across the product user interface
- Enhanced headers that provide more user details, and the **Logout** option
- New icons on the top-level menus
- Table enhancements:
  - New **Actions** drop-down menu that lists all the operations that you can perform on the objects that are displayed in the table
  - New **Table Tasks** drop-down menu that lists all the operations that you can perform on the table
  - New object state icons and text color that highlight the state of objects that are displayed in the table

vomadm utility

Along with the graphical user interface, now the Veritas Operations Manager users can make use of the `vomadm` command-line utility to perform various operations. The supported operations are grouped in the following categories:

- Host management
  You can use the `host-mgmt` option to manage the configured managed hosts in Veritas Operations Manager.
- Deployment management
  You can use the `hotfix` option to install or uninstall a hot fix on the managed hosts.
- Business entity management
  You can use the `makeBE` option to perform the various operations that are related to business entities. For example, create a business entity, edit a business entity, import a business entity, and export the content of a business

entity. These operations are supported for organization entities and Virtual Business Services (VBS).

Support for restoring backups of UNIX-based Management Server in high-availability configuration

On UNIX, the `vom_bkup.pl` backup script can now be used to restore the backup of a Management Server in high-availability configuration.

vomsc restart command

The `vomsc` command now has the `restart` option. You can use the `restart` option to restart a service, or all the services that the script manages.

Support for Red Hat Enterprise Linux 6.1

You can now install Veritas Operations Manager 4.1 Management Server and managed host on a Red Hat Enterprise Linux 6.1 host.

Issues fixed in the Veritas Operations Manager 4.1 release

Table 1-3 lists the Management Server issues that have been fixed in the Veritas Operations Manager 4.1 release.

Table 1-3 Management Server issues fixed in Veritas Operations Manager 4.1

Incident	Description
2349173	Service groups and resources that are deleted from a Veritas Cluster Server configuration are still displayed in the Veritas Operations Manager console.
2379041	In a VVR Bandwidth report, the column for total data that is transmitted from the source to the target host is incorrectly sorted in a string-based manner.
2409821	When policy checks are run on the business entities that contain agentless hosts, Veritas Operations Manager does not provide a clear message indicating that the policy checks skip the agentless hosts.
2535218	Incorrect tier information is displayed in Veritas Operations Manager license reports.
2553241	Custom scripts are not run on the specified schedule.

Table 1-3 Management Server issues fixed in Veritas Operations Manager 4.1 *(continued)*

Incident	Description
2568201	Management Server configuration fails with an "Primary Broker Configuration Failed" error after the configuration in the browser.
2573076	Management Server configuration fails with an "Authentication Failed" error.
2600232	The emailed Uptime Analysis reports show incorrect information.
2602058	The Uptime Analysis report incorrectly repeats all the service groups under every cluster.

Table 1-4 lists the managed host issues that have been fixed in the Veritas Operations Manager 4.1 release.

Table 1-4 Managed host issues fixed in Veritas Operations Manager 4.1

Incident	Description
2397372	For a UNIX host that is configured using agentless discovery, the path count is displayed incorrectly for the disks that are either not managed by any multipathing software, or are managed by non-supported multipathing software.
2405802	The number of columns is incorrectly displayed for striped volumes on UNIX agentless hosts.
2416221	The agentless discovery of Windows hosts is not supported in MPIO environments.
2422442	The UNIX agentless host configuration fails and does not display the exact cause of the SSH failure.
2430265	Faults are not reported for agentless hosts when Privilege Control Software (PCS) is removed.
2478766	An incorrect error message is displayed while configuring a Windows agentless host with Storage Foundation or Veritas Operations Manager managed host installed.
2479822	The layout of AIX LVM volumes is incorrectly displayed for agentless hosts.
2485692 and 2486793	VMware ESX server and virtual machine storage correlation works only when you have a single SCSI controller given from the ESX server to the guest.

Table 1-4 Managed host issues fixed in Veritas Operations Manager 4.1 *(continued)*

Incident	Description
2487010	The disk state is displayed incorrectly for Windows agentless hosts.
2487229	Dynamic disk groups are displayed for agentless hosts when there are no dynamic disks.
2490221	The mount points are not discovered properly on Windows agentless hosts with volumes that are mounted multiple times.
2495820	The agentless configuration of a Windows host on the console fails after five minutes.
2497125	The refresh of a Windows agentless host from a Windows control host displays an error.
2509605	Converting a Windows agentless host to an agent host results in duplicate entries for the host.
2528856	Veritas Operations Manager does not recognize some Windows file systems while performing thin provisioning reclamation.
2531024	The `vxlist disk` command incorrectly reports the ZFS managed disks as SVM devices.
2553166	The unallocated size incorrectly displays as 0 for many disks.

Chapter 2

System requirements

This chapter includes the following topics:

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 4.0 Update 3 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 6 Red Hat Enterprise Linux 6.1	x86 64-bit is the supported architecture. For RHEL 6.0 on x86 64-bit, and RHEL 6.1 on x86 64-bit, the 32-bit `glibc` package must be installed.
SUSE Linux Enterprise Server 9 SUSE Linux Enterprise Server 10	x86 64-bit is the supported architecture.
Solaris 10	SPARC is the supported architecture.
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.

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

Operating system supported	Notes
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, and PowerPC; Storage Foundation 4.1 is supported on x86 and Xeon (32- and 64-bit). For RHEL 6.0 on x86 64-bit, and RHEL 6.1 on x86 64-bit, the 32-bit `glibc` package 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 SPARC Solaris 10 x86	
Windows Server 2003 Windows Server 2008 Windows 2008 R2	Supported on x86, x64, and IA64.

Veritas Operations Manager operating system requirements for 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 SPARC
- Solaris 10 x86
- 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 Web site :

www.symantec.com/techsupp/

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 are already consumed by other software applications running on the host.

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 VMware virtualization infrastructure.
- Disk space required: 15GB of disk space for every 1000 managed hosts.

For a managed host:

- CPU required: See Veritas Storage Foundation documentation.
- Memory required: See Veritas Storage Foundation documentation.
- Disk space required:
  - On UNIX hosts: 50MB to 200MB in `/var/opt` for discovery state files; 100MB in `/opt`.
  - On Windows hosts: 50MB to 200MB in *`Install_path`*`\Veritas\VRTSsfmh`; 100MB in `%COMMONAPPDATAFOLDER%\Symantec`.

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/TECH157641

See "About the frequency of managed host information discovery" on page 27.

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.
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.
VMware	360	ESX servers, virtual machines, and their storage dependencies. **Note:** This information is discovered only when Control Host Add-on is installed on a managed host that is designated as the control host.

Family	Frequency in minutes	Discovered information
Agentless	360	The following information on the hosts that are configured on the control host for agentless: ■ The IP addresses, operating system, and the usage of the CPU and memory ■ The host bus adapters (HBAs) on the host ■ The disks on the hosts and their correlation with the array LUNs and multipathing ■ The volumes and the volume groups on the native Volume Manager ■ The mount points of the file systems and the correlation of the file systems with the disks ■ In a VMware guest environment, the correlation of the guest with the virtual machine and the correlation of the storage in the guest with the storage exported from the ESX server. **Note:** This information is discovered only when Control Host Add-on is installed on a managed host that is designated as the control host.

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.

Supported hardware

The following TechNotes contain the Hardware Compatibility List (HCL) for Veritas Operations Manager 4.1 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

The following TechNotes contain the Hardware Compatibility List (HCL) for Veritas Operations Manager 4.1 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

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.

Network and firewall requirements

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

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

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

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

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

Port	Protocol	Initiator	Purpose	Effect if blocked
5634	TCP	Management Server	Management Server configuration	Management Server cannot be configured.
			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:** We recommend that you keep port 5634 open between managed hosts for scalability and performance optimization.	Managed host cannot be added to the Management Server domain.

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

Port	Protocol	Initiator	Purpose	Effect if blocked
14161	TCP	Web console	Run the Management Server console	Users cannot access the Management Server console.

About the consumption of the managed host components

The managed host components of Veritas Operations Manager consume certain amount of CPU, memory, and network bandwidth for various functions.

Various processes and services in Veritas Operations Manager impose different amount of load on the managed hosts. The processes and services and their consumption on the managed host are as follows:

- UNIX - Uses the XPRTLD, VXDCLID, sfmh-discovery.pl daemons. The CPU and the memory consumption for these daemons is minimal on a managed host.
- Windows - Uses the XPRTLD daemon. The CPU and the memory consumption for this daemon is minimal on a managed host.
- Discovery - The discovery in Veritas Operations Manager is ephemeral. Therefore, the CPU and the memory consumption for the discovery is minimal on a managed host.

The network bandwidth consumption for the managed hosts is primarily related to the heartbeats that occur every five minutes. The heartbeat operation sends data that has a size of less than 1KB to Management Server. The data reporting occurs only if there is a configuration change on the storage objects that are associated to the managed host. Certain amount of network bandwidth is also used for the data replication.

See "About the frequency of managed host information discovery" on page 27.

Chapter 3

Software limitations

This chapter includes the following topics:

- VCS configuration check reports violations only if at least one node in the cluster is running Veritas Cluster Server (2117417)
- Agent discovery of a VMware guest (2495586)
- Limitations related to the correlation between the disks and the disk groups
- No support to online and offline multiple virtual machines using the Virtual Business Service start and stop operations (2177421)
- Virtual Business Service start operation does not validate the service group's resource criticality (2169223)
- Unable to start the Virtual Business Service (VBS) if the virtual machine hosting the service groups of the VBS is already down
- Discovery of VMware VirtualCenter server or ESX server is not case–sensitive (2567318)
- Core density may not get calculated properly on HP-UX11iv2 hosts
- Disk information of the managed hosts with HP Smart Array CCISS driver is not discovered (2603958, 2605134)

No coexistence of managed host and CommandCentral Storage Management Server

Do not install Veritas Operations Manager managed host on a host that has CommandCentral Storage Management Server installed on it. Even if the installation succeeds, the operation to add the host to the Management Server domain fails.

Live statistics for initiators are not supported on HP-UX (2001078)

You cannot view live statistics for initiators in the performance charts on the HP-UX hosts that have Veritas Volume Manager 5.0, or earlier releases.

Performance charts are not supported in certain cases for multiple objects that belong to different hosts (2023666)

Performance charts are not supported for multiple disks, volumes, or file systems that belong to different hosts that are not shared as part of a CVM/CFS configuration. However, you can view performance charts for multiple disks, volumes, or file systems from different hosts that are shared as part of a CVM/CFS configuration.

Performance charts are also not supported for multiple initiators that belong to different hosts. However, you can view performance charts for multiple initiators from the same host.

Performance graphs cannot be viewed for Windows managed hosts

In Veritas Operations Manager, you cannot view performance graphs for Windows managed hosts.

Volume layout not discovered for LDM-managed volumes mounted without a drive letter

Veritas Operations Manager does not discover the layout for the volumes that are mounted without a drive letter on a Windows host (that does not have Storage Foundation for Windows installed on it) when the volume manager type is Microsoft LDM. As a result, the **Layout** column for this volume is displayed as **Unknown** on the Veritas Operations Manager console.

Backup and restore limitations in Veritas Operations Manager 4.1

On UNIX, the `vom_bkup.pl` backup script cannot be used to back up and restore an existing Management Server in high-availability configuration for disaster recovery.

On Windows, the `vom_bkup.pl` 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. To restore the backed up data, contact Symantec Technical Support.

Veritas Operations Manager does not support the discovery of LDoms and Zones together on the same host (2281088)

Veritas Operations Manager does not support the discovery of LDoms and Zones if they co-exist on the same Solaris host. In a configuration where both the LDoms and the Zones co-exist, Veritas Operations Manager discovers LDoms.

Veritas Operations Manager Add-on for Storage Foundation Administration 4.1 limitations

The Storage Foundation operations that you can perform using the Veritas Operations Manager Add-on for Storage Foundation Administration are not supported on the managed hosts that have the `VRTSsfmh` package versions lower than 4.0.

The Veritas Operations Manager Add-on for Storage Foundation Administration does not support all the Storage Foundation operations. For the list of supported operations, refer to the *Veritas Operations Manager Add-on for Storage Foundation Administration User's Guide*.

Deployment-related limitations

You cannot upgrade Veritas Operations Manager Management Server from version 2.*x* to version 4.1. You need to either upgrade to version 3.*x* and then to version 4.1, or, remove your 2.*x* installation and perform a fresh installation of Veritas Operations Manager 4.1.

Windows Management Server high availability configuration limitations

Veritas Operations Manager supports only the Windows Server versions 2008 (64-bit) and 2008 R2 (64-bit) for configuring the Windows Management Server in high availability environment.

Veritas Operations Manager does not support configuring the disaster recovery feature on a Windows Management Server high availability configuration.

Solaris Zones virtualization support limitations

You must install the `VRTSsfmh` package on the Global Zone. You cannot install the `VRTSsfmh` package on the non-Global Zones.

Solaris Zones virtualization in Veritas Operations Manager does not support slices. Veritas Operations Manager supports only full disks.

Solaris Zones virtualization in Veritas Operations Manager does not support discovery of secure Oracle, DB2, and Sybase database instances running in the non-Global Zones.

Discovery limitations for virtualization support

Veritas Operations Manager has the following discovery limitations for virtualization support:

- Veritas Operations Manager does not support storage discovery for the Oracle VM Server (OVM) for SPARC (previously Solaris LDOM), the Linux Kernel Virtual Machine (KVM), and the IBM AIX Logical Partitions (LPAR) environments.
- For virtualization environments like KVM, LDOM, and LPAR, Veritas Operations Manager displays only the Power ON state of a virtual machine.
- For the Linux-based LPAR guest virtual machines that are configured on an LPAR server, which is in turn managed by an HMC server, the operating system and the operating system version are not discovered.

While creating the storage template, the file system is created with default setting when template indicates no file system needs to be created (2335583)

For Windows managed host, when you try to provision storage for a volume, the file system is created by default (user interface creates empty file system entry), even if you do not select the create file system option. Also, the next available drive letter is assigned to the file system.

Log on to console fails on Internet Explorer if Management Server host name has the underscore (_) character

When you install or upgrade Management Server to 4.1 on a Windows 2003 host, and attempt to log on to the console using Internet Explorer, the log on may fail. The failure occurs if the console is launched using the Management Server host name, and the host name contains the underscore (_) character.

Internet Explorer does not allow the underscore (_) character in the host name. Do not install Management Server on such a host.

VCS configuration check reports violations only if at least one node in the cluster is running Veritas Cluster Server (2117417)

VCS configuration policy check in Veritas Operations Manager does not report any violations if Veritas Cluster Server is not running on any of the systems in the cluster. Also, if the cluster has a single system and Veritas Cluster Server is not running on that system, the VCS configuration check does not report violations.

Agent discovery of a VMware guest (2495586)

If you install an agent after changing the MAC ID of a VMware guest that is currently being discovered using agentless discovery, you need to manually unconfigure agentless discovery.

Agent configuration of a host that had previously been configured using agentless discovery, should unconfigure agentless discovery on the host. However, changing the MAC ID of the VMware guest does not unconfigure agentless discovery, as changing the MAC ID changes the ID used to identify the host in the Veritas Operations Manager database. As a result, duplicate entries for the host (agent and agentless) are displayed. On the next scheduled discovery or manual refresh of the agentless host, the host will display as faulted. You must manually unconfigure agentless discovery of the host to remove any duplicate entries.

If you do not change the MAC ID of the VMware guest after configuring it using agentless discovery, you do not need to manually unconfigure the host; you can configure the host using an agent.

Limitations related to the correlation between the disks and the disk groups

The following limitations exist in Veritas Operations Manager 4.1, which are related to the correlation between the disks and the disk groups:

- You cannot view the disk information in the file system details view, or in the disk group details view, when one partition of a disk contains a file system that is mounted on it, and the other partition belongs to a disk group.
- You cannot view the disk information in the details view of one of the disk groups, when two partitions of a disk belong to two disk groups.

No support to online and offline multiple virtual machines using the Virtual Business Service start and stop operations (2177421)

This issue is applicable to the hybrid service groups and parallel service groups that are configured on the virtual machines in a Virtual Business Service (VBS). For the VBS start and stop operations, the VBS Availability Add-on does not start or stop multiple virtual machines. You can online or offline the service groups on all systems. However, you cannot start or stop all virtual machines. Currently, the VBS Availability Add-on is not intended to start or stop multiple virtual machines.

Virtual Business Service start operation does not validate the service group's resource criticality (2169223)

Using VBS Availability Add-on, when you start a Virtual Business Service (VBS), the start operation does not validate whether the service group has any non-critical resource. So, the operation does not detect any fault that occurs while bringing these resources online, nor does it detect if such resources are already faulted when the VBS start is attempted. If such faults exist, Veritas Operations Manager waits for the VBS to start completely, and, eventually times out aborting the VBS start operation. You can choose to abort the operation. As a preventive step, configure all the resources of a service group as critical.

Unable to start the Virtual Business Service (VBS) if the virtual machine hosting the service groups of the VBS is already down

This issue is observed when you have configured a VBS's Service Group on a virtual machine, and virtual machine "auto-start" and "auto-stop" options are selected while configuring the service groups dependencies using the VBS Availability Add-on. If the virtual machine is turned-off, the Veritas Operations Manager still displays the service group's state as Online on the Veritas Operations Manager console. It happens because it captures the last state of the service group in the Veritas Operations Manager database. If you try to online the VBS, the Veritas Operations Manager notifies the user that the VBS is already online.

Discovery of VMware VirtualCenter server or ESX server is not case–sensitive (2567318)

While discovering VMware VirtualCenter server or ESX server, Veritas Operations Manager cannot distinguish between two or more virtual disks whose names differ only in case. Only one of such disks is discovered in Veritas Operations Manager.

Core density may not get calculated properly on HP-UX11iv2 hosts

Core density(#cores/physical processor) discovered on HP-UX 11.23 managed hosts may not be correct due to CLI-related limitations. Incorrect value of core density makes the LDR unable to calculate Symantec Performance Value Unit (SPVU) information for such hosts. The user can assign the SPVU manually for the hosts.

Disk information of the managed hosts with HP Smart Array CCISS driver is not discovered (2603958, 2605134)

The issue is applicable to agent and agentless discoveries of managed hosts in Veritas Operations Manager. Presently, the disk information of the managed host with HP Smart Array CCISS driver is not discovered in Veritas Operations Manager.

Chapter 4

Known issues

This chapter includes the following topics:

Management Server issues

The following issues relate to Veritas Operations Manager Management Server.

Inconsistent behavior when you configure the LDAP domain if the LDAP server does not respond or server name is invalid (2024598)

If the LDAP server name is invalid or if it does not respond within five minutes when you configure the LDAP domain, the configuration fails with inconsistent results. Either the 'Invalid CA certificate' error message is displayed, or the configuration proceeds to the second stage with an empty search base.

Workaround:

In both the cases, you must not proceed with configuring the LDAP domain. You must fix the LDAP server name to point to correct server.

Operating system-based authentication domains are removed after you refresh the authentication broker in a Windows Management Server-HA setup (2362587)

In a Windows Management Server-HA setup, if you refresh the authentication broker after the first failover, the operating system-based authentication domain on the node where Management Server is active is removed.

Workaround:

In a Windows Management Server-HA setup, you can use the authentication domains that are not based on the operating system to log on to Management Server.

Veritas Operations Manager prompts you to overwrite the search query even when you save the query for the first time (2299458)

This issue is observed when you use 3.*x* Management Server with configured 3.*x* managed hosts, and you have installed the Storage Insight Add-on. When you upgrade Management Server from version 3.*x* to 4.1, and run and save the search query (under the **Search** option), you see the following error message:

Query by that name already exists, Do you want to update?

Veritas Operations Manager prompts you to overwrite the search query even when you save the query for the first time.

Workaround:

You need to reinstall the Storage Insight Add-on on Management Server.

VirtualCenter discovery configuration fails if the discovery of the member ESX servers is already configured in Veritas Operations Manager (2334962)

In Veritas Operations Manager, the VirtualCenter configuration fails if you have configured it after you configure one or more ESX servers that the VirtualCenter manages.

Workaround:

You must not configure the individual ESX servers if you plan to configure the VirtualCenter server that manages the ESX servers. If any such configuration of ESX servers exists in your datacenter, you must remove them before you configure the VirtualCenter that manages the ESX servers.

Delayed discovery of VMware VirtualCenter server by Control Hosts in Veritas Operations Manager (2342314)

In Veritas Operations Manager, the discovery of some of the VMware VirtualCenter servers using Control Hosts takes a long time to complete. This issue occurs because some of the datastores that are associated with the VirtualCenter server do not respond on time, which results in timeout.

Workaround:

From the VMware SDK log, you can identify the datastores that cause the delay in the discovery of VirtualCenter server. In the VirtualCenter server that contains the datastore, navigate to **Administration > vServer Settings > Timeout Settings** and set the timeout to a lower value.

Log on to the Veritas Operations Manager console may fail on Firefox (1939352)

When you try to log on to the Veritas Operations Manager console on Firefox, you may get the following error:

```
Secure Connection Failed
An error occurred during a connection to <system>
Peer reports it experienced an internal error.
(Error code: ssl_error_internal_error_alert)
```

Workaround:

Perform any one of the following modifications on the configuration settings for Firefox:

- Disable TLS
- Enable SSL 2 encryption protocols

To disable TLS in Firefox

1. In Firefox, select **Tools** > **Options**.
2. In the **Options** dialog box, click **Advanced**.
3. In the **Advanced** panel, under the **Encryption** tab, clear the **Use TLS 1.0** check box.

To enable SSL 2 encryption protocols in Firefox

1. In Firefox, in the address bar, type **about:config** and press **Enter**.
2. On this page, use **Filter** to search for the `security.enable_ssl2` setting.

3 Select the `security.enable_ssl2` setting and do one of the following to set the value to `true`:

- Double-click the `security.enable_ssl2` setting.
- Right-click the `security.enable_ssl2` setting and then click **Toggle**.

4 Restart Firefox.

Authentication broker crashes while performing LDAP authentication (2017319)

On a host in which LDAP is configured with PAM and TLS is enabled, the authentication broker may crash while performing LDAP authentication.

Workaround:

Perform the following changes.

- Disable `start_tls`.
- Remove PAM from authsequence.

To disable the start_tls parameter

- In the `/etc/ldap.conf` file, after `ssl start_tls` add the following line:

```
ssl no
```

To remove PAM from authsequence

- In the `EAT_DATA_DIR/root/.VRTSat/profile/VRTSatlocal.conf` file, delete `pam` from the following entry:

```
"DefaultAuthSequence"="pam unixpwd nis nisplus"
```

XPRTLD daemon fails when Veritas Operations Manager starts because of the corrupt AT pem files in the `VRTSsfmh` package (2145925)

The XPRTLD daemon fails when Veritas Operations Manager starts, if the AT pem files (the certificate files in the `VRTSsfmh` package) is corrupt.

Workaround:

To repair the corrupt AT pem files on UNIX:

1. Stop the XPRTLD daemon by using the following command:

   ```
   /opt/VRTSsfmh/adm/xprtldctrl stop
   ```

2. Delete all the files in the directory `/var/VRTSat_lhc/` by using the following command :

   ```
   rm -rf /var/VRTSat_lhc/*
   ```

3. Take a backup of the credentials in the `/var/VRTSat/.VRTSat/profile/certstore/` directory, by using the following command:

   ```
   mv /var/VRTSat/.VRTSat/profile/certstore/*.0 /tmp/backupcreds/
   ```

4. In the directory, delete the pem files by using the following commands:

   - `rm /var/VRTSat/.VRTSat/profile/certstore/keystore/PubKeyFile.pem`
   - `rm /var/VRTSat/.VRTSat/profile/certstore/keystore/PrivKeyFile.pem`

5. Restart any running shared broker process by using the following command:

   ```
   /opt/VRTSat/bin/vxatd
   ```

6. Authenticate the local host to create a self-signed certificate by using the following commands:

   ```
   export EAT_HOME_DIR=/opt/VRTSsfmh

   export EAT_DATA_DIR=/var/opt/VRTSsfmh/sec

   cd $EAT_HOME_DIR/bin

   ./vssat authenticate -d localhost
   ```

7. Start the XPRTLD daemon by using the following command:

   ```
   /opt/VRTSsfmh/adm/xprtldctrl start
   ```

To repair the corrupt AT pem files on Windows:

1. Stop the XPRTLD daemon by using the following command:

   ```
   net stop xprtld
   ```

2. Delete all the files in the following directory:

   ```
   %ALLUSERSPROFILE%\Application
   Data\VERITAS\Security\Authentication\VRTSat_lhc
   ```

3. Take a backup of the credential in the following directory:

AT_PROFILE_DIR\certstore* c:\temp*

You can get the AT Profile directory from the following locations:

- For 64-bit Windows:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VERITAS\Security\Authentication\Credential Manager\Profiles\SYSTEM\ ProfileDir
- For 32-bit Windows:
  HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\Security\Authentication\Credential Manager\Profiles\SYSTEM\ProfileDir

4 Delete the following pem files:

- *AT_PROFILE_DIR*\certstore\keystore\PubKeyFile.pem
- *AT_PROFILE_DIR*\certstore\keystore\PrivKeyFile.pem

5 Restart any running shared broker process by using the following commands:

- sc stop vrtsat
- sc start vrtsat

6 Authenticate the local host to create a self-signed certificate by using the following commands:

```
set EAT_HOME_DIR=%PROGRAMFILES%\VERITAS\VRTSsfmh

set EAT_DATA_DIR=%ALLUSERSPROFILE%\Symantec\VRTSsfmh\sec

cd %EAT_HOME_DIR%\bin

vssat authenticate -d localhost
```

7 Start the XPRTLD daemon by using the following command:

```
net start xprtld
```

Status of all SF Manager 2.*x* hosts is shown as healthy on an upgraded Veritas Operations Manager 4.1 setup (2009372)

When you view the status of hosts on an upgraded Veritas Operations Manager 4.1 console that has SF Manager 2.*x* managed hosts, the status of all the hosts is shown as healthy even though some of the hosts have reported faults.

Workaround:

You need to upgrade the 2.*x* managed hosts to Veritas Operations Manager 4.1 and then clean up the 2.*x* faults.

To clean up the 2.*x* faults

1 Create a file `a.sql` that has the following contents:

```
call HABDBSYNC.SP_ccsf_db_cleanup_21_faults();
```

2 Run the following:

```
export LD_LIBRARY_PATH=/opt/VRTSsfmcs/asa11/lib32:$LD_LIBRARY_PATH
/opt/VRTSsfmh/bin/xdbadm -f ./a.sql -c /var/opt/VRTSsfmcs/conf -o
/etc/vx/VRTSsfmcs/.odbc.ini -d SFMdb3 -v
```

Certain views in Veritas Operations Manager are not displayed properly after upgrading Management Server to the 4.1 version (2133867)

After you upgrade Management Server to 4.1, certain views in Veritas Operations Manager are not displayed properly.

Workaround:

To display the views correctly, you must clear the browser cache after you upgrade Management Server to version 4.1.

In Internet Explorer, you can configure the temporary Internet files settings to avoid this problem.

To configure the temporary Internet files settings in Internet Explorer:

1 Select **Tools > Internet Options**.

2 In the **General** tab of the **Internet Option** dialog box , under **Temporary Internet Files Section** click **Settings**.

3 Choose the **Every time visit to the page** option and click **OK**.

4 In the **Internet Options** dialog box, click **OK**.

Pagination issue is observed in the Host table of Business entity overview page (2369071)

This issue is observed when you have created a Virtual Business Service with a large number of managed hosts. On the business entity overview page, in the **Servers** tab, the **Hosts** table does not display the hosts correctly. The first page displays the data correctly; however, when you click on the subsequent pages, only blank table without any record is displayed.

Workaround:

On the right upper corner of the **Hosts** table, click **Table Tasks** > **Settings**. On the **Table Settings** page, for the **Rows Per Page** field, select **Show All**.

Now instead of displaying the records across multiple pages, Veritas Operations Manager shows all records in the first page itself.

Uninstalling Management Server removes the managed host package from a Storage Foundation for Windows host

When you uninstall Veritas Operations Manager Management Server from a Storage Foundation for Windows host, the managed host package is removed from the host. So, you cannot add the host to another Management Server domain.

Workaround:

Install Veritas Operations Manager host management on the host. After installation, you can add the host to a Management Server domain.

VMware virtual machine storage mapping information is not populated if the virtual machine name contains a single quote (2510591)

This issue is applicable to VMware virtual machines discovery in Veritas Operations Manager. For any virtual machine that contains a single quote in its name, the virtual machine disk (VMDK) information is not listed in the **Storage Mapping** tab on the overview page of virtualization servers.

There is no workaround for this issue.

Veritas Operations Manager displays stale application status (2564572)

This issue occurs with the virtual machines where Symantec ApplicationHA is configured to monitor applications. In ApplicationHA, if the virtual machine auto-recovery is configured, the virtual machine is restored if the application being monitored fails to start after a configurable number of attempts. If the virtual machine auto-recovery is triggered, the last successful virtual machine snapshot is restored from the backup. It also restores the applications running on the virtual machine. However, Veritas Operations Manager fails to discover the restored application status, and continues to display the application as faulted.

Workaround:

To display the current application status, refresh the Veritas Operations Manager console.

Mountpoint may appear as garbled characters, if encoding is not supported (2377238)

For Japanese locale, Veritas Operations Manager supports discovery in three native encodings: shiftjis on Windows, eucJP on UNIX, and utf8 on UNIX. If the mountpoint is created using any other encoding, Veritas Operations Manager cannot discover it properly and the mountpoint may appear as garbled characters in the Veritas Operations Manager console.

Manual refresh of HMC server and VMware VirtualCenter server required after migration of virtual machines (2605533)

This issue is applicable to VMware vCenter Server and HMC configurations in Veritas Operations Manager. It is observed when you migrate a VMware virtual machine from one ESX server to another ESX server (both servers are under the same VMware vCenter Server), or an LPAR virtual machine from one LPAR server to another LPAR Server (both LPAR servers are under same HMC).

Post migration, the changes are not reflected immediately on Veritas Operations Manager console. The changes are reflected only after the scheduled automatic scan is performed.

Workaround:

You need to manually refresh the configuration to see the changes.

To manually refresh the configuration:

1. Go to **Settings > Virtualization Management**.
2. Select the HMC server or VMware VirtualCenter server.
3. Click **Actions > Refresh Configuration**.

Microsoft Exchange Server 2007 to VCS service group correlation is not present in the first discovery cycle of Veritas Operations Manager (2604162)

In the first discovery cycle of Veritas Operations Manager, the correlation between the Microsoft Exchange Server and the VCS service group is not complete, and no data is available.

Workaround:

Two options are available to resolve the issue:

- Perform the host refresh from the Veritas Operations Manager console. Here, the managed host has VCS and Exchange Server installed on it.

- Wait until the next discovery cycle, which is approximately six hours.

VMware virtualization discovery fails if the vCenter server uses non-default HTTPS port (2611025)

By default, the VMware vCenter Server uses port number 443 for HTTPS protocol, and port number 80 for HTTP protocol communication. But, if a non-default port is used, the VMware virtualization discovery may fail.

Workaround

To discover the vCenter Server with the non-default port number, you need to use the following format:

MYvCenter.example.com:<non-default port>

For example, **MYvCenter.example.com:65535**

Lack of support for managed host upgrade from version 2.x to 4.1 with the Management Server version 4.1 (2587766, 2604312)

The following issues are observed when you add the 2.x managed hosts to 4.1 Management Server:

- **When you add a 2.x managed host to the 4.1 Management Server, it is not displayed with the correct version on the Host Management page of Veritas Operations Manager console (2587766)**
  This issue is applicable to the 2.x managed host that is added to the Veritas Operations Manager Management Server, which is running versions later than 2.0. If you upgrade the managed host and the Management Server to version 4.x, the added hosts are not updated with the correct versions in the Veritas Operations Manager console, and the following error is displayed:
  vxconfigd is not running on client host.
  The Veritas Operations Manager displays managed host with 2.x version though they are already upgraded to version 4.x.
- **2.0 managed hosts are added successfully, but they are not displayed on the Host management page of the Veritas Operations Manager console (2604312)**
  When you try to add or upgrade a 2.0 managed host to the 4.1 Management Server, it is not displayed under **Settings** > **Host Management** page of Veritas Operations Manager console.

Workaround:

Before upgrading the managed host, remove the managed host from the Management Server. Upgrade the managed host manually to 3.x, or 4.x, and then add it to Veritas Operations Manager Management Server.

Error in installing add-ons after upgrading certain Management Server-HA setups to Veritas Operations Manager 4.1 (2603669)

If you upgrade Management Server to Veritas Operations Manager 4.1 in a Management Server-HA setup, that has /etc/default/.sfm_resolv_ha.conf file on it and you try to install Veritas Operations Manager 4.1 add-ons on Management Server, you get the following error message:

```
Failed to perform the operation.

Operation failed for one or more hosts.

Host = hostname

Host Error = Host not configured to the SFM CS
```

Workaround:

You need to remove `/etc/default/.sfm_resolv_ha.conf` file from Management server, if it exists and then update the value of *mh_hostname* entry in files.

To update the value of *mh_hostname*:

1. Log on to one of the managed hosts, and copy the value of *mh_hostname* entry from the `/etc/default/sfm_resolv.conf` file.
2. Modify the `/etc/default/sfm_resolv.conf` file on Management Server. Update the value for *mh_hostname* entry in the file with the value retrieved in step #1.
3. Modify the `/var/opt/VRTSsfmh/domain.conf` file on master node. Update the value for *mh_hostname* entry in the file with the value retrieved in step #1.
4. Restart xprtld and then run following commands:
   - `/opt/VRTSvcs/bin/hares -offline SFM_Services_XPRTLDD -sys master_node`
   - `/opt/VRTSvcs/bin/hares -online SFM_Services_XPRTLDD -sys master_node`
5. Verify the updated *mh_hostname* in the output.
6. Proceed with installation of add-ons.

Coexistence of ApplicationHA Console and Veritas Operations Manager Management Server in the ApplicationHA Console upgrade scenario (2581661)

This issue is observed for the coexistence scenario of ApplicationHA Console (Symantec ApplicationHA 5.1 SP2 or Symantec ApplicationHA 6.0) and the Veritas Operations Manager Management Server version 3.1.*x*. When you upgrade the ApplicationHA console, the `VRTSsfmh` package is also upgraded. As a result, there is a version mismatch between the `VRTSsfmh` package and `VRTSsfmcs` package. Since the `VRTSsfmcs` package is at a lower version, it is incompatible with the `VRTSsfmh` package. This results in broken functionality of Veritas Operations Manager Management Server.

Workaround:

You need to upgrade Veritas Operations ManagerManagement Server to version 4.0 RU1, or later.

Managed host issues

The following issues relate to host management.

Managed hosts stop communicating with Management Server after Veritas Cluster Server is installed (2341920)

After Veritas Cluster Server is installed, upgraded, or removed from a managed host that has the `VRTSsfmh` package, the managed host stops communicating with Management Server. This issue occurs because the local host credentials for the managed host are corrupted when Veritas Cluster Server is installed, upgraded, or removed.

Workaround:

Stop the XPRTLD component, delete the local host credentials for the managed host, and then restart the XPRTLD component using the following commands:

On a UNIX host:

```
/opt/VRTSsfmh/adm/xprtldctrl stop

rm -rf /var/opt/VRTSsfmcs/sec/root

/opt/VRTSsfmh/adm/xprtldctrl start
```

On a Windows host:

```
net stop xprtld
```

```
rd /s C:\ProgramData\Symantec\VRTSsfmh\sec

net start xprtld
```

Veritas Operations Manager creates new certificates when you restart XPRTLD.

Cannot add a managed host with pure IPv6 address to Management Server that supports IPv4 and IPv6 (2137308)

If you install Management Server on a computer that supports both the IPv4 and the IPv6 network addresses, and configure it using a fully qualified domain name, you cannot add a managed host that has a pure IPv6 network address to this Management Server.

Workaround:

To avoid this issue, you must configure Management Server using only the hostname. Make sure that the `/etc/hosts` file in the `/etc` directory also contains the IPv6 address and hostname.

Issue related to upgrading the managed hosts (from 3.*x* to 4.1) that have LUNs from IBM XIV storage array (2367519)

This issue is related to all managed hosts having IBM XIV enclosure connected to them. When you upgrade the managed hosts from version 3.*x* to 4.1, on the Veritas Operations Manager console, two entries are displayed for the same enclosure. The first entry is a dangling object, which has no association with any of the objects. The other entry has Disk, LUNs, array port , and the initiators associations setup, and is reported correctly.

It is to protect the deletion information for the shared objects.

Workaround:

After upgrading the managed host to Veritas Operations Manager 4.1, the discrepancy of dangling object is automatically cleaned up by the scheduled run of a stored procedure. It runs at 3:00 AM every morning on the Management Server.

Exchange service group is not listed in the Exchange Servers table (1976615)

After you add a host that has an Exchange Server installed in the high availability environment to Management Server, the Exchange service group is not discovered. This issue does not get resolved even after you perform a refresh host operation.

Workaround:

You need to refresh the database family.

To refresh the Veritas Operations Manager database family

- Run the following command:

```
/opt/VRTSsfmh/bin/mh_ctl.pl --family DB --refresh
```

Quick I/O cache value is not enabled after performing the storage provisioning operation on AIX managed hosts (2131183)

If you use a VxFS file system-based storage provisioning template on which the Quick I/O cache (CQIQ) value is set as 'Yes' to provision storage on AIX managed host, the storage provisioning operation is successfully completed. However, cache I/O does not get updated appropriately. The 'qio_cache_enable' value in `vxtunefs` output remains '0'.

Workaround:

On AIX platform, the tune VxFS parameters are not set properly. You can use the `vxtunefs` from the managed node.

Information on the disks and the LUNs for a Windows host where Storage Foundation for Windows is newly installed are not displayed on the console (2345887)

Information on the disks and the LUNs for a Windows host on which Storage Foundation for Windows is newly installed are not displayed on the console. This happens because the information that are discovered by the Storage Foundation agent is deleted by the Logical Device Manager (LDM) agent.

Workaround:

After restarting the host following the installation of Storage Foundation for Windows, select the host from **Settings** > **Host Management** in the Veritas Operations Manager and refresh it twice.

Cannot replace or recover a disk removed from a UNIX host (2317671)

Using the Veritas Operations Manager Add-on for Storage Foundation Administration, you can replace or recover a faulted disk. But, using this add-on, you cannot replace or recover a disk that is removed using the `rmdisk` command on a UNIX host.

Workaround:

To replace or recover a disk that is removed using the `rmdisk` command on a UNIX host, use the CLI, Veritas Enterprise Administrator console, or the Add-on for Storage Foundation Administration for UNIX.

After the replace disk operation, the faulted disk status remains as replaceable (2353612)

In Veritas Operations Manager, after you perform Replace Disk operation, the faulted disk status does not change. It still displays the state as **in Use (Replaceable)**. The state will change if the disk is removed, or initialized.

Workaround:

You need to use the command-line interface (CLI), Veritas Enterprise Administrator console, or the Storage Foundation Administration for Unix Add-on to perform this operation.

Thin LUNs on the hosts that run Storage Foundation for Windows 5.1 SP1 are not discovered as thin (2513466)

In Veritas Operations Manager, the thin LUNs on the hosts that run Storage Foundation for Windows version 5.1 SP1 are not discovered as thin.

Workaround:

Download the hot fix for Storage Foundation for Windows version 5.1 SP1 from the following location, and run it on the host:

https://sort.symantec.com/patch/detail/4697

After the successful installation, restart the host.

CPU count incorrect for managed hosts on Windows Server 2003 (2437565)

The CPU count that is displayed for Windows Server 2003 managed hosts on the Veritas Operations Manager console, does not match the actual CPU count on the host. The figure that is displayed is the count of cores and not the count of physical CPUs.

The issue occurs due to a Windows Server 2003 operating system issue. For more information, visit the Microsoft Web site.

http://support.microsoft.com/kb/932370

Exchange Server information is not displayed after managed host upgrade to 4.1 (1976615)

When you upgrade a managed host that has Exchange Server to version 4.1, the Exchange Server information is no longer displayed in the Veritas Operations Manager console.

Workaround:

You need to unconfigure the host and then reconfigure it from Veritas Operations Manager console.

Remote switch operation fails between secure clusters (2530605)

If you try to switch global service groups between clusters, that are configured in secure mode, the operation fails and following error message is displayed:

```
VCS WARNING V-16-1-50824

Command (hagrp -switch servicegroupname
targetsystemname targetclustername failed

At least Group Operator
privilege required on remote cluster targetclustername
```

Workaround:

Veritas Operations Manager uses the Veritas Storage Foundation Messaging Service to run Veritas Cluster Server commands. By default, this service runs in the Local System account context. Configure this service to run in the Domain Administrator account context and then perform the switch operation. Change the service account on each of the managed hosts in the clusters.

To change the service account context:

1. Open the Windows Services MMC snap-in.
2. Right-click **Veritas Storage Foundation Messaging Service** and then click **Properties**.
3. Click the **Log On** tab and do the following:
   - Click **This account**, click **Browse**, and in the **Select User** dialog box, specify a user account that has Domain Administrator privileges.
   - Click **OK**.
4. Type the user account password in the **Password** and **Confirm password** fields. Click **OK**.
5. Proceed with the service group operations.

Adding an agentless host to a Linux-based control host fails

If a control host is Linux-based and does not have the 32-bit `libgcc` package installed on it, you cannot add agentless hosts to the control host.

Workaround:

Install the 32-bit `libgcc` package on the control host.

Add host operation fails for HP-UX managed hosts (2601265)

In the Veritas Operations Manager, if you try to add the HP-UX managed host through agent, sometimes the operation fails. The following error message is displayed:

CS host is not reachable from managed host.

Workaround:

Restart the XPRTLD process on the managed host that you want to add, and then add the host.

Addition of agentless Solaris managed host may fail for some arp configurations (2581177)

When you try to add the Solaris managed host using the agentless mechanism in Veritas Operations Manager, the operation may fail for some arp configurations. It happens when the valid MAC address is not found at either of following places:

- prtconf -pv
- arp 'hostname'

Workaround

No workaround is available.

Agentless discovery issues

The following issues relate to the agentless discovery of hosts.

Agentless configuration of hosts using IPv6 addresses fails (2414252)

Configuration of agentless hosts using IPv6 addresses does not work. You must specify the host name or IPv4 address of the host that you want to configure using agentless discovery.

Removal of agentless host while refresh is in progress results in bad configuration (2480954)

Removal of an agentless host while the refresh operation is in progress, results in a bad configuration state where the host reappears after the refresh operation is complete, but you cannot subsequently perform refresh operations on it. Also periodic discovery will not occur for these hosts. You must remove the host again from the Veritas Operations Manager console to clean up the configuration.

Incorrect error message displayed when configuring agentless UNIX hosts without enough free space (2428471)

If you configure a UNIX host using agentless discovery and the host does not have enough free space in the /var/tmp directory, or if the /var/tmp directory on the host is not writable by the user configured for agentless discovery, then the host configuration fails as expected. However, the error message displayed does not identify the cause. The operation fails with the "Cannot configure the host using SSH" error message.

Agentless configuration of Windows hosts running non-English locale fails (2484139)

If you configure a Windows host using agentless discovery running a non-English locale, the configuration fails with the "Failed to determine free space on the remote host" error message. You cannot configure Windows hosts running non-English locales using agentless discovery. These hosts must be configured using an agent.

Configuration fails for agentless host with user name containing DBCS characters (2427619)

If you configure a host using agentless discovery that has a user name containing characters from Double Byte Character Set (DBCS), the configuration fails. This generally occurs with user names for locales other than English.

Timezone and GMT offset information not displayed for agentless hosts (2294669)

The timezone and GMT offset information are not displayed for hosts that are configured using agentless discovery.

fstab information displayed incorrectly for file systems on Linux agentless host (2418023)

Information about whether file systems are in fstab is displayed incorrectly for Linux hosts configured using agentless discovery.

Incorrect discovery state displayed for agentless hosts that are refreshed (2578260)

When you refresh an agentless host that is configured under a control host, which is not Management Server, the correct discovery state is not reflected in the **Host Management** view. The **discovery state** column does not change to Refreshing.

There is no workaround for this issue. The issue has no impact on the refresh operation, and the discovery state displays correctly after the refresh.

Agentless discovery fails if a host has volume names, mount point names, or disk label names that contain equals(=) sign(2590669)

Agentless discovery of Windows hosts fails if a host has disk label name, volume name, or file system mount point name containing equals sign(=). If you configure such hosts for agentless discovery in Veritas Operations Manager, no disks, volumes and file systems information is reported for such hosts.

Workaround:

To fix this issue:

1. Change the names of such volumes, mount points, or disk labels to remove the '=' sign.
2. Remove such hosts from Veritas Operations Manager.
3. Re-configure the agentless discovery of the host.

Volume group and logical volume information can be inconsistent, if Volume group is created on shared disks (2567056)

If volume group of a Logical Volume Manager is created on the disk, that is shared on multiple hosts, the Volume group and Logical volume is accessible to all the hosts. As a result, the last configured or discovered Host overwrites the properties of the volume group and logical volume .

Failed EMC PowerPath paths are not displayed for agentless Windows 2008 hosts (2611064)

On the **Paths** tab for a disk's view, the failed EMC PowerPath paths are not displayed for agentless Windows 2008 hosts. Only the paths that are enabled are shown.

Storage Provisioning Add-on issues

The following issues relate to the Storage Provisioning Add-on.

A volume is migrated to any available enclosure if no target array is specified (2143010)

If you do not specify the enclosure while performing the volume migration operation, the view that lists the status of volume migrations displays no value in the **Target array** column. However, the volume migration task is performed successfully by selecting any available enclosure.

Storage Insight Add-on issues

The following issues relate to the Storage Insight Add-on.

The vxlist utility does not display the information on the physical disks for the LUNs (2219286)

If a LUN is masked to the host that is added to multiple Management Servers, the `vxlist -l lun` command on the host does not get the information on the physical disks (PDEVs).

Cannot configure an EMC CLARiiON enclosure on a Windows control host using a security file (2221574)

You cannot configure an EMC CLARiiON enclosure on a Windows control host using a security file.

Workaround:

To configure an EMC CLARiiON using a security file, choose a UNIX control host instead of a Windows control host.

NetApp enclosures are not discovered after the Storage Insight Add-on is upgraded to version 4.1 (2492978)

The NetApp enclosures that are configured using the Storage Insight Add-on version 4.0 are not discovered after the add-on is upgraded to version 4.1.

Workaround:

Remove the configurations for the NetApp enclosures. Configure the enclosures again using the Storage Insight Add-on version 4.1.

VBS Availability Add-on issues

The following issues relate to the Veritas Operations Manager Add-on for Virtual Business Services:

Veritas Operations Manager does not validate if the cluster node is managed by the Management Server during the VBS start operation (2566050)

When you perform the Virtual Business Service (VBS) start operation, Veritas Operations Manager does not check whether Management Server manages the cluster node. Veritas Operations Manager brings the service group online using the `-any` option on the available systems for that service group.

Workaround:

Although there is no functional loss, it is recommended that you add all the cluster nodes to the Management Server domain.

Scripting Add-on issues

The following issues relate to the Scripting Add-on.

Post Management Server upgrade, the Scripting Add-on uses the current time of the Management Server to run the previous scripts

This issue is related to the Scripting Add-on and the upgrade of Veritas Operations Manager Management Server to version 4.1. Post Management Server upgrade, if you try to reschedule the old scripts with the new time, the Scripting Add-on uses the current time of the upgraded Management Server to run the scripts.

Workaround:

Upgrade the Scripting Add-on to version 4.1.

Scripting Add-on runs the Perl scripts successfully only when the Perl executable installed with Veritas Operations Manager is used (2589815)

For the Perl scripts, it is recommended that you use the Perl executable that is installed with Veritas Operations Manager. For the Windows platforms, it is the default for scripts with the `.pl` extension. For UNIX platforms, using the Perl executable from other paths may result in errors if the script does not handle the Perl 5 library path properly. This recommendation does not affect shell, bat, or other executable scripts that are available with the Scripting Add-on.

Workaround:

To run the script successfully, ensure that the Perl executable location is specified as follows:

```
#!/opt/VRTSsfmh/bin/perl
```

Other issues

This section lists additional issues that cannot be categorized in the rest of the Veritas Operations Manager known issues sections.

Duplicate entries for the disks that are part of a virtual machine (2481982)

If a virtual machine that runs Storage Foundation has non RDM disks on it and the enclosure-based naming scheme is enabled for the disks, Veritas Operations Manager displays the disks twice on the **Hosts** > **Disks** tab. This issue occurs because the disks are discovered by VxVM and the operating system on the enclosures.

Workaround:

Change the disk naming scheme to c#t#d#.

Composite business entities do not inherit all user configurations done for the child business entities (2349751)

In Veritas Operations Manager, a composite business entity inherits some of the objects and the corresponding configurations of its child business entities. It does not inherit the following:

- Start and stop order of the service groups that were configured using the Veritas Operations Manager Virtual Business Services Availability Add-on

- Virtual machine auto start and stop settings for the business entity that were configured using the Veritas Operations Manager Virtual Business Services Availability Add-on
- LDom capacity planning settings that were configured using the Veritas Operations Manager LDom Capacity Management Add-on

Workaround:

You need to re-configure these settings for the composite business entity.

vomsc command does not work properly in Management Server HA-DR setup (2605531)

The `vomsc` command does not work properly and displays the incorrect status of services running on Management Server, if the Management Server has High Availability and Disaster Recovery installed.

Workaround:

You can use following commands to stop and start the Web server:

- To stop the Web server, run the following command:
  `/opt/VRTSvcs/bin/hares -offline SFM_Services_WEB -sys` *`active node name`*
- To start the Web server, run the following command:
  `/opt/VRTSvcs/bin/hares -online SFM_Services_WEB -sys` *`active node name`*

Appendix A

Getting help

This appendix includes the following topics:

Veritas Operations Manager on the Web

For comprehensive, up-to-date information about Veritas Operations Manager, visit the Symantec Web site:

http://go.symantec.com/vom

Getting help

If an issue arises while you use the products, refer to the product documentation and online help. If necessary, report it to Symantec.

For technical assistance, visit

www.symantec.com/enterprise/support/index.jsp

This site provides access to resources such as TechNotes, product alerts, software downloads, hardware and software compatibility lists, and the customer email notification service. Use the Knowledge Base Search feature to access additional product information, including current and past releases of product documentation.

Using the product documentation

The following guides provide information about Veritas Operations Manager:

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

For complete host operating system and system resource specifications, as well as any known limitations or issues 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 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/TECH157641

Commenting on product documentation

Submit comments about the product documentation to the following email address:

storage_management_docs@symantec.com

Please include the following information with your documentation comments:

- The title and product version of the guide you are commenting on
- The topic (if relevant) you are commenting on
- Your comment
- Your name