

# Veritas™ Operations Manager 6.0 Release Notes

June 2014



# 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: 6.0

Documentation version: 6.0 Rev 2

## Legal Notice

Copyright © 2014 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, Veritas, Veritas Storage Foundation, CommandCentral, NetBackup, Enterprise Vault, and LiveUpdate are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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

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

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

Symantec Corporation  
350 Ellis Street  
Mountain View, CA 94043

<http://www.symantec.com>

# Technical Support

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

Symantec's support offerings include the following:

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

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

[www.symantec.com/business/support/](http://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/](http://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/](http://www.symantec.com/business/support/)

## Customer service

Customer service information is available at the following URL:

[www.symantec.com/business/support/](http://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](mailto:customercare_apac@symantec.com)

Europe, Middle-East, and Africa [semea@symantec.com](mailto:semea@symantec.com)

North America and Latin America [supportolutions@symantec.com](mailto: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](mailto: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	
Overview of this release .....	13
About Veritas Operations Manager .....	13
What's new in Veritas Operations Manager 6.0? .....	14
New product interface .....	14
Multi-Site Management .....	14
Storage area network (SAN) fabric and switches discovery .....	14
Near real-time update of VMware virtual machine states .....	15
IBM System Storage SAN Volume Controller enclosure discovery using Storage Insight Add-on .....	15
Online and offline product Help .....	15
Ability to set timeout for the recovery plan .....	15
Hitachi Dynamic Tier (HDT) discovery supported for the Hitachi HDT capable enclosures .....	16
Patch Installer Add-on .....	16
Support for deduplication of file systems on managed hosts .....	16
Support for monitoring selected objects as a Business Application .....	16
Report on NAS Pool allocation .....	17
Support for collecting and viewing audit information .....	17
Support for monitoring usage of thin pools .....	17
Ability to configure the monitoring of applications by VCS .....	18
Ability to configure performance metering on Windows hosts .....	18
Ability to configure performance metering on EMC VNX (Block) enclosure .....	19
Ability to create an Organization to group objects in a perspective to achieve multi-tenancy .....	19
Ability to assign permissions to user groups on perspectives, Organizations, or objects .....	19
Ability to access the information discovered by Veritas Operations Manager using REST Web services API .....	20
Support for new Storage Foundation operations in Veritas Operations Manager .....	21
Deprecated features in Veritas Operations Manager 6.0 .....	22

	Veritas Operations Manager add-ons merged with Veritas Operations Manager Management Server .....	23
	Issues fixed in the Veritas Operations Manager 6.0 release .....	23
	About upgrading the Management Server .....	24
Chapter 2	System requirements .....	25
	Operating system requirements .....	25
	Third-party required libraries .....	25
	32-bit SNIA Common HBA API required on Windows hosts .....	25
	System resource requirements .....	26
	About space estimation for data logs .....	27
	About the frequency of managed host, enclosure and switch information discovery .....	30
	Web browser requirements .....	32
	Network and firewall requirements .....	32
	Internet Protocol version requirements .....	34
	About the consumption of the managed host components .....	35
Chapter 3	Software limitations .....	36
	Veritas Operations Manager 6.0 managed host not supported on AIX in Network Installation Manager .....	37
	No coexistence of managed host and CommandCentral Storage Management Server .....	37
	Live statistics for initiators are not supported on HP-UX .....	37
	Volume layout not discovered for LDM-managed volumes mounted without a drive letter .....	38
	Backup and restore limitations in Veritas Operations Manager 6.0 .....	38
	Veritas Operations Manager does not support the discovery of LDOMs and Zones together on the same host .....	38
	Deployment-related limitations .....	38
	Windows Management Server high availability configuration limitations .....	39
	Solaris Zones virtualization support limitations .....	39
	Discovery limitations for virtualization support .....	39
	VCS configuration check reports violations only if at least one node in the cluster is running Symantec Cluster Server .....	39
	Limitations related to the correlation between the disks and the disk groups .....	40
	No support to online and offline multiple virtual machines using the Virtual Business Service start and stop operations (2177421) .....	40



Virtual Business Service start operation does not validate the service group's resource criticality (2169223) .....	40
Discovery of VMware VirtualCenter server or ESX server is not case-sensitive (2567318) .....	41
Core density may not get calculated properly on HP-UX11iv2 hosts .....	41
Tier information is not displayed for some devices in a FAST managed storage group (2795204) .....	41
IBM System Storage DS enclosure discovery is not supported through HiCommand Server 7 in Veritas Operations Manager (2708346) .....	41
For EMC Celerra and VNX file enclosures, NAS file system to Storage Pool correlation is not available (3339001) .....	42
CIFS shares from NetApp and Celerra arrays that are mapped to a Windows host are not discovered .....	42
Performance charts may not be displayed for EMC Symmetrix array ports and adapters (3247859) .....	42
Inconsistency in storage calculation is observed for unclaimed VPLEX extents (2844028) .....	42

## Chapter 4

Known issues .....	43
Management Server issues .....	43
Managed hosts with duplicate virtual machine identifiers are automatically removed by Veritas Operations Manager (3340537) .....	43
Delayed discovery of VMware VirtualCenter server by Control Hosts in Veritas Operations Manager (2342314) .....	44
Authentication broker crashes while performing LDAP authentication (2017319) .....	44
XPRTLD daemon fails when Veritas Operations Manager starts because of the corrupt AT pem files in the <code>VRTSsfmh</code> package (2145925) .....	45
Status of all SF Manager 2.x hosts is shown as healthy on an upgraded Veritas Operations Manager 6.0 setup (2009372) .....	47
Uninstalling Management Server removes the managed host package from a Storage Foundation for Windows host .....	48
Veritas Operations Manager displays stale application status (2564572) .....	48
Manual refresh of HMC server and VMware VirtualCenter server required after migration of virtual machines (2605533) .....	48

Performance metering of a VMware ESX server may not work properly after failover (2814844) .....	49
For VMware virtual machine, the virtual storage correlation is not functional if a SCSI controller of non-default type is used (3056561) .....	49
ESX servers not able to access an RDM disk associated with a shared datastore might cause failed discovery of RDM disk by Veritas Operations Manager (2736293) .....	50
Occasionally the Management Server console shows blank views during navigation or blank wizard panels for the operations (3333313) .....	50
Erroneous managed host status reported in Veritas Operations Manager high availability (HA) environment (2780631) .....	50
Cannot search for some objects using size as criteria (3216639) .....	51
OS version name shown for Windows hosts varies in English and non-English system locale (3271960) .....	51
Information on running tasks is accurate only for managed hosts 6.0 and later (3077899) .....	51
Sometimes Internet Explorer displays a security warning when you navigate between pages in the console (2999524) .....	51
Managed hosts previous to version 5.x are not listed for storage provisioning and volume migration .....	52
Managed host issues .....	52
Issue related to upgrading the managed hosts (from 3.x to 6.0) that have LUNs from IBM XIV storage array (2367519) .....	52
Quick I/O cache value is not enabled after performing the storage provisioning operation on AIX managed hosts (2131183) .....	52
Thin LUNs on the hosts that run Storage Foundation for Windows 5.1 SP1 are not discovered as thin (2513466) .....	53
CPU count incorrect for managed hosts on Windows Server 2003 (2437565) .....	53
Remote switch operation fails between secure clusters (2530605) .....	53
Add host operation fails for HP-UX managed hosts (2601265) .....	54
Some performance charts are not available for VMware ESX server version 4.1 managed through vCenter server 5.0 (2800239) .....	54
Unable to view performance graphs for VxVM disk and volume on Windows platform (3054870) .....	54

Cannot add a managed host to Management Server using the IPv6 address of the host (2816487) .....	55
Incorrect statistics returned by DMP if Storage Foundation version is prior to 5.0 MP3 (2796418) .....	55
Create disk group operation fails when triggered from slave node in a clustered configuration (3196104) .....	55
On HP-UX managed hosts, the path initiator and array port information is not displayed for some disks (3073128) .....	55
Violated license deployment policies are not displayed correctly (3342986) .....	56
Agentless discovery issues .....	56
Agentless configuration of hosts using IPv6 addresses fails (2414252) .....	56
Agentless configuration of Windows hosts running non-English locale fails (2484139) .....	56
Configuration fails for agentless host with user name containing DBCS characters (2427619) .....	56
Volume group and logical volume information can be inconsistent, if Volume group is created on shared disks (2567056) .....	56
Storage Insight Add-on issues .....	57
After the first discovery of IBM SVC array, manual refresh of putty cache may be required (3114164) .....	57
For locally replicated EMC Symmetrix LUNs, last synchronization time is available only for SYMCLI version 7.4 or later (3249430) .....	57
Manual discovery of Symmetrix enclosure is required when SYMCLI version is upgraded on the Storage Insight add-on discovery host (3289628) .....	58
Cannot configure an EMC CLARiiON enclosure on a Windows control host using a security file (2221574) .....	58
NetApp enclosures are not discovered after the Storage Insight Add-on is upgraded to version 6.0 .....	58
Performance metering of enclosures may not work properly after failover (2814844) .....	59
Performance tab is not displayed if vFiles are discovered for NetApp enclosures (33342029) .....	59
Information on FAST managed storage groups for EMC Symmetrix VMAX enclosures is not discovered periodically (2842124) .....	59
Array group information is incorrect in Enclosure Storage Summary chart for Hitachi arrays (2820150) .....	60
Password file option does not work while configuring HP EVA enclosures on Windows hosts (2757601) .....	60

	EMC Celerra enclosure details are not discovered for users with read-only access rights, and Imported Administrator or Operator role .....	60
	Network File System on Solaris cannot be discovered if the Fully Qualified Host Name is used in vfstab file but not used for mounting the file system (2747735) .....	61
	Virtual Business Service issues .....	61
	Veritas Operations Manager does not validate if the cluster node is managed by the Management Server during the VBS start operation (2566050) .....	61
	Storage Insight SDK Add-on issues .....	61
	Edit and Test operations on Storage Insight Plug-in are not supported using Internet Explorer on 64-bit Windows hosts (2826079) .....	61
	Other issues .....	62
	Duplicate entries for the disks that are part of a virtual machine (2481982) .....	62
	Symantec ApplicationHA Console single sign-on breaks after Veritas Operations Manager 6.0 managed host installation or upgrade on ApplicationHA hosts .....	62
	Unable to configure Management Server with a user name in Russian language using Firefox browser .....	62
	Coexistence of ApplicationHA Console 6.0 and Veritas Operations Manager 6.0 not supported (2739241) .....	63
	Resource attributes not discovered for RVGPrimary Resource .....	63
Chapter 5	Documentation addenda and errata .....	64
	Online help add-on .....	64
Appendix A	Getting help .....	65
	Veritas Operations Manager on the Web .....	65
	Getting help .....	65
	Using the product documentation .....	65

# Overview of this release

This chapter includes the following topics:

- [About Veritas Operations Manager](#)
- [What's new in Veritas Operations Manager 6.0?](#)
- [Deprecated features in Veritas Operations Manager 6.0](#)
- [Veritas Operations Manager add-ons merged with Veritas Operations Manager Management Server](#)
- [Issues fixed in the Veritas Operations Manager 6.0 release](#)
- [About upgrading the Management Server](#)

## About Veritas Operations Manager

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

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

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

A typical Veritas Operations Manager deployment consists of the following:

- Management Server

- Managed hosts

A Veritas Operations Manager deployment may also discover the following:

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

## What's new in Veritas Operations Manager 6.0?

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

### New product interface

The new Management Server console provides ease of navigation and a perspective driven, role-based approach for efficient management of different storage and clustering assets across your data center. Depending on the type of the object and the nature of the operation, you can use the provided perspectives – Storage, Availability, Virtualization, and Server. You can perform a variety of tasks at the perspective-level. For example, group similar objects in an Organization, assign permissions, perform search using one or more parameters, create and save the search queries, use Global Dashboard to view the overall status of the data center, view solutions and reports and so on. The Organizations can also be used in multi-tenant environments where the objects are accessible to specific users based on their roles and the assets they manage in the data center.

### Multi-Site Management

Multi-Site Management facilitates uniform configuration and management of campus clusters across Symantec Storage Foundation and Cluster Server objects. Using the Veritas Operations Manager Management Server console, you can tag the site name to the enclosure and to the cluster's hosts. Multi-Site Management supports campus cluster, replicated data cluster (RDC), and mixed mode (campus cluster and RDC).

### Storage area network (SAN) fabric and switches discovery

Using the Fabric Insight Add-on, you can discover Cisco and Brocade SAN switches that are configured in the Management Server domain. For Cisco switch discovery, Simple Network Management Protocol (SNMP) is used. For Brocade switch discovery, you can use either HTTP communication or Brocade Network Advisor (BNA).

## Near real-time update of VMware virtual machine states

Any change in the state of a VMware virtual machine in the Management Server domain is now updated in Veritas Operations Manager database in near real-time. You need to configure the Management Server as the SNMP trap receiver and add VMware vCenter Server to the Management Server. When a virtual machine's state changes, the managing VMware vCenter Server generates the corresponding SNMP trap. The SNMP trap is then received by the Management Server using the `xtrapd` daemon, which updates the database. By default, near real-time update of VMware virtual machines is enabled.

## IBM System Storage SAN Volume Controller enclosure discovery using Storage Insight Add-on

The Storage Insight Add-on now supports the deep discovery of IBM System Storage SAN Volume Controller (SVC) and IBM Storwize V7000 enclosures (only Block Device).

## Online and offline product Help

Veritas Operations Manager help is now provided in two modes – offline and online. The offline mode requires you to first download and install the Veritas Operations Manager Help add-on on the Management Server. For the online mode, the help content is hosted on the web, and is accessed directly when you launch the product help.

Visit Symantec Operations Readiness Tools (SORT) to download the Veritas Operations Manager Help add-on:

<https://sort.symantec.com/vom>

## Ability to set timeout for the recovery plan

While executing a recovery plan using Veritas Operations Manager Management Server console, you can specify the duration (in minutes) you want to wait while the Virtual Business Service, the custom script, or the service group tasks run. If any task is not completed in the specified time, Veritas Operations Manager marks the task as failed.

## Hitachi Dynamic Tier (HDT) discovery supported for the Hitachi HDT capable enclosures

For HITACHI enclosures, dynamic tiering related information is discovered by Storage Insight Add-on if the HITACHI enclosure has dynamic tier enabled thin pools.

## Patch Installer Add-on

Patch Installer Add-on adds the capability of using the Management Server console to download and install supported Symantec Storage Foundation High Availability (SFHA) updates on managed hosts that require them. Supported updates are those that have been configured as deployable by Veritas Operations Manager. The Management Server console shows which updates are deployable.

This release of Patch Installer Add-on (version 1.0) supports installing SFHA updates for Windows only, not for UNIX/Linux.

## Support for deduplication of file systems on managed hosts

The deduplication feature in Storage Foundation enables customers to use file system deduplication to optimize existing primary storage. Enabling deduplication at the file system layer results in storage savings and avoids complex and expensive appliances typically associated with file deduplication.

You can now use Veritas Operations Manager Management Server console to run deduplication on file systems on managed hosts.

File systems for deduplication must meet the following requirements:

- Storage Foundation 6.0 or later
- Veritas File System (VxFS) disk layout version 9 or later
- Veritas Operations Manager managed host (VRTSsfmh) version 5 or later

Veritas Operations Manager does not support deduplication on Windows file systems.

## Support for monitoring selected objects as a Business Application

The Business Application feature lets you group related storage and cluster objects and monitor their status.

Veritas Operations Manager can discover some applications, such as some database applications, and display information about their related objects. In cases where Veritas Operations Manager is unable to discover an application, you can create a Business Application to represent your application using a base object. For example,



if the application MyApp is the only one that uses a specific disk group, MyAppDG, then MyAppDG can be used as the base object for the MyApp Business Application. Veritas Operations Manager is able to determine all associated objects for that disk group and collect the data for monitoring in the Business Application.

You can select one or more of the following objects when creating Business Applications:

- Hosts
- Volumes
- Disk Groups
- Service Groups
- Databases
- Exchange Servers

## Report on NAS Pool allocation

The Storage perspective of Veritas Operations Manager Management Server provides the report on physical storage to pool allocation for the NAS devices (information on Aggregates/Storage Pools of NetApp and Celerra enclosures).

## Support for collecting and viewing audit information

You can use the Management Server console to view audit information collected by Management Server. For audit purposes, Management Server collects information on all activities initiated using the Management Server console. This audit tracking also includes activities which were prevented from being carried out because they were not authorized.

You can also enable advanced authorization settings for Management Server. With this setting enabled, a panel is displayed when an operation is performed so that the user can enter the reason for the operation.

## Support for monitoring usage of thin pools

The Storage Insight Add-on lets you monitor the subscribed and the consumed size of the thin pools on your enclosures. Using the Storage Insight Add-on, you can set high and low threshold levels for the subscribed and the consumed size of the thin pools. When the consumed size of the thin pools reaches the high threshold level, Veritas Operations Manager raises a fault alert to Management Server. The low threshold for the consumed size results in a risk alert. Similarly, when the

subscribed size reaches the low or the high threshold level, Veritas Operations Manager raises a risk or a fault alert, respectively.

You can perform this operation on the following types of enclosures:

- EMC Symmetrix
- EMC CLARiiON
- HITACHI
- IBM XIV
- HP 3PAR
- IBM SVC
- EMC VNX

## Ability to configure the monitoring of applications by VCS

You can use the application configuration feature in Veritas Operations Manager 6.0 to configure monitoring of applications that are running in virtual or physical environment. Veritas Operations Manager uses the VCS application configuration wizard to configure application monitoring.

This feature is enabled only with VCS versions 6.0.1 (Windows), 6.0.2 (Linux) and an agent pack that is installed on VCS versions 6.1.0 (Solaris, AIX), or later versions. In case of Linux and UNIX, ensure that `VRTSvcs wiz` package is installed.

## Ability to configure performance metering on Windows hosts

Using Veritas Operations Manager 6.0 lets you gather performance statistics for Windows hosts. You can also disable performance statistics gathering if required. You can view the performance graphs for the following resources:

- Host
- File system
- Volume
- Disk

Performance charts for disk and volume are available only if they are managed by Storage Foundation (VxVM).

## Ability to configure performance metering on EMC VNX (Block) enclosure

Veritas Operations Manager 6.0 lets you gather performance statistics for EMC VNX (Block) enclosure that is configured using Storage Insight Add-on version 6.0.

If you upgrade from Storage Insight Add-on version 5.0 to 6.0, and if you have EMC VNX (Block) enclosure configured using Storage Insight Add-on version 5.0, then metering for the enclosure is enabled by default.

You can also disable performance statistics gathering if required.

## Ability to create an Organization to group objects in a perspective to achieve multi-tenancy

Using Veritas Operations Manager 6.0, you can create an Organization which is a collection of objects in a perspective that can be secured and managed as a group. Organizations can be created in all perspectives except in the Management Server perspective. The objects within the Organization may or may not represent the physical organization of the objects in the actual data center. Using Organizations you can configure multi-tenant environments and control visibility of the data through scoping.

You can create an Organization using the hosts in the **Server** perspective, using clusters in the **Availability** perspective, using enclosures in the **Storage** perspective, and virtualization servers in the **Virtualization** perspective. **SFHA Licensing** uses the same Organizations as the **Server** perspective.

## Ability to assign permissions to user groups on perspectives, Organizations, or objects

Using Veritas Operations Manager 6.0, you can assign one of the following permissions to the user groups on a perspective, Organization, or on an object.

- Admin
- Operator
- Guest

Operator role is applicable only in the **Availability** perspective.

In terms of objects, in the **Server** perspective, you can assign permissions explicitly on the hosts, in the **Availability** perspective on clusters and service groups, on enclosures in the **Storage** perspective, and virtualization servers in the **Virtualization** perspective.

Permissions on an object are explicitly assigned or inherited from the parent Organization or the perspective.

## Ability to access the information discovered by Veritas Operations Manager using REST Web services API

Veritas Operations Manager 6.0 provides an API that can be accessed over the HTTP protocol using any standard HTTP client. The interface provides the ability to query Veritas Operations Manager discovered data and to manage user-defined attributes for certain object types.

The API can be used for:

- Searching the objects that match specified criteria.
- Retrieving the discovered and extended attributes of objects.
- Defining and setting extended attribute values.

These APIs can be invoked using the XPRCTL component or any other HTTP client like cURL. Following are the supported objects and the perspective to which they belong:

**Table 1-1**

Object	Perspective
Host, disk, disk group, volume, system HBA, exchange server, Virtual Business Services - dependency, Virtual Business Services, databases, database - volume manager, database - volume manager disk, database - volume manager disk group, tablespace, instances, database - file, license, package, and product	Server
Cluster, service group, resource, system, Virtual Business Services - dependency, and Virtual Business Services.	Availability
Enclosure, logical device (LDEVs), port, HBA, replication, RAID group, thin pool, rank, policy, share, vfiler (NetApp) or Virtual Data Mover (VNX or Celerra), NAS Filesystem Replication, physical device (PDEVs), storage volume, fabric, switch, switch chassis, switch port, zone, zone member, connectivity	Storage

**Table 1-1** (continued)

Object	Perspective
Virtualization server, virtual machine, storage mapping, disk, storage pool, cluster, and system HBA.	Virtualization

Operations other than defining and setting extended attributes are not supported currently.

## Support for new Storage Foundation operations in Veritas Operations Manager

Using Veritas Operations Manager 6.0 you can perform the following Storage Foundation operations:

### Disk and disk group operations

- Setting disk usage
- Evacuating disks
- Rescanning disks
- Bringing disks online
- Taking disks offline
- Upgrading disk groups
- Splitting disk groups
- Moving disk groups
- Joining disk groups
- Running or scheduling Trim

### Volume operations

- Moving volumes
- Setting volume usage
- Splitting snapshots
- Starting synchronization of snapshots

### File system operations

- Remounting file systems
- Checking file systems

- Creating file systems snapshots
- Remounting file systems snapshot
- Mounting file system snapshot
- Unmounting file system snapshot
- Removing file systems snapshot

Replication operations

- Configuring Storage Foundation replications
- Adding a Secondary
- Pausing the replication to a Secondary
- Resuming the replication of a Secondary
- Starting replication to a Secondary
- Stopping replication to a Secondary
- Switching a Primary
- Taking over from an original Primary
- Removing a Secondary

## Deprecated features in Veritas Operations Manager 6.0

The following Veritas Operations Manager Management Server features and add-ons are not supported with the 6.0 release of Veritas Operations Manager:

- Veritas Operations Manager Management Server platform support:
  - The Management Server 6.0 is not supported on Solaris platform.
- Veritas Operations Manager add-ons:
  - Package Anomaly Add-on for Veritas Operations Manager
  - Veritas Operations Manager Scripting Add-on
  - LDOM Capacity Management Add-on
  - Storage Foundation Administration for UNIX
  - Storage Foundation Administration for Windows
- Veritas Operations Manager Management Server features:
  - Composite Business Entities

- Composite Virtual Business Services
- Archiving of report output
- Adding secondary authentication broker
- Activity board
- Veritas Enterprise Administrator (VEA) alerts and tasks. In lieu of this, use vom events to create a rule.

## Veritas Operations Manager add-ons merged with Veritas Operations Manager Management Server

The following add-ons are now part of Veritas Operations Manager Management Server:

- Veritas Operations Manager Virtual Business Services Availability Add-on
- Veritas Operations Manager Thin Provisioning Reclamation Add-on
- Veritas Storage Foundation Add-on for Veritas Volume Replicator Bandwidth reporting
- ApplicationHA Add-on
- HSCL Pack 1 Add-on for Management Server

## Issues fixed in the Veritas Operations Manager 6.0 release

[Table 1-2](#) lists the Management Server issues that have been fixed in the Veritas Operations Manager 6.0 release.

**Table 1-2** Management Server issues fixed in Veritas Operations Manager 6.0

Incident	Description
2853154	Upgrade of Management Server in High Availability environment fails with database upgrade errors.
2908023	For virtual business service operations using the Veritas Operations Manager Management Server console, the performance issue (delay in response) of Service Group Order graph page of Veritas Operations Manager console is now resolved.

**Table 1-2** Management Server issues fixed in Veritas Operations Manager 6.0  
*(continued)*

Incident	Description
3012214	Firmware information for Hitachi arrays is not displayed in the Management Server console.
3098688	Unable to delete Fire drill Schedule with localized characters.

[Table 1-3](#) lists the managed host issues that have been fixed in the Veritas Operations Manager 6.0 release.

**Table 1-3** Managed host issues fixed in Veritas Operations Manager 6.0

Incident	Description
N.A.	Performance graphs cannot be viewed for Windows managed hosts.
2317671	Cannot replace or recover a disk removed from a UNIX host.
2353612	After the replace disk operation, the faulted disk status remains as replaceable.
2856380	Issues in the Add Host(s) wizard while adding agentless hosts to Management Server domain.
2941489	Cross Enclosure Mirroring Policy check was not showing correct violations for mirror which have subdisks in plex from same enclosure.
2976267	Vulnerability on port 5634/tcp over SSL.
3089901	VOM 5.0 (vxdisk -o thin,fssize list) triggers panic/memory corruption.
3225782	vxdclid can spin or lock in OpenSSL code on vxlist requests.

## About upgrading the Management Server

After you upgrade the Management Server to version 6.0, the objects and features from the previous version of Veritas Operations Manager are moved to the appropriate perspectives of Veritas Operations Manager 6.0.

However, note that some of the objects and features are not migrated to Veritas Operations Manager 6.0 after the upgrade. It is recommended that you refer to the *Veritas Operations Manager Management Server Installation and Configuration Guide* to know more about the migrated and non-migrated features and objects.



# System requirements

This chapter includes the following topics:

- [Operating system requirements](#)
- [Third-party required libraries](#)
- [System resource requirements](#)
- [Web browser requirements](#)
- [Network and firewall requirements](#)
- [About the consumption of the managed host components](#)

## Operating system requirements

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

## Third-party required libraries

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

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

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

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

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

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

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

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

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

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

## System resource requirements

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

For Management Server:

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

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

Additional considerations for system resource requirements for Veritas Operations Manager:

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

For a managed host:

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

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

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

---

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

---

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

<http://www.symantec.com/docs/TECH210708>

<http://www.symantec.com/docs/TECH210708>

## About space estimation for data logs

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

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

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

Data logs for host, volume, disk, file system, path, and initiator are stored on the managed host. The data logs for virtualization server, virtual machine, path, and initiator are stored on the Control Host. For storage array (port, adapter, and enclosure), data log for 1 day is stored on the discovery host, where as all the other logs are stored on Management Server.

---

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

---

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

**Table 2-1** Space estimation for data logs

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

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

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

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

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

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

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

Family	Frequency in minutes	Discovered information
Host	1440	The operating system, packages, and networking for the host. Typically, most of the information that is related to this family does not change frequently.
SF	30	Volume Manager, File Systems, and the related storage network.
VCS	60	Symantec Cluster Server and the related information.

Family	Frequency in minutes	Discovered information
DB	360	Oracle, DB2, MSSQL, and Sybase databases and their storage dependencies.
LDR	1440	The licenses that are installed on the hosts.
NR	5	Configuration status and external faults.
Native	360	Third-party volume management information.
Zones	120	Oracle Solaris zones and their storage dependencies.
LDoms	120	Oracle Solaris LDoms, and related CPU and memory information.
KVM	120	KVMs, and their correlation with the host.
Hyper-V	120	Virtual machines and storage discovery.
LPAR	360	Hosts, guests, and storage information.
VMware	360	ESX servers, virtual machines, and their storage dependencies. <b>Note:</b> This information is discovered only when Control Host Add-on is installed on a managed host that is designated as the control host.
Agentless	360	The following information on the hosts that are configured on the control host for agentless: <ul style="list-style-type: none"><li>■ The IP addresses, operating system, and the usage of the CPU and memory</li><li>■ The host bus adapters (HBAs) on the host</li><li>■ The disks on the hosts and their correlation with the array LUNs and multipathing</li><li>■ The volumes and the volume groups on the native Volume Manager</li><li>■ The mount points of the file systems and the correlation of the file systems with the disks</li><li>■ 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.</li></ul> <b>Note:</b> This information is discovered only when Control Host Add-on is installed on a managed host that is designated as the control host.

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

---

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

---

## Web browser requirements

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

## Network and firewall requirements

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

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

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

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



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

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

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

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

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

## Internet Protocol version requirements

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

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

**Table 2-4**      IPV4 and IPV6 support

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

See [“Network and firewall requirements”](#) on page 32.

## About the consumption of the managed host components

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

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

- UNIX/Linux - 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. A certain amount of network bandwidth is also used for the data replication.

# Software limitations

This chapter includes the following topics:

- Veritas Operations Manager 6.0 managed host not supported on AIX in Network Installation Manager
- No coexistence of managed host and CommandCentral Storage Management Server
- Live statistics for initiators are not supported on HP-UX
- Volume layout not discovered for LDM-managed volumes mounted without a drive letter
- Backup and restore limitations in Veritas Operations Manager 6.0
- Veritas Operations Manager does not support the discovery of LDOMs and Zones together on the same host
- Deployment-related limitations
- Windows Management Server high availability configuration limitations
- Solaris Zones virtualization support limitations
- Discovery limitations for virtualization support
- VCS configuration check reports violations only if at least one node in the cluster is running Symantec Cluster Server
- 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)

- Discovery of VMware VirtualCenter server or ESX server is not case-sensitive (2567318)
- Core density may not get calculated properly on HP-UX11iv2 hosts
- Tier information is not displayed for some devices in a FAST managed storage group (2795204)
- IBM System Storage DS enclosure discovery is not supported through HiCommand Server 7 in Veritas Operations Manager (2708346)
- For EMC Celerra and VNX file enclosures, NAS file system to Storage Pool correlation is not available (3339001)
- CIFS shares from NetApp and Celerra arrays that are mapped to a Windows host are not discovered
- Performance charts may not be displayed for EMC Symmetrix array ports and adapters (3247859)
- Inconsistency in storage calculation is observed for unclaimed VPLEX extents (2844028)

## Veritas Operations Manager 6.0 managed host not supported on AIX in Network Installation Manager

Installation of Veritas Operations Manager 6.0 managed host on AIX using Network Installation Manager (NIM) is not supported.

## 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

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.

## 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 6.0

On Linux, the `vom_backup.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_backup.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

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.

## Deployment-related limitations

You cannot upgrade Veritas Operations Manager Management Server from versions prior to 6.0 to version 6.1 directly.

For upgrading from versions prior to 6.0, do the following:

- First upgrade to version 6.0, and then upgrade to version 6.0.

## 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.

Veritas Operations Manager does not support discovery of disk slices for Solaris Zones virtualization. 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 Linux Kernel Virtual Machine (KVM) environment.
- For LPARs, 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.

## VCS configuration check reports violations only if at least one node in the cluster is running Symantec Cluster Server

VCS configuration policy check in Veritas Operations Manager does not report any violations if Symantec Cluster Server is not running on any of the systems in the

cluster. Also, if the cluster has a single system and Symantec Cluster Server is not running on that system, the VCS configuration check does not report violations.

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

The following limitations exist in Veritas Operations Manager 6.0, 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 start-stop feature 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 start-stop feature 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)

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, VBS operation will not complete. You can choose to abort the operation. As a preventive step, configure all the resources of a service group as critical.



## 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.

## Tier information is not displayed for some devices in a FAST managed storage group (2795204)

In a FAST managed storage group for an EMC Symmetrix VMAX enclosure, the tier information is not displayed for devices that are not part of the tiers associated to the policy of that storage group.

If you select a storage group from the **FAST** tab of a Symmetrix VMAX enclosure in the **Storage** perspective, in the **FAST Managed Devices** view, the **Tier Name** is displayed as **[OutOfPolicy]**, and the **Tier Type**, **Protection Level** are displayed as **Unknown**."

## IBM System Storage DS enclosure discovery is not supported through HiCommand Server 7 in Veritas Operations Manager (2708346)

Hitachi HiCommand Server supports the management and discovery of a variety of array vendors, and models including IBM System Storage DS arrays. However, Veritas Operations Manager 6.0 does not discover IBM System Storage DS enclosures using HiCommand Server 7.

## For EMC Celerra and VNX file enclosures, NAS file system to Storage Pool correlation is not available (3339001)

For EMC Celerra and VNX file enclosures, Veritas Operations Manager does not discover the NAS file system to Storage Pools correlation.

## CIFS shares from NetApp and Celerra arrays that are mapped to a Windows host are not discovered

Veritas Operations Manager does not discover Common Internet File System (CIFS) shares from NetApp and Celerra arrays, that are mapped to a Windows host by a non-system account user.

## Performance charts may not be displayed for EMC Symmetrix array ports and adapters (3247859)

Since SYMCLI reports point-in-time statistics samples for EMC Symmetrix array ports and adapters, if an array port or an adapter is not serving IO during the statistics collection then, the performance charts for these objects may not be displayed. The message "Performance statistics are not available for the selected duration." is displayed.

## Inconsistency in storage calculation is observed for unclaimed VPLEX extents (2844028)

This issue is observed for EMC VPLEX enclosures that are configured using Storage Insight Add-on. If there are any unclaimed VPLEX extents, you might observe a discrepancy between the Physical Un-configured data reported by the waterfall chart, and the used capacity reported under the **Storage Volumes** tab of VPLEX node. The discrepancy is not present if the extents are used by any VPLEX device.

# Known issues

This chapter includes the following topics:

- [Management Server issues](#)
- [Managed host issues](#)
- [Agentless discovery issues](#)
- [Storage Insight Add-on issues](#)
- [Virtual Business Service issues](#)
- [Storage Insight SDK Add-on issues](#)
- [Other issues](#)

## Management Server issues

The following issues relate to Veritas Operations Manager Management Server.

### Managed hosts with duplicate virtual machine identifiers are automatically removed by Veritas Operations Manager (3340537)

Veritas Operations Manager can manage virtual hosts (configured as agents), only if they have unique virtual machine identifiers associated with them. If such hosts (with duplicate identifiers) are found, they are automatically removed from the Veritas Operations Manager database. It can be observed for the following two scenarios:

#### **When the Management Server is upgraded to version 6.0:**

The hosts which are configured as agents in Veritas Operations Manager (with duplicate virtual machine identifiers) will be removed from Veritas Operations Manager during the upgrade process.

**To identify the hosts with duplicate identifiers in Veritas Operations Manager:**

- 1 First install the HotFix HF050001960-38 on Veritas Operations Manager 5.0 Management Server.
- 2 Run the script installed by the HotFix to get the list of duplicate virtual machines configured in the Veritas Operations Manager domain.

After the Management Server is upgraded to version 6.0, you need to again add these hosts to Veritas Operations Manager. Ensure that while adding the hosts, unique UUID is assigned to the hosts (BIOSUUID for VMware virtual machine).

**When new host is added to Veritas Operations Manager with the VM ID that is already associated with an existing managed host:**

In this case, the existing managed host data is removed from the Veritas Operations Manager database and only the newly added host will be displayed on the Management Server console. You need to ensure that while adding new virtual machine to Veritas Operations Manager, unique UUID is assigned to the machine (BIOSUUID for VMware virtual machine).

For more information, refer to following Technote:

<http://www.symantec.com/docs/TECH211826>

## 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.

## 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) are 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 :

```
#cd /var
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 xpirtld
```

## Status of all SF Manager 2.x hosts is shown as healthy on an upgraded Veritas Operations Manager 6.0 setup (2009372)

When you view the status of hosts on an upgraded Veritas Operations Manager 6.0 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 6.0 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/lib:$LD_LIBRARY_PATH
/opt/VRTSsfmh/bin/xdbadm -f ./a.sql -c /var/opt/VRTSsfmcs/conf -o
/etc/vx/VRTSsfmcs/.odbc.ini -d SFMdb3 -v
```

The best practice is to upgrade the `VRTSsfmh` to the same version as the Management Server.

## 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.

## 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, rescan the managed host.

## 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 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Virtualization**.
- 3 Right-click the virtualization server and select **Refresh Configuration**.
- 4 In the **Refresh Virtualization Configuration** wizard panel, click **Refresh**.
- 5 In the **Result** panel click **OK**.

## Performance metering of a VMware ESX server may not work properly after failover (2814844)

If Management Server is configured in high availability environment, and if Control Host Add-on is installed then, performance metering of VMware ESX server may not work properly after failover, until the next discovery cycle.

The following may occur until the next discovery cycle:

- Performance metering does not start for the VMware ESX server.
- Performance charts for which the duration is selected as Live, do not show any information.
- Incorrect error messages may be displayed in the performance chart.

Workaround:

You need to manually refresh the VMware ESX server discovery.

**To manually refresh the VMware ESX server discovery**

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Virtualization**.
- 3 Right-click the virtualization server and select **Refresh Configuration**.
- 4 In the **Refresh Virtualization Configuration** wizard panel, click **Refresh**.
- 5 In the **Result** panel click **OK**.

## For VMware virtual machine, the virtual storage correlation is not functional if a SCSI controller of non-default type is used (3056561)

For VMware virtual machine on Windows, Linux, or Solaris platforms, the virtual storage correlation (vDisk correlation) does not happen if a SCSI controller of non-default type is used.

## ESX servers not able to access an RDM disk associated with a shared datastore might cause failed discovery of RDM disk by Veritas Operations Manager (2736293)

This is applicable to VMware virtualization discovery using Veritas Operations Manager. This issue is encountered when an RDM disk (providing storage to the virtual machine) is associated with a datastore, which is shared among multiple ESX servers and some of these ESX servers do not have access to the RDM disk. In such cases, the RDM disk may not be discovered by Veritas Operations Manager.

Workaround:

Ensure that all ESX servers have access to the RDM disk.

## Occasionally the Management Server console shows blank views during navigation or blank wizard panels for the operations (3333313)

While performing any operation or navigating through Veritas Operations Manager Management Server views, user might come across blank page or blank wizard panels. To resolve this issue, you need to refresh the Web browser or clear cache, and then retry the navigation or the operation.

## Erroneous managed host status reported in Veritas Operations Manager high availability (HA) environment (2780631)

This issue is encountered if a Veritas Operations Manager Management Server is configured in a high availability (HA) environment. It is applicable to UNIX and Windows platforms.

When a managed host faults, its status is reported as down in the Veritas Operations Manager database. Assume that a managed host is down and the Management Server fails over from one node to another. For example, from MS1 to MS2.

Now if the managed host again comes up during the Management Server HA transition, MS2 node records the managed host's status as up. However, the fault and the down state of the managed host reported by MS1 are not cleared from the Veritas Operations Manager database (since Near-Real time data is not shared).

Workaround:

Perform a re-scan operation from the active Management Server node so that the correct state for the faults related to XPRTLTD up/down is updated on the Veritas Operations Manager console.

## Cannot search for some objects using size as criteria (3216639)

In the Management Server console Search window, using size as a search criteria will not work for the following objects:

- Disk
- Disk group
- Volume
- Virtual machine
- Virtualization server

## OS version name shown for Windows hosts varies in English and non-English system locale (3271960)

The way the operating system name and version is displayed for Windows hosts may vary for English and non-English system locale.

## Information on running tasks is accurate only for managed hosts 6.0 and later (3077899)

In the Management Server console, the information on running tasks in the Recent Tasks pane shows only for managed hosts 6.0 and later.

## Sometimes Internet Explorer displays a security warning when you navigate between pages in the console (2999524)

Sometimes as you navigate through pages in the Management Server console, Internet Explorer displays the security warning:

"Do you want to view only the webpage content that was delivered securely?"

Workaround:

On the security message, you can click **No** to continue to the page.

Alternatively, you can disable the security warning message in Internet Explorer.

**To disable the security warning message in Internet Explorer**

- 1 Go to **Tools > Internet Options > Security**.
- 2 On the **Security** tab, click **Custom Level**.
- 3 In the **Miscellaneous** section, select **Enable** under **Display mixed content**.

## Managed hosts previous to version 5.x are not listed for storage provisioning and volume migration

If using the Storage Provisioning and Enclosure Migration Add-on, storage provisioning and volume migration is supported only on managed hosts that run Veritas Operations Manager version 5.x or later. Hosts with earlier versions are not listed for storage provisioning and volume migration operations.

## Managed host issues

The following issues relate to host management.

### Issue related to upgrading the managed hosts (from 3.x to 6.0) 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 6.0, 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 6.0, 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.

### 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.

## 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>

## 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.

## 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.

## Some performance charts are not available for VMware ESX server version 4.1 managed through vCenter server 5.0 (2800239)

In Veritas Operations Manager **Available Memory** and **Used Swap** performance charts are not available for VMware ESX server version 4.1, which is discovered through the vCenter server version 5.0.

## Unable to view performance graphs for VxVM disk and volume on Windows platform (3054870)

In the Management Server console, if the performance graphs for VxVM disk and volume on Windows platform are not displayed, do the following:

- Ensure that the value of the **DisablePerformanceCounters** registry key in **HKLM\System\CurrentControlSet\Services\vxio\Performance** location is zero.

- Restart the XPRTLD service.

To restart the XPRTLD service, run the following commands at the command prompt:

- `net stop xprtld`
- `net start xprtld`

## Cannot add a managed host to Management Server using the IPv6 address of the host (2816487)

You cannot add a managed host to Management Server using the IPv6 address of the host.

Workaround:

Add the host to Management Server using its hostname.

## Incorrect statistics returned by DMP if Storage Foundation version is prior to 5.0 MP3 (2796418)

The performance statistics returned by Dynamic Multipathing (DMP) paths is incorrect if Storage Foundation version is prior to 5.0 MP3 on a managed host. The I/O displayed in the **Bytes Read/Written** performance graphs for the initiator, multipathing path, and enclosure is greater than the actual I/O.

## Create disk group operation fails when triggered from slave node in a clustered configuration (3196104)

In a clustered configuration, the create disk group operation fails when triggered from slave node and also if the disk naming schemes are different in master and slave.

## On HP-UX managed hosts, the path initiator and array port information is not displayed for some disks (3073128)

On the Management Server console, when you display information about the disks on HP-UX managed hosts, the path initiator and array port information is not displayed for some disks. The affected disks are those coming from controller number >512 or target number >15.

## Violated license deployment policies are not displayed correctly (3342986)

In the **Management Server** perspective, under **Faults and Risks**, if a rule is created to view the license deployment policies which are at risk or faulted and if the rule is triggered because of a violated policy, then the fault is not displayed in the **Faults** tab.

The **License deployment summary** table in **SFHA Licensing** displays incorrect number of violated policies.

## 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.

### 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.

### 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 .

## Storage Insight Add-on issues

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

### After the first discovery of IBM SVC array, manual refresh of putty cache may be required (3114164)

This issue is encountered when you have configured the IBM SVC array successfully with password or PPK key file and the array discovery is not happening after the first discovery cycle. To resolve this issue, you need to perform a manual refresh of putty cache as described below:

Workaround:

#### To refresh putty cache on Linux or Solaris platforms

- 1 Log on to the discovery host.
- 2 Navigate to `/root/.putty/sshhostkeys` to locate the sshhostkeys.
- 3 Remove array host entry.
- 4 Re-configure IBM SVC array using the Storage Insight Add-on.

#### To refresh putty cache on Windows platform

- 1 Open Windows registry.
- 2 Navigate to  
`HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\SshHostKeys`.

Ensure to use the same user credentials that are used to configure the IBM SVC array.

- 3 Delete the rows that contain the IP address of the IBM SVC array.

The mismatch in PPK key may happen if the administrator has configured a new SSH key pair for the given user. If you are using the PPK file authentication, you need to get the new PPK file from the administrator and use it to configure the array.

### For locally replicated EMC Symmetrix LUNs, last synchronization time is available only for SYMCLI version 7.4 or later (3249430)

This is applicable to the deep discovery of EMC Symmetrix enclosure using Storage Insight Add-on. For locally replicated LUNs, the last synchronization time is not

available on the Veritas Operations Manager Management Server console if SYMCLI version 7.3.x or earlier is used.

#### Workaround

You need to use SYMCLI version 7.4, or later to obtain this information.

## Manual discovery of Symmetrix enclosure is required when SYMCLI version is upgraded on the Storage Insight add-on discovery host (3289628)

This is applicable to the deep discovery of EMC Symmetrix enclosure using Storage Insight Add-on. If SYMCLI version is upgraded on the discovery host, the Symmetrix enclosure configuration should be refreshed manually from the Veritas Operations Manager console to discover some of the Symmetrix 's features (for example, FAST) if the upgraded SYMCLI version supports those features.

## 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 6.0

The NetApp enclosures that are configured using Storage Insight Add-on version 4.x are not discovered after the add-on is upgraded to version 6.0.

#### Workaround:

Edit the configuration, and enable NAS discovery for NetApp enclosure.

#### To edit the configuration and enable NAS discovery for NetApp enclosure

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Device**.
- 3 Expand **Enclosures** to locate NetApp.

- 4 In the **NetApp Configurations** list, right-click the enclosure, and select **Edit Configuration**.
- 5 In the **Edit Configuration** panel, select the **Enable NAS discovery** check box.

## Performance metering of enclosures may not work properly after failover (2814844)

If Management Server is configured in high availability environment, and if the enclosure is discovered through Storage Insight Add-on then, performance metering of the enclosure may not work properly after failover, until the next discovery cycle.

The following may occur until the next discovery cycle:

- Performance metering does not start for the enclosure.
- Performance charts for which the duration is selected as Live, do not show any information.
- Incorrect error messages may be displayed in the performance chart.

Workaround:

You need to manually refresh the enclosure discovery.

### To manually refresh the enclosure discovery

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Device**.
- 3 In the **Enclosure Configuration** tab locate the enclosure.
- 4 Right-click the enclosure and select **Refresh Configuration**.
- 5 In the **Refresh Configuration** panel, click **Yes**.

## Performance tab is not displayed if vFilers are discovered for NetApp enclosures (33342029)

For a NetApp enclosure, if vFilers are discovered using Storage Insight Add-on 6.0, then the **Performance** tab is not displayed for the enclosure.

## Information on FAST managed storage groups for EMC Symmetrix VMAX enclosures is not discovered periodically (2842124)

When an EMC Symmetrix VMAX enclosure is configured using Storage Insight Add-on, the storage distribution information for a FAST managed storage group

across different FAST tiers, may not get discovered as part of the periodic discovery cycle.

To optimize discovery time, the periodic discovery checks Symmetrix audit log to determine if any change has happened only for specific function classes and action codes.

#### Workaround

Refresh the enclosure from the Veritas Operations Manager console to view the updated information for FAST managed storage groups.

#### To manually refresh the enclosure discovery

- 1 In the Home page on the Management Server console, click **Settings**.
- 2 Click **Device**.
- 3 In the **Enclosure Configuration** tab locate the enclosure.
- 4 Right-click the enclosure and select **Refresh Configuration**.
- 5 In the **Refresh Configuration** panel, click **Yes**.

## Array group information is incorrect in Enclosure Storage Summary chart for Hitachi arrays (2820150)

When you view the **Enclosure Summary chart** for Hitachi, the array group bar may extend beyond the physical bar. This issue occurs when you create array groups with shared physical devices (PDEVs).

## Password file option does not work while configuring HP EVA enclosures on Windows hosts (2757601)

This issue is applicable to the deep array discovery of HP EVA enclosures using Storage Insight Add-on 6.0. On Windows host where the Storage Scripting System Utility (SSSU) CLI utility version is prior to 9.4, the password file option does not work while configuring HP EVA enclosures.

#### Workaround:

Install SSSU CLI utility version 9.4, or later, on the Windows host. Then, configure the HP EVA enclosure, and use the password file option.

## EMC Celerra enclosure details are not discovered for users with read-only access rights, and Imported Administrator or Operator role

This issue is applicable to the deep array discovery of EMC Celerra enclosure using Storage Insight Add-on 6.0. If the user with read-only privilege, and Imported

Administrator or Operator role, attempts to configure the enclosure, the enclosure details are not retrieved during the array discovery.

Workaround:

Assign the nasadmin role to the user.

## Network File System on Solaris cannot be discovered if the Fully Qualified Host Name is used in vfstab file but not used for mounting the file system (2747735)

If Network File System (NFS) on Solaris is mounted without providing the Fully Qualified Host Name (FQHN) but the `/etc/vfstab` file contains FQHN, the NFS file system cannot be discovered in Veritas Operations Manager 6.0.

## Virtual Business Service issues

The following are Virtual Business Service issues

### 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.

## Storage Insight SDK Add-on issues

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

### Edit and Test operations on Storage Insight Plug-in are not supported using Internet Explorer on 64-bit Windows hosts (2826079)

This issue is observed on a 64-bit Windows host where Storage Insight SDK Add-on is installed. Using Internet Explorer, you cannot upload the Storage Insight Plug-in

file (.sfa). So, the **Edit** and **Test** operations cannot be performed in Internet Explorer.

Workaround:

You need to use other Web browsers to edit and test the Storage Insight Plug-in. For example, Mozilla Firefox or Google Chrome.

## 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##`.

### Symantec ApplicationHA Console single sign-on breaks after Veritas Operations Manager 6.0 managed host installation or upgrade on ApplicationHA hosts

When Veritas Operations Manager 6.0 managed host is installed or upgraded on a host that has either Symantec ApplicationHA 5.1 Service Pack 2 or Symantec ApplicationHA 6.0 installed on it, the ApplicationHA Console single sign-on fails to work.

There is no workaround for the issue.

### Unable to configure Management Server with a user name in Russian language using Firefox browser

Using the Firefox browser, you cannot configure Management Server if your user name is in Russian language. The basic authentication mechanism does not work properly in Firefox, only if the user name is in Russian language.

## Coexistence of ApplicationHA Console 6.0 and Veritas Operations Manager 6.0 not supported (2739241)

ApplicationHA console 6.0 and Veritas Operations Manager 6.0 have compatibility issues and the two products cannot coexist on a single server.

Work around:

Upgrade the ApplicationHA console to 6.0.1.

## Resource attributes not discovered for RVGPrimary Resource

On a UNIX cluster with VCS version lower than 6.1, attributes for RVGPrimary resource do not get discovered through Veritas Operations Manager.

# Documentation addenda and errata

This chapter includes the following topics:

- [Online help add-on](#)

## Online help add-on

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

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

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



# Getting help

This appendix includes the following topics:

- [Veritas Operations Manager on the Web](#)
- [Getting help](#)
- [Using the product documentation](#)

## 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](http://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

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

**Table A-1** Names of Veritas Operations Manager Guides

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

**Table A-2** URLs for Veritas Operations Manager documentation

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

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

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

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