Veritas™ Operations Manager Management Server 6.1 Release Notes

December 2014

Symantec™

Veritas™ Operations Manager Management Server Release Notes

Product version: 6.1

Document version: 6.1 Rev 3

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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/contact_techsupp_static.jsp

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

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

- Product release level
- Hardware information

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

About Symantec Connect

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

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

Documentation

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

doc_feedback@symantec.com

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

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

Contents

Chapter 1

Overview of this release

This chapter includes the following topics:

About Veritas Operations Manager

Veritas Operations Manager by Symantec gives you a single, centralized management console for the 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

New features and changes in Veritas Operations Manager 6.1

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

Support for SFHA 6.2 features

You need to apply the hotfix 6.1.0.100 or higher in order to have support for the following:

- Red Hat Enterprise Linux 7
- Symantec Storage Foundation High Availability 6.2 features including SmartIO and Flexible Storage Sharing (FSS) for AIX and Solaris

Ability to enable and disable authentication domains

Using Veritas Operations Manager 6.1 you can enable or disable authentication domains that are associated with an authentication broker, LDAP, or AD.

Ability to monitor file system capacity on Windows hosts

Using Veritas Operations Manager 6.1 you can monitor the file system capacity for Windows hosts.

Ability to perform operations in Veritas Operations Manager using REST Web services API

Using REST Web services API in Veritas Operations Manager 6.1 you can perform the following operations:

- Start and stop Virtual Business Services.
  This operation can be performed in the **Server** and **Availability** perspective.
- Start and stop VVR replication.
- Run a recovery plan.
- Provision storage using a storage template.
- Perform thin reclamation on disks, volumes, and thin pools of an enclosure.

Ability to access information for new objects discovered by Veritas Operations Manager using REST Web services API

Using REST Web services API in Veritas Operations Manager 6.1 you can access information for the following new objects listed in Table 1-1

Table 1-1 Objects and perspective

Object	Perspective
Replicated volume group	Server
Replication link between primary and secondary RVGs	Server
Hosts participating in RVG replication	Server
Smart IO cache area	Server
Cluster volume manager (CVM)	Server
Storage provisioning templates	Server
Recovery plan	Availability
View all tasks	All perspectives except the Management Server perspective.
View all the sub-tasks	All perspectives except the Management Server perspective.

Support for SmartIO cache area

SmartIO supports the use of multi-vendor Solid-State Devices (SSDs) as read-write cache for the high-transaction applications running on a system to improve overall I/O performance. The Veritas Operations Manager Management Server console now supports the following SmartIO cache area-related operations:

- Creating, modifying, and deleting a cache.
- Enabling and disabling SmartIO caching.

Ability to define threshold settings on objects and receive notifications

Using Veritas Operations Manager 6.1 Management Server console, you can set the threshold values on the respective objects for the metrics that are described in Table 1-2 on the respective objects. A Risk or Fault is raised when the threshold condition is violated.

Table 1-2 Objects and metrics

Object	Metrics
Host	CPU Utilization Available Memory Average CPU Load
Disk, volume, and path associated with a host.	Average Read Latency Average Write Latency
Host Initiator	Average Read Latency Average Write Latency Read Queue Length Write Queue Length Read Errors Write Errors
Cluster and service group	Failover Duration

Support for Flexible Storage Sharing

Flexible Storage Sharing (FSS) is a feature of Symantec Storage Foundation Cluster File System High Availability (SFCFSHA) that enables network sharing of local storage, cluster wide. The local storage can be in the form of Direct Attached Storage (DAS) or internal disk drives.

The Veritas Operations Manager Management Server console now supports FSS-related operations and views for FSS-capable clusters, as follows:

- Veritas Operations Manager discovers whether FSS is enabled for a disk group and the information is shown in the console.
- Veritas Operations Manager discovers whether a disk is exported (network shared disk), remote, or neither and will show the FSS state for a disk in the console.
  Disk export is an FSS-specific operation performed on a disk that is locally visible to a host to make it visible to all hosts in the CVM cluster. A remote disk is a disk that has been exported from another host in the cluster.
- The Management Server console contains wizards for support of the FSS operations of enabling/disabling FSS for an existing disk group and exporting/unexporting disks for shared use in the CVM cluster. Wizards for existing SF operations support FSS operations as needed.

- During volume creation for an FSS-enabled disk group, you can specify to mirror the volume across hosts. The Cross Enclosure/Host Mirroring policy signature can help validate that mirrored volumes are not based off local storage from a single host.

Refer to the *Symantec Storage Foundation and High Availability Solutions Software Compatibility List* for information on FSS support by your SFCFSHA version and platform.

Ability to view information about CVM clusters

Symantec Storage Foundation Cluster File System High Availability (SFCFSHA) includes the Cluster Volume Manager (CVM) as a component. In the Veritas Operations Manager Management Server console, a storage clusters node has now been added to the Server perspective to help you monitor information about CVM clusters. Similar views are provided in the Veritas Operations Manager Web services API.

You can view the following information in the Server perspective:

- A table of all CVM clusters
- Detailed information about objects in a selected cluster. such as hosts, all disks of all hosts, shared disk groups, volumes and file systems, and applications
- The correlation of shared and exported storage across hosts in a cluster

The global search feature now includes clusters as an object. You can create and save search queries based on cluster attributes.

Operations available from a host, such as disk, disk group, and volume operations, are available from the same objects when viewed in the cluster context.

Unified alerting and central view for policy check violations

Policy check scans in Veritas Operations Manager identify resources that do not meet specified standards. In earlier releases, when a policy check scan was run, you would need to check individual hosts to find out if violations were detected on that host.

The unified alerting feature provides a central view to manage and monitor all faults. The data center faults list now includes faults generated for policy check violations. You can set up a rule to receive offline notification on any policy violations. Details on the specific violations are still available at the host level so that you can take the steps necessary to resolve the violation.

Improved recovery plans

Veritas Operations Manager 6.1 provides following enhancements to recovery plans:

- You can now specify description and timeout for each step in a recovery plan.
- While creating or editing a recovery plan, you can import the tasks from an existing recovery plan.
- In a recovery plan, service groups can now be site aware for stretched clusters.

Other enhancements include displaying start time and end time for each task, displaying return-code for a custom script execution, and allowing users to delete multiple recovery plans.

Site aware service group operations

While performing service group operations in a campus cluster, now you can also provide site-related information. With site-level awareness, the administrator can fail over a service group to another site in an event of failure at the local site. The feature is supported for the following service group operations:

- Online
- Offline
- Switch

Symantec HA Plug-in for vSphere Web Client

The Symantec HA Plug-in for vSphere Web Client allows you to use VMware vSphere Web Client for Symantec ApplicationHA operations. The Symantec HA Plug-in for vSphere Web Client enables the capabilities of Symantec High Availability Console in the VMware vSphere Web Client. After you have installed the Symantec HA Plug-in for vSphere Web Client, you need to register Symantec HA Plug-in with the required VMware vCenter Server using the Management Server Console. With the 6.1 release of Veritas Operations Manager, you can view the **Dashboard** and **Application Health View** on the VMware vSphere Web Client. The Symantec HA Plug-in for vSphere Web Client can also be deployed in high availability configuration of Veritas Operations Manager Management Server.

Ability to refresh the discovery of one or more ESX Servers

Using the Management Server Console, now you can refresh the discovery of one or more ESX Servers that are configured under a specific VMware vCenter Server.

Enhanced near-real time discovery of VMware infrastructure

The near real-time discovery of VMware infrastructure is enhanced by the incorporation of the following features:

- Concurrent discovery of vCenter Servers and ESX servers: It allows concurrent discovery of vCenter Servers and ESX servers configured in the Management Server domain thereby providing improved performance for virtual infrastructure discovery in Veritas Operations Manager.
- Partial discovery of ESX servers: It enables the discovery of sub-set of ESX servers managed under a VMware vCenter Server.
- Veritas Operations Manager now discovers additional VMware events. For example, VM created and VM migrated.

Enhancements in Hardware and Software Compatibility

Veritas Operations Manager 6.1 provides support for additional array models, new array firmware and command-line versions, and applications. For more information, refer to the *Veritas Operations Manager Hardware and Software Compatibility List (HSCL)*.

Multi-site management support on Windows platform

Multi-site management operations are now supported on Windows platform also.

Updated alert topics

Following two alert topics are updated in Veritas Operations Manager 6.1:

Old alert topic	New alert topic
event.alert.vom.host.low.memory	event.alert.vom.host.memory.available.risk
event.alert.vom.host.high.cpu.util	event.alert.vom.host.cpu.utilization.risk

When you upgrade from Veritas Operations Manager version 6.0 to 6.1, and if there are any rules defined on the Management Server that include these old topics, then you need to update the rules with the new alert topics.

Discontinued support for Control Host Add-on on Solaris platform

Veritas Operations Manager version 6.1 does not support Control Host Add-on 6.1 installed on Solaris managed host 6.1.

If you have already configured Control Host Add-on 6.0 on a Solaris host, do the following:

1. Add a Linux or Windows managed host 6.1 to the Management Server 6.1 domain.
2. Install Control Host Add-on add-on 6.1 on the host.
3. Manually unconfigure the resources, vCenter, HMC, agentless hosts from the Solaris host and reconfigure them on the new host.

Script file is not provided for this migration.

Issues fixed in the Veritas Operations Manager 6.1 release

Table 1-3 lists the Management Server issues that have been fixed in the Veritas Operations Manager 6.1 release.

Table 1-3 Management Server issues fixed in Veritas Operations Manager 6.1

Incident	Description
3342029	Performance tab is not displayed if vFilers are discovered for NetApp enclosures.
3371936	Linux localhost Pluggable Authentication Modules (PAM) authentication fails.
3376238	Unable to discover any ESX hosts.
3382393	**Settings > Management Server** view displays a blank page.
3386374	Veritas Operations Manager disk group search does not show host.
3388634	Symantec Performance Value Unit (SPVU) value calculated by Veritas Operations Manager is not correct.
3401595	License Lifecycle report shows BIRT exception if user's browser locale is set to any language other than English or English-US.
3402716	Unable to list database files from API.
3403690	**Suppress Faults** or **Restore faults** view displays a blank page.
3409720	On a Management Server with non-english system locale, **Settings > SORT > SFHA download settings** view displays a blank page.
3412518	Fabric discovery configuration fails for Cisco switches that had numeric WWNs.

Table 1-3 Management Server issues fixed in Veritas Operations Manager 6.1 *(continued)*

Incident	Description
3428179	In Veritas Operations Manager 6.0, list of hot fixes is not visible in **Settings > Deployment > Repository > Hot fixes** view.
3436627	Installation of Veritas Operations Manager hot fixes fails.
3448174	Unable to configure an LDAP domain in Veritas Operations Manager.
3450721	Unable to edit overridden attribute at resource level .
3461555	Windows RVG not visible in Management Server.
3468815	RVG appears as faulted in the left hand object tree-view.
3504553	HBAAPP opens and rewinds tape devices even when used with -P option,.
3508836	Extended attributes that are defined on fabrics, switches, and zones are deleted after scheduled data purging.
3509361	Entries in **Edit Virtualization** panel for vSphere do not show slash as separator between domain and user.
3480301	Storage migration from a vSCSI LUN to NPIV is not supported in Veritas Operations Manager 6.0.
3439331	Extraneous multiple scrollbars overlaying some of the screen areas.
3499471	Direct download of add-on fails.
3505363	Smart folder does not filter result set.

Table 1-4 lists the managed host issues that have been fixed in the Veritas Operations Manager 6.1 release.

Table 1-4 Managed host issues fixed in Veritas Operations Manager 6.1

Incident	Description
3369799	Alert not raised in case a disk path is removed.
3387083	Real-time discovery is not getting triggered for remote group notifications.
3396404	Veritas Operations Manager 6.0 shows file system as faulted for all hosts having same LV_UUID.
3401547	Veritas Operations Manager 6.0 does not listen to VEA alerts for Windows when the disk group has all the disks in failed state.

Table 1-4 Managed host issues fixed in Veritas Operations Manager 6.1 *(continued)*

Incident	Description
3405147	disks are not visible from **HOST > DiskGroup > DG name > Disks** view for the agentlessly discovered hosts.
3408281	Control Host Add-on needs to update the Java Runtime Environment (JRE).
3411022	Unable to add second host on Linux managed host with InfiniBand MAC addresses.
3446094	VVR Bandwidth report is not generated on Windows platform.
3450713	Unable to bring the disks online from Management Server console on Windows hosts.
3485022	Vulnerability issue of port 5634 on HP-UX managed hosts.
3477610	Veritas Operations Manager fails to discover server disks and disk groups due to incorrect Symmetrix device serial numbers reported in `HBA.JSON`.

Chapter 2

System requirements

This chapter includes the following topics:

Operating system requirements

For information on Operating system requirements for Veritas Operations Manager 6.1, 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

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

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

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

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

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

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

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

System resource requirements

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

For Management Server:

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

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

Additional considerations for system resource requirements for Veritas Operations Manager:

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

For a managed host:

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

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

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

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

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

About space estimation for data logs

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

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

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

Data logs for host, volume, disk, file system, path, and initiator are stored on the managed host. The data logs for virtualization server, virtual machine, path, and initiator are stored on the Control Host. For storage array (port, adapter, and

enclosure), data log for 1 day is stored on the discovery host, where as all the other logs are stored on Management Server.

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

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

Table 2-1 Space estimation for data logs

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

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

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

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

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

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

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

Family	Frequency in minutes	Discovered information
Host	1440	The operating system, packages, and networking for the host. Typically, most of the information that is related to this family does not change frequently.

Family	Frequency in minutes	Discovered information
SF	30	Volume Manager, File Systems, and the related storage network.
VCS	60	Symantec Cluster Server and the related information.
DB	360	Oracle, DB2, MSSQL, and Sybase databases and their storage dependencies.
LDR	1440	The licenses that are installed on the hosts.
NR	5	Configuration status and external faults.
Native	360	Third-party volume management information.
PCV_NOTIFY	30	Policy check violations computed on Management Server and on managed hosts earlier than 6.1. Violations computed on managed hosts 6.1 or later do not require separate discovery.
Zones	120	Oracle Solaris zones and their storage dependencies.
LDoms	120	Oracle Solaris LDoms, and related CPU and memory information.
KVM	120	KVMs, and their correlation with the host.
Hyper-V	120	Virtual machines and storage discovery.
LPAR	360	Hosts, guests, and storage information.

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

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

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

See "System resource requirements" on page 25.

Web browser requirements

For information on Web browser requirements for Veritas Operations Manager 6.1, 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.
5636	TCP	Management Server	Management Server database configuration	Management Server cannot be configured.
5634	TCP		Management Server communications with the managed hosts	Managed host cannot be added to the Management Server domain.
5634	TCP	managed hosts	Managed host to send heartbeats; also used to upload the data from the managed host to Management Server **Note:** It is recommended that you keep port 5634 open between managed hosts for scalability and performance optimization.	Managed host cannot be added to the Management Server domain.
14161	TCP	Web browser	Run the Management Server console	Users cannot access the Management Server console.

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

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

Internet Protocol version requirements

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

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

Table 2-4 IPV4 and IPV6 support

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

See "Network and firewall requirements" on page 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.

See “About the frequency of managed host, enclosure and switch information discovery” on page 29.

Chapter 3

Software limitations

This chapter includes the following topics:

Veritas Operations Manager 6.1 managed host not supported on AIX in Network Installation Manager

Installation of Veritas Operations Manager 6.1 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 6.1

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

On Windows, the `vom_bkup.pl` backup script can back up an existing Management Server in high-availability configuration. However, you cannot use the backup script to restore the high-availability configuration. This feature is currently not supported. To restore the backed up data, contact Symantec Technical Support.

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

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 6.1.

Windows Management Server high availability configuration limitations

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

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

Solaris Zones virtualization support limitations

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

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 6.1, which are related to the correlation between the disks and the disk groups:

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

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.

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.

Veritas Operations Manager does not properly support clustered Veritas Volume Replicator (VVR)

Veritas Operations Manager does not properly show replicated volume group (RVG) and host relationships for Veritas Volume Replicator (VVR) in clustered environments.

Limitations on SF operations on Windows CVM cluster

In the Management Server console, operations on SF disk groups of the cluster-shared type and operations on volumes on such disk groups are not available on a Windows CVM cluster.

Add host operation fails for RHEL 7 managed hosts

In the Veritas Operations Manager console, if you try to add a RHEL 7 managed host through agent, sometimes the operation fails. This failure occurs due to the new firewall daemon (firewalld) introduced in RHEL 7.

Workaround:

Do one of the following:

- Check the status of the firewall daemon using the following command:

  ```
  systemctl status firewalld
  ```

  If the daemon is running then you need to turn it off using the following command:

  ```
  systemctl stop firewalld
  ```

- If you want to allow only a specific port, use the following command:

  ```
  firewall-cmd --permanent --zone=public --add-port=port/tcp
  ```

  Where, *port* is the port number that you want to allow.

Chapter 4

Known issues

This chapter includes the following topics:

Management Server issues

The following issues relate to Veritas Operations Manager Management Server.

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 xprtld
```

Status of all SF Manager 2.*x* hosts is shown as healthy on an upgraded Veritas Operations Manager 6.1 setup (2009372)

When you view the status of hosts on an upgraded Veritas Operations Manager 6.1 console that has SF Manager 2.*x* managed hosts, the status of all the hosts is shown as healthy even though some of the hosts have reported faults.

Workaround:

You need to upgrade the 2.*x* managed hosts to Veritas Operations Manager 6.1 and then clean up the 2.*x* faults.

To clean up the 2.*x* faults

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

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

2 Run the following:

```
/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 vCenter 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**.

Note: The Veritas Operations Manager also provides near real-time discovery of VMware infrastructure based on certain VMware events. It can capture VM migration events (for example, VM migrated and DRS VM migrated) from VMware vCenter Server and update the VMware data in Veritas Operations Manager database in near real-time. If the near real-time discovery of VMware infrastructure is enabled, you do not need to manually refresh the VMware vCenter Server. For the detailed instructions on configuring the near real-time discovery of VMware events, refer to the *Veritas Operations Manager Management Server Installation and Configuration Guide*.

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.

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 XPRTLD up/down is updated on the Veritas Operations Manager console.

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.

Near real-time updates of VMware virtual machine power state are not functional for the non-default database location on Windows Management Server (3530272)

This issue is observed when Veritas Operations Manager Management Server is installed on the Windows platform. If the Management Server database is installed on any other location than its default location, the virtual machine power states are not updated in near-real time.

The correct virtual machine states are discovered and updated by the periodic VMware family discovery in Veritas Operations Manager.

Veritas Operations Manager does not discover virtual machines with same BIOS GUID on a Hyper-V Server (3509138)

Veritas Operations Manager does not discover multiple Hyper-V virtual machines with the same BIOS GUID. Note that multiple virtual machines with the same BIOS GUID can co-exist on a Hyper-V Server (Parent partition). However, Veritas Operations Manager discovers only single virtual machine because it uses BIOS GUID as the unique identifier to discover such virtual machines.

There is no workaround for the issue.

Disk information for the cluster does not display correct data for host (3532746)

You may not be able to view the disks correctly in the **Disks** tab when you select the cluster in the **Server** perspective, if you upgrade a managed host to 6.1 and:

- The host is part of a CVM cluster.
- The disks are not in any disk group or volume group.
- The disks are under the control of some native volume manager such as .LVM or ZFS instead of VxVM.

These disks appear correctly under the **Disks** tab of the respective host.

Workaround:

After upgrading the Veritas Operations Manager managed hosts package on these hosts to 6.1, remove all the managed hosts that share such disks from the Management Server domain once and then add them again to the Management Server domain.

Disk correlation does not happen for LDOM storage container after enabling MPxIO on the SAN disks (3370824)

In the Virtualization perspective of Management Server console, the disk correlation for storage containers is shown. However, after you enable Solaris Multiplexed I/O (MPxIO) on the SAN disks, the disks correlation for LDOM storage containers does not happen. It is important to note that the issue is observed only for the Virtualization perspective; the disks to volume or disk group correlation is operational in the Server perspective.

There is no workaround available for the Virtualization perspective. If you have System perspective privileges, you can see the disks correlation.

Managed host issues

The following issues relate to host management.

Issue related to upgrading the managed hosts (from 3.*x* to 6.1) that have LUNs from IBM XIV storage array (2367519)

This issue is related to all managed hosts having IBM XIV enclosure connected to them. When you upgrade the managed hosts from version 3.*x* to 6.1, on the Veritas Operations Manager console, two entries are displayed for the same enclosure. The first entry is a dangling object, which has no association with any of the objects. The other entry has Disk, LUNs, array port , and the initiators associations setup, and is reported correctly.

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

Workaround:

After upgrading the managed host to Veritas Operations Manager 6.1, the discrepancy of dangling object is automatically cleaned up by the scheduled run of a stored procedure. It runs at 3:00 AM every morning on the Management Server.

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 Symantec 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 Symantec Storage Foundation for Windows version 5.1 SP1 are not discovered as thin.

Workaround:

Download the hot fix for Symantec 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.

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.

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 6.1.

Bandwidth tab displays incorrect data for a UNIX host (3484788)

The bandwidth information for a replicated volume group that is displayed in the **Data Transmitted** column in the **Bandwidth** tab for a UNIX host is incorrect. This happens only if the host is reporting to multiple Management Servers.

Control Host add-on upgrade process on a Windows host shows completed but unable to add or delete vCenter (3517058)

This issue occurs because the `vmwarecollector` process is running on the host during the upgrade process.

Workaround:

To complete the upgrade process, do the following:

1. Disable performance metering on the host (Right-click the host, select **Properties**, and then select the **Performance** tab).
2. Ensure that the `vmwarecollector` process is completed before starting the upgrade.

   Note: If the process is running, let it complete. Do not terminate the process because it may corrupt the statistical data that is collected from the vCenter server.

3. Upgrade the Control Host add-on on the host.
4. Enable performance metering on the host (Right-click the host, select **Properties**, and then select the **Performance** tab).

Live statistics for memory usage on Solaris managed host shows incorrect free memory (3518586)

On a Solaris managed host, when a user views the live statistics for memory utilization, the free memory displayed does not tally with the data reported by `vmstat` command.

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 6.1

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 6.1.

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**.

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**.

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 6.1. 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 6.1. 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.

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.

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**."

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.

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 6.1 does not discover IBM System Storage DS enclosures using HiCommand Server 7.

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.

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.

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.

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.

Storage Insight Plug-in upload operation sometimes fails on Internet Explorer Web browser (3485662)

When you try to upload the Storage Insight Plug-in file (`.sfa`) using Internet Explorer Web browser (versions 8, 10, and 11), the operation may fail.

Workaround:

Use other Web browsers to upload the Storage Insight Plug-in. For example, Mozilla Firefox and Google Chrome.

Fabric Insight Add-on issues

The following issues are related to Fabric Insight Add-on.

SAN switch discovery fails when Veritas Operations Manager Management Server, configured in high availability mode, is used as a discovery host (3513295)

When Veritas Operations Manager Management Server (configured in high availability environment) is used as a discovery host for the switch configuration, the switch discovery is not successful. When you configure the switch discovery

using the Management Server console, though the configuration completes, the switch details are not discovered.

Workaround:

Use other managed host than the Management Server, install Fabric Insight Add-on on it, and then use it as the discovery host for the switch discovery.

Symantec HA Plug-in for vSphere Web Client issues

The following issues are related to Symantec HA Plug-in for vSphere Web Client.

Status and system data on the high availability (HA) dashboard disappear abruptly when Symantec HA Plug-in for vSphere Web Client is used with VMware vSphere 5.1 (3509084)

This is applicable to Symantec HA Plug-in 6.1 for vSphere Web Client. If you use VMware vSphere version 5.1 with the plug-in, the **Status** and **System** column entries disappear abruptly from the Symantec high availability dashboard.

To resolve this issue, use one of the following options:

- Clear the web browser cache and then restart VMware vSphere Web Client.
- Click some other tab in the VMware vSphere Web Client (for example, **Storage Reports**), refresh the web browser, and then go to the **Symantec High Availability** tab.

Note: This issue is encountered only with VMware vSphere version 5.1. With VMware vSphere version 5.5, the **status** and **system** columns data is available on the high availability dashboard.

Post application configuration, the notify sink resource `VCSAppMonNSRes` remains in faulted state (3491987)

For Greenfield customers, the notify sink resource `VCSAppMonNSRes` will remain in the faulted state because standalone HA Console is not available. However, the user can offline `VCSAppMonNSRes` resource.

For Brownfield customers, the notify sink resource `VCSAppMonNSRes` will remain in the Online state only if the user has decided to retain the existing HA Console installation along with the vSphere Desktop Client.

There is no workaround for the issue.

High Availability tab is visible even after un-registration of vSphere plug-in in Veritas Operations Manager Management Server (3498886)

After you unregister the vSphere plug-in in the Veritas Operations Manager Management Server, the High Availability tab is still visible to the user in the vSphere Web Client.

Workaround:

For the un-registration of single vCenter Server:

When single vCenter Server is configured and you have un-registered the vSphere plug-in, you need to delete the cached plug-in data from following location:

```
C:\ProgramData\VMware\vSphere Web
Client\vc-packages\vsphere-client-serenity
```

After you have deleted the data, restart the VMware vSphere Web Client service.

For multiple vCenter Servers, proceed as follows:

- If you have un-registered the vSphere plug-in from some vCenter Servers, restart VMware vSphere Web Client service.
- If you have un-registered the vSphere plug-in from all vCenter Servers, first, delete the cache data, and then restart the VMware vSphere Web Client service.

After these steps are run successfully, the High Availability tab is no longer visible on the vSphere Web Client.

Symantec ApplicationHA Console single sign-on breaks after Veritas Operations Manager 6.1 managed host installation or upgrade on ApplicationHA hosts

When Veritas Operations Manager 6.1 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.

Symantec High Availability Dashboard sometimes does not appear (3494263)

If you navigate to an ESX cluster or datacenter in the inventory tree of the VMware vSphere Web Client, the Symantec High Availability Dashboard does not appear. This issue occurs only if a virtual machine that does not have a unique universal

identifier (UUID), is associated with a vCenter server where you have registered the Symantec HA Plug-in for vSphere Web Client.

Workaround:

Identify any virtual machines in your setup that do not have a UUID, assign a UUID to each virtual machine, and then refresh the Dashboard.

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#.

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 6.1 not supported (2739241)

ApplicationHA console 6.0 and Veritas Operations Manager 6.1 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.

Incorrect size discovered for disks greater than 2 TB (3330363)

If the size of the disk is greater than 2 TB, HBAAPP cannot discover the capacity of the disk correctly on a Solaris x86 or HP-IA host. For such disks, the capacity is discovered as 2 TB.

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.

This issue appears only if the user had VMware VirtualCenter server or ESX server configured in Veritas Operations Manager 6.0 environment and he upgrades to Veritas Operations Manager 6.1.

Offline instances not displayed in instance tab for MSSQL HA configuration (3516063)

In case of MSSQL HA configuration, offline instances are not displayed on instance tab for MSSQL database in **Server** perspective.

Only one virtual machine configured as resource gets discovered (3488469)

If a service group has multiple virtual machines configured as resources, only one of the virtual machines is displayed in the **vSystems** tab.

Policy check violation not generated for Disk Connectivity policy check (3530346)

In Veritas Operations Manager 6.1, **Disk Connectivity** policy check does not report violations correctly in all the scenarios.

Appendix A

Documentation addenda and errata

This appendix includes the following topics:

Errata for Veritas Operations Manager 6.1 offline help

This section contains the errata in the offline help for Veritas Operations Manager 6.1.

Using the Management Server console

In this chapter, in the following topics, the version of Veritas Operations Manager in the images should read as 6.1:

- About the Management Server console Home page
- About the elements in a perspective view
- About viewing the summarized information
- About viewing the solutions
- About viewing the reports

Appendix B

Getting help

This appendix includes the following topics:

Veritas Operations Manager on the Web

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

http://go.symantec.com/vom

Getting help

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

For technical assistance, visit

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

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

Using the product documentation

Table B-1 lists the Veritas Operations Manager guides and Table B-2 lists the URLs for Veritas Operations Manager documentation:

Table B-1 Names of Veritas Operations Manager Guides

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

Table B-2 URLs for Veritas Operations Manager documentation

URL	Description
https://sort.symantec.com/documents	Latest version of the product documentation.
http://www.symantec.com/connect/videos/vom-videos	List of How-to videos.
http://www.symantec.com/docs/TECH218376	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.