Veritas InfoScale™ Operations Manager 7.1 Release Notes

April 2016

VERITAS™

Veritas InfoScale™ Operations Manager 7.1 Release Notes

Document version: 7.1 Rev 0

Last updated: 2016-04-27

Legal Notice

Copyright © 2016 Veritas Technologies LLC. All rights reserved.

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

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

https://www.veritas.com/about/legal/license-agreements

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

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

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

Veritas Technologies LLC

500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

.

Technical Support

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

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

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

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

Documentation

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

https://sort.veritas.com/documents

Documentation feedback

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

doc_feedback@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

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

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1 Overview of this release 11

About Veritas InfoScale Operations Manager 11
New features and changes in Veritas InfoScale Operations Manager 7.1 12
Ability to enable encryption 12
Ability to set a host prefix for disks 12
Support for multiple cache areas, live performance charts, and more SmartIO tasks 13
Ability to determine optimal caching with SmartAssist 13
Ability to control max IOPS for application co-existence 14
Ability to map and unmap remote disks 14
Ability to discover Docker container information 14
Integration of InfoScale Access operations with Management Server console GUI 15
Veritas InfoScale Operations Manager 7.1 Managed Host components are not released on HP-UX 15
Issues fixed in the Veritas InfoScale Operations Manager 7.1 release 15

Chapter 2 System requirements 16

Operating system requirements 16
Third-party required libraries 16
32-bit SNIA Common HBA API required on Windows hosts 17
System resource requirements 17
About space estimation for data logs 18
About the frequency of managed host, enclosure and switch information discovery 21
Supported hardware 24
Web browser requirements 25
Network and firewall requirements 25
Internet Protocol version requirements 27
About the consumption of the managed host components 28

Chapter 3 Software limitations 30

Veritas InfoScale Operations Manager 7.1 managed host not supported on AIX in Network Installation Manager 31
No coexistence of managed host and CommandCentral Storage Management Server 31
Live statistics for initiators are not supported on HP-UX 31
Volume layout not discovered for LDM-managed volumes mounted without a drive letter 32
Backup and restore limitations in Veritas InfoScale Operations Manager 7.1 32
Veritas InfoScale Operations Manager does not support the discovery of LDoms and Zones together on the same host 32
Deployment-related limitations 32
Windows Management Server high availability configuration limitations 33
Solaris Zones virtualization support limitations 33
Discovery limitations for virtualization support 33
VCS configuration check reports violations only if at least one node in the cluster is running Cluster Server 34
Limitations related to the correlation between the disks and the disk groups 34
Core density may not get calculated properly on HP-UX11iv2 hosts 34
CIFS shares from NetApp and Celerra arrays that are mapped to a Windows host are not discovered 34
Veritas InfoScale Operations Manager does not properly support clustered Veritas Volume Replicator (VVR) 35
Limitations on SF operations on Windows CVM cluster 35
Add host operation fails for RHEL 7 managed hosts 35
ESX servers not able to access an RDM disk associated with a shared datastore might cause failed discovery of RDM disk by Veritas InfoScale Operations Manager 36
Sometimes Internet Explorer displays a security warning when you navigate between pages in the console 36
Cannot configure an EMC CLARiiON enclosure on a Windows control host using a security file 36
Veritas InfoScale Operations Manager does not validate if the cluster node is managed by the Management Server during the VBS start operation 37

Chapter 4 Known issues 38

Management Server issues 38
Manual upgrade of a VRTS package fails if publisher is set to Symantec (3869503) 38
Delayed discovery of VMware VirtualCenter server by Control Hosts in Veritas InfoScale Operations Manager (2342314) 39
Authentication broker crashes while performing LDAP authentication (2017319) 39
XPRTLD daemon fails when Veritas InfoScale Operations Manager starts because of the corrupt AT pem files in the `VRTSsfmh` package (2145925) 40
Uninstalling Management Server removes the managed host package from a Storage Foundation for Windows host 42
Veritas InfoScale Operations Manager displays stale application status (2564572) 42
Manual refresh of HMC Server and VMware vCenter Server required after migration of virtual machines (2605533) 42
Performance metering of a VMware ESX server may not work properly after failover (2814844) 43
For VMware virtual machine, the virtual storage correlation is not functional if a SCSI controller of non-default type is used (3056561) 44
Erroneous managed host status reported in Veritas InfoScale Operations Manager high availability (HA) environment (2780631) 44
Information on running tasks is accurate only for managed hosts 6.0 and later (3077899) 45
Managed hosts previous to version 5.x are not listed for storage provisioning and volume migration 45
Veritas InfoScale Operations Manager does not discover virtual machines with same BIOS GUID on a Hyper-V Server (3509138) 45
Disk information for the cluster does not display correct data for host (3532746) 45
Disk correlation does not happen for LDOM storage container after enabling MPxIO on the SAN disks (3370824) 46
Qualsys scan may at times fail for port 5634 (2903776) 46
Managed host issues 46
Quick I/O cache value is not enabled after performing the storage provisioning operation on AIX managed hosts (2131183) 46

Thin LUNs on the hosts that run Storage Foundation for Windows 5.1 SP1 are not discovered as thin (2513466) 47
Add host operation fails for HP-UX managed hosts (2601265) 47
Unable to view performance graphs for VxVM disk and volume on Windows platform (3054870) 47
Cannot add a managed host to Management Server using the IPv6 address of the host (2816487) 48
Incorrect statistics returned by DMP if Storage Foundation version is prior to 5.0 MP3 (2796418) 48
Create disk group operation fails when triggered from slave node in a clustered configuration (3196104) 48
On HP-UX managed hosts, the path initiator and array port information is not displayed for some disks (3073128) 48
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) 48
Bandwidth tab displays incorrect data for a UNIX host (3484788) 49
CVR operations may not work correctly in case of managed host versions lower than 7.0(3745404) 49
Adding managed host versions lower than 7.0 to an upgraded 7.0 Management results in error 49
Management Server console displays incorrect version for ApplicationHA guests (3873640) 49
Unable to add older managed hosts to freshly installed Management Server 7.0 or 7.1 50
Management Server console displays incorrect version for ApplicationHA guests (3873640) 50
Unable to complete ‘add secondary’ workflow in some cases (3874690) 50
VRTSsfmh 7.1 and VxVM 7.0 co-existence issue on AIX (3870438) 51
Agentless discovery issues 51
Agentless configuration of hosts using IPv6 addresses fails (2414252) 52
Storage Insight Add-on issues 52
After the first discovery of IBM SVC array, manual refresh of putty cache may be required (3114164) 52
For locally replicated EMC Symmetrix LUNs, last synchronization time is available only for SYMCLI version 7.4 or later (3249430) 53

Manual discovery of Symmetrix enclosure is required when SYMCLI version is upgraded on the Storage Insight add-on discovery host (3289628) 53
Performance metering of enclosures may not work properly after failover (2814844) 53
Information on FAST managed storage groups for EMC Symmetrix VMAX enclosures is not discovered periodically (2842124) 54
Password file option does not work while configuring HP EVA enclosures on Windows hosts (2757601) 54
EMC Celerra enclosure details are not discovered for users with read-only access rights, and Imported Administrator or Operator role 55
Tier information is not displayed for some devices in a FAST managed storage group (2795204) 55
IBM System Storage DS enclosure discovery is not supported through HiCommand Server 7 in Veritas InfoScale Operations Manager (2708346) 55
Virtual Business Service issues 55
Virtual Business Service start operation does not validate the service group's resource criticality (2169223) 55
Storage Insight SDK Add-on issues 56
Edit and Test operations on Storage Insight Plug-in are not supported using Internet Explorer on 64-bit Windows hosts (2826079) 56
Storage Insight Plug-in upload operation sometimes fails on Internet Explorer Web browser (3485662) 56
Fabric Insight Add-on issues 56
SAN switch discovery fails when Veritas InfoScale Operations Manager Management Server, configured in high availability mode, is used as a discovery host (3513295) 56
Veritas HA Plug-in for vSphere Web Client issues 57
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) 57
High Availability tab is visible even after un-registration of vSphere plug-in in Veritas Operations Manager Management Server (3498886) 57
ApplicationHA Console single sign-on breaks after Veritas InfoScale Operations Manager 7.1 managed host installation or upgrade on ApplicationHA hosts 58

Some operations in HA console add-on tab may become unresponsive at time (3805588) 58
Other issues 58
Duplicate entries for the disks that are part of a virtual machine (2481982) 59
Unable to configure Management Server with a user name in Russian language using Firefox browser 59
Coexistence of ApplicationHA Console 6.0 and Veritas InfoScale Operations Manager 7.1 not supported (2739241) 59
Resource attributes not discovered for RVGPrimary Resource 59
Discovery of VMware VirtualCenter server or ESX server is not case–sensitive (2567318) 59
Offline instances not displayed in instance tab for MSSQL HA configuration (3516063) 60
Only one virtual machine configured as resource gets discovered (3488469) 60
A single host may have two entries on the host tab in certain conditions(3724295) 60
Incorrect virtual machine count in case of duplicate biosuuid (3782776) 60
Need to refresh the array for Datastore to NFS correlation 60
Special characters not allowed in the password while configuring the array (3677693) 61
Creating Atleast Dependency of resources for VCS 7.0 on windows is allowed 61
Resource dependency for VCS 7.0 on Windows cannot be viewed 61
Applicable hosts pane disappears if you filter hot fixes by platform (3874690) 61

Appendix A Getting help 62

Veritas InfoScale Operations Manager on the Web 62
Getting help 62
Using the product documentation 62

Chapter 1

Overview of this release

This chapter includes the following topics:

- About Veritas InfoScale Operations Manager
- New features and changes in Veritas InfoScale Operations Manager 7.1
- Issues fixed in the Veritas InfoScale Operations Manager 7.1 release

About Veritas InfoScale Operations Manager

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

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

In Veritas InfoScale 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 InfoScale Operations Manager deployment consists of the following:

- Management Server
- Managed hosts

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

- Virtualization environment

- SAN/NAS or Unified storage
- SAN fabrics

New features and changes in Veritas InfoScale Operations Manager 7.1

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

Ability to enable encryption

Starting with version 7.1, you can enable encryption for disk groups and volumes by selecting the **Enable Encryption** checkbox while creating a disk group or volume. The **Enable Encryption** check box is enabled for use only if the Key Management Server (KMS) client is configured on the host.

Note: 1. Encryption is supported only on Linux hosts.

2. Once you enable encryption, it cannot be disabled.

The following capabilities are not supported by volume encryption:

- Encryption of root and swap volumes
- Linked break-off snapshot of encrypted volumes
- Replication of encrypted volumes
- Encryption of existing volumes

For more information about creating disk groups and volumes, see the Managing hosts section in the *Veritas InfoScale™ Operations Manager 7.1 User Guide*.

For more information about encryption and KMS, see the *Storage Foundation Cluster File System High Availability 7.1 Administrator's Guide - Linux*.

Ability to set a host prefix for disks

Starting with version 7.1, you can set a host prefix for disks. You can use the **Set Host Prefix** wizard panel to enter the host prefix for the disks.

Note: This option is available only for Direct-attached storage (DAS).

For more information about setting host prefix , see the Managing hosts section in the *Veritas InfoScale™ Operations Manager 7.1 User Guide*.

Support for multiple cache areas, live performance charts, and more SmartIO tasks

Using Veritas InfoScale Operations Manager 7.1, you can configure multiple VxFS cache areas on the same system with SmartIO. You can also configure separate cache areas for Read and Writeback operations for the same filesystem. You can now specify the cache name.

The following SmartIO operations are now supported from the Management Server Console.

- Enable or disable SmartIO caching for specific mountpoints, volumes, or applications.
- Load files to a cache.
- Pin tablespaces or files to a cache or unpin tablespaces or files from a cache.

The Modify Cache menu is also updated in this release to allow you to specify a new cache size. The Modify Cache panel now displays the current cache size and the maximum available cache size.

SmartIO impact charts are also enhanced in 7.1. You can view live and six-hourly impact charts for SmartIO caching on Linux hosts. This is in addition to viewing charts for a day, week, month, or year. Volume and Disk level charts are now enhanced to display total reads, total writes, and average response time (with separate charts for average read latency and average write latency).

For more information, see the *Veritas™ InfoScale Operations Manager User Guide*.

Ability to determine optimal caching with SmartAssist

You can use the Management Server console to create and analyze I/O trace logs with the SmartAssist tool.

The SmartAssist tool lets you collect IO trace logs from a set of volumes, mount-points, disks, or diskgroups for a specified duration. The tool then analyzes the log to determine the optimal SmartIO cache size, related latency gain, and performance forecast.

You can also use the tool to perform similar analyses for any custom cache size that you plan to allocate.

Ability to control max IOPS for application co-existence

Veritas InfoScale Operations Manager 7.1 lets you balance application I/O requests so that multiple applications can co-exist on a common storage subsystem.

You can address this need by setting a maximum threshold on the I/O operations per second (IOPS) for the volumes of an application.

You can do so by setting limits or thresholds on the I/O operations per second (IOPS) for an application. You can use application volume groups (App VGs) to set the thresholds. An application volume group comprises a volume or group of volumes that are associated with an application. The available volumes in an App VG service I/O requests from an application until the application volume group reaches the maximum IOPS threshold. Thereafter Veritas Volume Manager (VxVM) throttles and queues the I/O requests. VxVM services the requests in the next available time interval on priority.

The Management Server Console also displays live charts for I/O operations per second (IOPS) for an application or App VG.

To support the above operations and live charts, the App VGs tab and Performance tab are added to the Management Server console, in this release.

Ability to map and unmap remote disks

Veritas InfoScale Operations Manager 7.1 lets you map a disk from a remote node in a cluster to a local node. You can use the mapped disk like other local storage on the node. You can also use the Management Server console to unmap the remote disk.

In the Management Server Console, you can view the mapped disk like other disks in the local storage list of the node. You can map a disk to multiple remote nodes. Mapping of disks is not persistent across cluster reboots. Mapping of disk groups is not supported the Management Server console. You can map disk groups from the command line. For details, see *Storage Foundation Administrator's Guide*.

Ability to discover Docker container information

Starting with release 7.1, Veritas InfoScale Operations Manager discovers host information under the Docker family. This information includes Docker images, Docker containers, and the storage that is exported to the containers. The information is polled and refreshed every 120 minutes.

Integration of InfoScale Access operations with Management Server console GUI

Veritas InfoScale Access Insight Add-on is introduced with Veritas InfoScale Operations Manager 7.1. The add-on allows you to directly manage multiple InfoScale Access clusters from the Management Server console GUI.

InfoScale Access is a software-defined scale-out network-attached storage (NAS) solution for unstructured data that works on commodity hardware. For more information, see Veritas InfoScale Access documentation.

Veritas InfoScale Operations Manager 7.1 Managed Host components are not released on HP-UX

In Veritas InfoScale Operations Manager 7.1, the VRTSsfmh package is not supported on managed hosts running the HP-UX operating system. This change has the following implications:

- You can upgrade Management Server to version 7.1. The upgraded management server seamlessly supports existing or new HP-UX managed hosts. To avail of this support, ensure that the HP-UX hosts are either running version 6.1 or version 7.0. Also ensure that the latest hot fixes are applied to the HP-UX managed hosts.
- You cannot upgrade existing HP-UX managed hosts to version 7.1.
- A newly-installed Management Server on version 7.1 does not support HP-UX hosts.

Issues fixed in the Veritas InfoScale Operations Manager 7.1 release

Table 1-1 lists the Management Server issues that have been fixed in the Veritas InfoScale Operations Manager 7.1 release.

Table 1-1 Issues fixed in Veritas InfoScale Operations Manager 7.1

Incident	Description
2530605	Remote switch operation fails between secure clusters.

Chapter 2

System requirements

This chapter includes the following topics:

- Operating system requirements
- Third-party required libraries
- System resource requirements
- Supported hardware
- Web browser requirements
- Network and firewall requirements
- About the consumption of the managed host components

Operating system requirements

For information on Operating system requirements for Veritas InfoScale Operations Manager 7.1, refer to the *Veritas InfoScale Operations Manager Hardware and Software Compatibility List (HSCL)* at the following URL:

https://www.veritas.com/support/en_US/article.000107928

Third-party required libraries

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

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

32-bit SNIA Common HBA API required on Windows hosts

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

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

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

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

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

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

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

System resource requirements

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

For Management Server:

Environment Size	CPU cores	Memory	Disk space
Small (up to 300 managed hosts)	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 InfoScale Operations Manager:

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

For a managed host:

- CPU cores: 1
- Memory: 1GB
- Disk space: 2GB
- Add 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, here:

https://www.veritas.com/support/en_US/article.000108276

About space estimation for data logs

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

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

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

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

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

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

Table 2-1 Space estimation for data logs

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

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
Enclosure	4	4	5 minutes	1 day	76	19
	4	8	2 hours	1 month	8	2
	4	8	1 day	1 year	190	46
File system	100	3	5 minutes	1 day	1423	14
	100	3	1 day	1 year	1784	18
Volume	100	4	1 minute	6 hours	2348	23
	100	4	5 minutes	1 day	1898	19
	100	4	2 hours	1 month	2348	23
	100	4	1 day	1 year	2379	24
Disk	100	4	1 minute	6 hours	2348	23
	100	4	5 minutes	1 day	1898	19
	100	4	2 hours	1 month	2347	23
	100	4	1 day	1 year	2379	23
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	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.
VVRBW	60	Bandwidth usage information for Volume Replicator (VVR).
Docker	120	Docker containters, docker images, and storage exported to containers.

Note: The discovery for the Storage Foundation and Cluster Server families is event driven and scheduled. This means that the discovery is triggered when configuration changes occur on the managed hosts. As a result, this information is updated in the Veritas InfoScale Operations Manager database in the following update. If configuration changes are not detected on the managed hosts, the communication between the managed host and Management Server is restricted to the heartbeat communication that occurs every five minutes.

See "System resource requirements" on page 17.

Supported hardware

For information on supported hardware for Veritas InfoScale Operations Manager 7.1, refer to the Veritas InfoScale Operations Manager Hardware and Software Compatibility List (HSCL) at the following URL:

https://www.veritas.com/support/en_US/article.000107928

See "Operating system requirements" on page 16.

See "System resource requirements" on page 17.

Web browser requirements

For information on Web browser requirements for Veritas InfoScale Operations Manager 7.1, refer to the *Veritas InfoScale Operations Manager Hardware and Software Compatibility List (HSCL)* at the following URL.

https://www.veritas.com/support/en_US/article.000107928

Network and firewall requirements

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

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

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

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

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

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

Port	Protocol	Initiator	Purpose	Effect if blocked
5634	TCP	Management Server	Management Server configuration	Management Server cannot be configured.
5636	TCP	Management Server	Management Server database configuration	Management Server cannot be configured.
5634	TCP		Management Server communications with the managed hosts	Managed host cannot be added to the Management Server domain.

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

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

Table 2-3 Default ports in a Veritas InfoScale 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.

See "Operating system requirements" on page 16.

See "System resource requirements" on page 17.

Internet Protocol version requirements

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

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

Table 2-4 IPV4 and IPV6 support

Components	IPV6	IPV4	Mixed Mode ((IPv4 and IPv6))
Management Server	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 25.

About the consumption of the managed host components

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

Various processes and services in Veritas InfoScale 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 InfoScale 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 21.

Chapter 3

Software limitations

This chapter includes the following topics:

- Veritas InfoScale Operations Manager 7.1 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 InfoScale Operations Manager 7.1
- Veritas InfoScale 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 Cluster Server
- Limitations related to the correlation between the disks and the disk groups
- Core density may not get calculated properly on HP-UX11iv2 hosts
- CIFS shares from NetApp and Celerra arrays that are mapped to a Windows host are not discovered

- Veritas InfoScale Operations Manager does not properly support clustered Veritas Volume Replicator (VVR)
- Limitations on SF operations on Windows CVM cluster
- Add host operation fails for RHEL 7 managed hosts
- ESX servers not able to access an RDM disk associated with a shared datastore might cause failed discovery of RDM disk by Veritas InfoScale Operations Manager
- Sometimes Internet Explorer displays a security warning when you navigate between pages in the console
- Cannot configure an EMC CLARiiON enclosure on a Windows control host using a security file
- Veritas InfoScale Operations Manager does not validate if the cluster node is managed by the Management Server during the VBS start operation

Veritas InfoScale Operations Manager 7.1 managed host not supported on AIX in Network Installation Manager

Installation of Veritas InfoScale Operations Manager 7.1 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 InfoScale 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 InfoScale 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 InfoScale Operations Manager console.

Backup and restore limitations in Veritas InfoScale Operations Manager 7.1

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 Veritas Technical Support.

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

Veritas InfoScale 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 InfoScale Operations Manager discovers LDoms.

Deployment-related limitations

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

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

- First upgrade to version 6.0, and then upgrade to version 7.1.

Windows Management Server high availability configuration limitations

Veritas InfoScale 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 InfoScale 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 InfoScale Operations Manager does not support discovery of disk slices for Solaris Zones virtualization. Veritas InfoScale Operations Manager supports only full disks.

Solaris Zones virtualization in Veritas InfoScale 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 InfoScale Operations Manager has the following discovery limitations for virtualization support:

- Veritas InfoScale Operations Manager does not support storage discovery for the Linux Kernel Virtual Machine (KVM) environment.
- For LPARs, Veritas InfoScale 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 Cluster Server

VCS configuration policy check in Veritas InfoScale Operations Manager does not report any violations if Cluster Server is not running on any of the systems in the cluster. Also, if the cluster has a single system and 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 InfoScale Operations Manager 7.1, 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 InfoScale 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 InfoScale Operations Manager does not properly support clustered Veritas Volume Replicator (VVR)

Veritas InfoScale 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.

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

This is applicable to VMware virtualization discovery using Veritas InfoScale 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 InfoScale Operations Manager.

Workaround:

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

Sometimes Internet Explorer displays a security warning when you navigate between pages in the console

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**.

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

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.

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

When you perform the Virtual Business Service (VBS) start operation, Veritas InfoScale Operations Manager does not check whether Management Server manages the cluster node. Veritas InfoScale 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.

Chapter 4

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
- Fabric Insight Add-on issues
- Veritas HA Plug-in for vSphere Web Client issues
- Other issues

Management Server issues

The following issues relate to Veritas InfoScale Operations Manager Management Server.

Manual upgrade of a VRTS package fails if publisher is set to Symantec (3869503)

The manual upgrade of any VRTS package fails with the following error message:

```
No updates available for this image.
```

This error occurs only when you manually upgrade the VRTS package through the command line interface. This issue is observed on systems running Oracle Solaris 11, with the publisher set to Symantec.

Workaround: Before performing a manual upgrade, you must unset the publisher as follows:

```
# pkg unset-publisher Symantec
# pkg set-publisher -p path to p5p for VRTS Veritas
# pkg install --accept VRTS package name
```

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

In Veritas InfoScale 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 InfoScale Operations Manager starts because of the corrupt AT pem files in the `VRTSsfmh` package (2145925)

The XPRTLD daemon fails when Veritas InfoScale 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
```

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

When you uninstall Veritas InfoScale 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 InfoScale Operations Manager displays stale application status (2564572)

This issue occurs with the virtual machines where 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 InfoScale 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 InfoScale 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 InfoScale 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 InfoScale 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 InfoScale 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.

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

This issue is encountered if a Veritas InfoScale 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 InfoScale 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 InfoScale 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.

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.

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 InfoScale Operations Manager version 5.x or later. Hosts with earlier versions are not listed for storage provisioning and volume migration operations.

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

Veritas InfoScale 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 InfoScale 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 InfoScale 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.

Qualsys scan may at times fail for port 5634 (2903776)

In the Management Server domain, the Qualsys scan may at times fail for port 5634.

Workaround:

In the `VRTSatlocal.conf` file, change the value of **SSLCipherSuite** attribute from **HIGH:MEDIUM:!eNULL:!aNULL:!SSLv2** to **RC4+SHA:!MD5:!aNULL:!eNULL:!SSLv2**. This file is located at the following locations:

- UNIX: `/var/opt/VRTSsfmh/sec/root/.VRTSat/profile/VRTSatlocal.conf`
- Windows: `\ProgramData\Symantec\VRTSsfmh\sec\systemprofile\VRTSatlocal.conf`

Managed host issues

The following issues relate to host management.

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 InfoScale 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.veritas.com/patch/detail/4697

After the successful installation, restart the host.

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

In the Veritas InfoScale 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.

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.

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 InfoScale Operations Manager 7.1.

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.

CVR operations may not work correctly in case of managed host versions lower than 7.0(3745404)

In cases where Management Server version is 7.0 and managed host version is lower than 7.0, some incorrect data may be discovered and displayed in the **Host** tab of the RVG.

Adding managed host versions lower than 7.0 to an upgraded 7.0 Management results in error

Any managed host version lower than 7.0 is not compatible with a Management Server that has been upgraded to 7.0.

If you upgrade your Management Server to 7.0 and then you try to add a managed host version that is lower than 7.0, it displays an improper error message that it is unable to communicate to the server.

Management Server console displays incorrect version for ApplicationHA guests (3873640)

This issue applies to environments where Veritas InfoScale components coexist with ApplicationHA.

If you install Veritas InfoScale Operations Manager Management Server 7.0 or later, the Management Server console displays incorrect version for Windows systems running ApplicationHA 6.x.

If you click **Licensing** > **Deployment Details**, the ApplicationHA version for systems with ApplicationHA 6.x, is displayed as 9.0.

Workaround

Perform the following steps.

1. Navigate to the following location on the Windows system running ApplicationHA.

   ```
   C:\Program Files\Veritas\cluster server\bin\
   ```

   Where C:\ is the system drive.

2. To view the correct ApplicationHA version, run the following command:

```
# had -version
```

Unable to add older managed hosts to freshly installed Management Server 7.0 or 7.1

This issue applies to fresh installations of Veritas InfoScale Manager Management Server 7.0 and 7.1.

If you install a Management Server with version 7.0 or 7.1, and then try to add managed hosts with a version lower than the respective Management Server version, an error message appears. The error message indicates communication failure between managed host and Management Server.

Management Server console displays incorrect version for ApplicationHA guests (3873640)

This issue applies to environments where Veritas InfoScale components coexist with ApplicationHA.

If you install Veritas InfoScale Operations Manager Management Server 7.0 or later, the Management Server console displays incorrect version for Windows systems running ApplicationHA 6.x. If you click **Licensing** > **Deployment Details**, the ApplicationHA version for systems with ApplicationHA 6.x, is displayed as 9.0.

Workaround

Perform the following steps to view the correct ApplicationHA version.

1. Navigate to the following location on the Windows system running ApplicationHA.

   ```
   c:\Program Files\Veritas\cluster server\bin\
   ```

   Where `c:\` is the system drive.

2. Run the following command:

   ```
   # hastart -version
   ```

   In the output, the Engine Version indicates the installed ApplicationHA version.

Unable to complete ‘add secondary’ workflow in some cases (3874690)

In a Cluster Volume Replication (CVR) environment, you may be unable to add a secondary for a replicated volume group (RVG). You may be unable to complete the 'add-secondary' workflow because in the disk-group creation menu, the option to create a shared disk group is disabled. This behavior occurs if you have not

already created a shared disk group on the host before you start adding the secondary.

Workaround

Create the required shared disk group from the cluster, and then start the 'add secondary' workflow.

VRTSsfmh 7.1 and VxVM 7.0 co-existence issue on AIX (3870438)

If VRTSsfmh 7.1 and VxVM 7.0 co-exist on an AIX host, the ‘vxdclid’ daemon may dump core with the following stack:

```
malloc_y()
malloc_common@AF105_87()
get_final_stats()
dmp_getstats()
collect_dmppath_iostats()
get_dmpstats()
logstats_work()
logstats_thread()
```

Workaround

1. Open the following file:

   `/etc/vx/dcli/sfm/conf/dcli_conf.ini file`

2. Comment out three lines from the file as follows:

   #DmpCtlrLog = /var/opt/VRTSsfmh/stats/1day.vrts_dmp_ctlr ;

   #DmpPathLog = /var/opt/VRTSsfmh/stats/1day.vrts_dmp_path ;

   #DmpEnclrLog = /var/opt/VRTSsfmh/stats/1day.vrts_dmp_enclr ;

3. Execute the following commands to restart 'vxdclid':

   # /opt/VRTSsfmh/bin/vxadm service stop

   # /opt/VRTSsfmh/bin/vxdclid

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.

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 InfoScale 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 InfoScale Operations Manager console to discover some of the Symmetrix ‘s features (for example, FAST) if the upgraded SYMCLI version supports those features.

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 InfoScale 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 7.1. 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 7.1. 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.

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 InfoScale 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 InfoScale Operations Manager 7.1 does not discover IBM System Storage DS enclosures using HiCommand Server 7.

Virtual Business Service issues

The following are Virtual Business Service issues

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.

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 InfoScale Operations Manager Management Server, configured in high availability mode, is used as a discovery host (3513295)

When Veritas InfoScale 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.

Veritas HA Plug-in for vSphere Web Client issues

The following issues are related to Veritas 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.

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:

- On vSphere 5.5U2: `C:\ProgramData\VMware\vSphere Web Client\vc-packages\vsphere-client-serenity`
- On vSphere 6.0: - `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-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.

ApplicationHA Console single sign-on breaks after Veritas InfoScale Operations Manager 7.1 managed host installation or upgrade on ApplicationHA hosts

When Veritas InfoScale Operations Manager 7.1 managed host is installed or upgraded on a host that has either ApplicationHA 5.1 Service Pack 2 or ApplicationHA 6.0 installed on it, the ApplicationHA Console single sign-on fails to work.

There is no workaround for the issue.

Some operations in HA console add-on tab may become unresponsive at time (3805588)

In the Veritas InfoScale Operations Manager web console, some of the operations on Symantec HA tab that launch new pop-up windows, become unresponsive at times. there is no way to move to or close the pop-up window.

Workaround:

Click another tab and then come back to the HA console add-on tab.

Other issues

This section lists additional issues that cannot be categorized in the rest of the Veritas InfoScale 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 InfoScale 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 InfoScale Operations Manager 7.1 not supported (2739241)

ApplicationHA console 6.0 and Veritas InfoScale Operations Manager 7.1 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 InfoScale Operations Manager.

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

While discovering VMware VirtualCenter server or ESX server, Veritas InfoScale 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 InfoScale Operations Manager.

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

A single host may have two entries on the host tab in certain conditions(3724295)

A single host may be displayed twice on the hosts tab in the following conditions:

- If the replication is configured but it does not get started.
- if the replication is incorrectly configured in a way that one of the links is detached.

Incorrect virtual machine count in case of duplicate biosuuid (3782776)

If there are multiple virtual machines in the Management Server domain with same biosuuid, there is incorrect virtual machine count displayed on the **Overview** tab for the VMware virtualization server under the **Virtualization** perspective.

Workaround:

For the correct count and discovery of the virtual machines, you need to configure unique biosuuid for the virtual machines.

Need to refresh the array for Datastore to NFS correlation

After configuring the array and the vCenter server ,you need to refresh the array to get the proper Datastore to NFS correlation.

Special characters not allowed in the password while configuring the array (3677693)

While configuring an array, if you provide a user-password that contains any special character, the configuration of the array may fail.

Creating Atleast Dependency of resources for VCS 7.0 on windows is allowed

Resource dependency for Veritas Cluster Server (VCS) 7.0 on Windows platform cannot be viewed in Veritas InfoScale Operations Manager 7.1 since Atleast Dependency feature is not supported on Windows platform for VCS 7.0. Still, Veritas InfoScale Operations Manager 7.1 incorrectly allows creating Atleast Dependency of resources for VCS version 7.0 on Windows.

Resource dependency for VCS 7.0 on Windows cannot be viewed

In Veritas InfoScale Operations Manager 7.1, you cannot view the resource dependency for Veritas Cluster Server (VCS) 7.0 on Windows.

Applicable hosts pane disappears if you filter hot fixes by platform (3874690)

In the Repository view of the Management Server console, if you try to filter available hot fixes by platform, the list of applicable hosts disappears.

To view this behavior, click **Settings** > **Deployment**. In the Repository view, expand **Hot Fixes** to navigate to **Veritas InfoScale Operations Manager Managed Host** in the left pane. In the Hot Fixes tab, the list of available hot fixes is displayed in the upper pane. In the lower pane, the list of applicable hosts is displayed. In the upper pane, if you try to select a platform from the **Platform** filter, the lower pane disappears from the display.

Workaround

Do one of the following

- Do not use the upper pane of the Hot Fixes tab. Navigate to the required host in the lower pane, and then apply the required hot fix.
- Do not use the Platform filter in the upper pane of the Hot Fixes tab. Scroll to the required hot fix, and then apply the hot fix.

Appendix A

Getting help

This appendix includes the following topics:

- Veritas InfoScale Operations Manager on the Web
- Getting help
- Using the product documentation

Veritas InfoScale Operations Manager on the Web

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

https://www.veritas.com/product/storage-management/infoscale-operations-manager

Getting help

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

For technical assistance, visit

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

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 InfoScale Operations Manager guides and Table A-2 lists the URLs for Veritas InfoScale Operations Manager documentation:

Table A-1 Names of Veritas InfoScale Operations Manager Guides

Title	Description
Veritas InfoScale Operations Manager Hardware and Software Compatibility List (HSCL)	The list of hardware and software compatibility, available here: https://www.veritas.com/support/en_US/article.000107928
Veritas InfoScale Operations Manager Release Notes	The release information such as new features, fixed issues, known issues, and limitations.
Veritas InfoScale Operations Manager Installation and Configuration Guide *Veritas InfoScale Operations Manager User Guide* *Veritas InfoScale Operations Manager Add-ons User Guide*	The information about Veritas InfoScale Operations Manager.
Veritas InfoScale Operations Manager Frequently Asked Questions	A list of frequently asked questions about Veritas InfoScale Operations Manager.
Veritas InfoScale Operations Manager Third-Party License Agreements	The information about the third-party software that is used in Veritas InfoScale Operations Manager.
Veritas InfoScale Operations Manager Quick Start Guide	The short and concise information about installation, configuration, and discovery of assets in Veritas InfoScale Operations Manager.

Table A-2 URLs for Veritas InfoScale Operations Manager documentation

URL	Description
https://sort.veritas.com/documents	The latest version of the product documentation.
http://www.veritas.com/community/videos/vom-videos	The list of How-to videos.
https://www.veritas.com/support/en_US/article.000108276	The late breaking news that is related to this release.

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