

Veritas InfoScale Operations Manager 8.0.2 Patch 400

Last updated: 2024-02-08

Legal Notice

Copyright © 2024 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
2625 Augustine Drive
Santa Clara, CA 95054
<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:

infoscaledocs@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	Enhancements in this patch	5
	New faults	5
	Update in Tomcat directory and files ownership	6
	Configuring SecureFS (immutable checkpoint)	6
	Immutable Checkpoint - File System Options	7
Chapter 2	Deprecated features	9
	Deprecated features	9
Chapter 3	Known issue	10
	Configure replication operation for encrypted volumes is not supported (15442)	10

Enhancements in this patch

This chapter includes the following topics:

- [New faults](#)
- [Update in Tomcat directory and files ownership](#)
- [Configuring SecureFS \(immutable checkpoint\)](#)

New faults

Fault for Veritas Volume Replicator

A new fault of type warning is implemented for Veritas Volume Replicator to identify when SRL and data volumes are on the same disk. The fault is raised on the RVG consisting of such SRL and data volume, and is then propagated to the respective host.

Fault message is '**SRL and data volumes are on the same disk**' and topic ID is '**event.alert.vom.vvr.datavol.srlvol.same.disk**'. The topic ID can be used to create rule in the Server perspective.

Fault for Veritas Cluster Server

A new fault of type error is implemented for VCS. The fault is raised on the remote cluster which shut down abruptly and is not able to update its resources or service groups status to the reporting Operations Manager Management Server.

VIOM Management Server is reporting the status of the remote cluster as faulted.

Fault message is '**Cluster is down. Administrative action is required.**' and topic ID is '**event.alert.vom.vcs.cluster.down**'. The topic ID can be used to create rule in the Availability perspective.

Update in Tomcat directory and files ownership

Ownership of the following directory and files has changed from **root:root** to **tomcat:tomcat**.

- /opt/VRTSsfmcs/webgui/tomcat/ dir
- /opt/VRTSsfmcs/webgui/tomcat/conf/context.xml 600
- /opt/VRTSsfmcs/webgui/tomcat/conf/catalina.properties 600
- /opt/VRTSsfmcs/webgui/tomcat/conf/catalina.policy 600
- /opt/VRTSsfmcs/webgui/tomcat/webapps 750
- /opt/VRTSsfmcs/webgui/tomcat/bin 750

Configuring SecureFS (immutable checkpoint)

In this patch release version 8.0.2.400, the secure file system feature is enhanced to identify the underlying application (Oracle) and then secure the file system accordingly. In the earlier version, SecureFS feature was available only for General Applications. However it is recommend that you install the patch if you want to use the SecureFS feature for general application or Oracle or both.

When you install the 8.0.2.400 patch and InfoScale 8.0.2 Update 2, you can configure immutable checkpoint on a file system that is mounted on a InfoScale volume. Immutable checkpoints are supported only on VxFS. Hence all directories including the sub directories should be VxFS mount points.

The feature supports General Applications, Oracle 19C, and Oracle 21C. Compliance (WORM) and Enterprise (SoftWORM) can be configured for all the listed applications.

To configure immutable checkpoint for Oracle application, ensure that you select the host and the volume on which Oracle is installed or configured.

For more information about how the feature works for Oracle application, refer to the Storage Foundation 8.0.2 Administrator's Guide - Linux documentation on [Veritas SORT](#).

To perform this task, your user group must be assigned the Admin role on the host or the Server perspective. The permission on the host may be explicitly assigned or inherited from a parent Organization.

To configure immutable checkpoint

- 1 In the Management Server console, go to the **Server** perspective and expand **Manage** in the left pane.
- 2 Expand **Organization** or **Uncategorized Hosts** to locate and select the host.
- 3 Expand the host and **Volumes** to locate the volume on which you want to configure immutable checkpoints.
- 4 Right-click the volume and select **File System > Configure SecureFS > Immutable Checkpoint**.
- 5 In the **Immutable Checkpoint - File System Options** panel, enter the required information.
See [“Immutable Checkpoint - File System Options”](#) on page 7.
- 6 Click **Finish** to secure the file system.

Immutable Checkpoint - File System Options

Use the **Immutable Checkpoint - File System Options** wizard panel to configure immutable checkpoints on an existing file system. Based on the file system that is selected, **General** or **Oracle** application type is displayed in the **Select Application** field. Use the drop-down option to change the system selected application type.

Fields mentioned in **Oracle options** table are displayed only if the selected host or volume has Oracle installed or configured.

Table 1-1 Oracle options

Field	Description
Orahome	Enter the directory path where Oracle is installed.
Username	Enter the username to access the application file.
SID	Enter the system identifier.

Table 1-2 Other options

Field	Description
Mode	Select between Compliance and Enterprise mode. Compliance (WORM) or Enterprise (SoftWORM) mode is set on the file system. Compliance (WORM) is the default mode which cannot be modified once configured. Although you can upgrade from Enterprise (SoftWORM) to Compliance mode.
Audit log	Logs certain events to persistent storage. Once enabled it cannot be disabled.
Checkpoint selection	
Interval	Specify the checkpoint frequency. You can select one of three options: hourly, daily, or weekly. Default selection is, every one hour.
Total checkpoints	Specify the total number of checkpoints that you want to set. Default selection is 1.
Retention	Specify the time for which the checkpoint should be retained. Based on the selected interval and total checkpoints the retention period is auto populated, however you can modify the value.

If checkpoints are already configured and you want to remove all the configurations, then select the **Unconfigure application checkpoints** checkbox. This clears all the checkpoints and the Oracle configurations if any on the selected volume.

See [“Configuring SecureFS \(immutable checkpoint\)”](#) on page 6.

Deprecated features

This chapter includes the following topics:

- [Deprecated features](#)

Deprecated features

The Ransomware and Corruption protection features, to secure a file system that is mounted on a InfoScale volume, are not available when you install this patch (8.0.2.400). The feature is documented in *InfoScale Operations Manager 8.0.2 Users Guide*, **chapter** *Managing file systems*.

If you have secured your files systems using these features in version 8.0.2, contact the Veritas Support team to reconfigure the files systems using the latest patch.

Known issue

This chapter includes the following topics:

- [Configure replication operation for encrypted volumes is not supported \(15442\)](#)

Configure replication operation for encrypted volumes is not supported (15442)

Using the Management Server console, you cannot perform the Configure replication operation on encrypted volumes. The operations fails.