

Veritas InfoScale Operations Manager 8.0.0 Patch 200

Last updated: 2022-08-30

Legal Notice

Copyright © 2022 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

VIOM Patch 8.0.0.200

This document includes the following topics:

- [Post-installation tasks for this patch](#)
- [Certificate expiry detection and renewal feature](#)
- [Implementing US Executive Order \(EO\) requirements](#)
- [Implementation of new VVR faults](#)

Post-installation tasks for this patch

After you install Patch 8.0.0.200 on a Veritas InfoScale Operations Manager (VIOM) Management Server, you need to upgrade below two add-ons if they are installed and enabled:

- Update Application Migration add-on to VRTSsfmappmig-8.0.0.200 or later.
- Update Veritas HA Plug-in for vSphere Web Client add-on to VRTSsfmhac-8.0.0.200 or later.

In case, if your Management Server is configured and running in FIPS mode, you may not be able to log in to VIOM GUI. To fix the issue, follow the steps:

1. Delete the `java.security` and `java.security.bkup` files from following location:

- a) `/opt/VRTSsfmcs/webgui/jre/lib/security/java.security`
- b) `/opt/VRTSsfmcs/webgui/jre/lib/security/java.security.bkup`

2. Take backup of existing `java.security` file and replace it with new file:

- a) `cd /opt/VRTSsfmcs/webgui/jre/conf/security/`
- b) `cp java.security java.security.bkup`
- c) `cp java.security.fips java.security`

3. Take backup of existing `setenv.sh` file and replace it with new file:

a) `cp /opt/VRTSsfmcs/webgui/tomcat/bin/`

b) `cp setenv sh setenv.sh.bkup`

c) `cp setenv.sh. fips setenv.sh`

4. Restart VIOM web server using the following

command: `/opt/VRTSsfmcs/bin/vomsc --restart web`

Certificate expiry detection and renewal feature

VIOM provides a provision to detect and renew VIOM Management Server and VIOM Agents certificates.

During the HOST discovery, VIOM performs the certificate expiry detection. If the expiry date of the certificate is found 120 days or less, then below fault appears on the VIOM GUI with number of remaining expiry days.

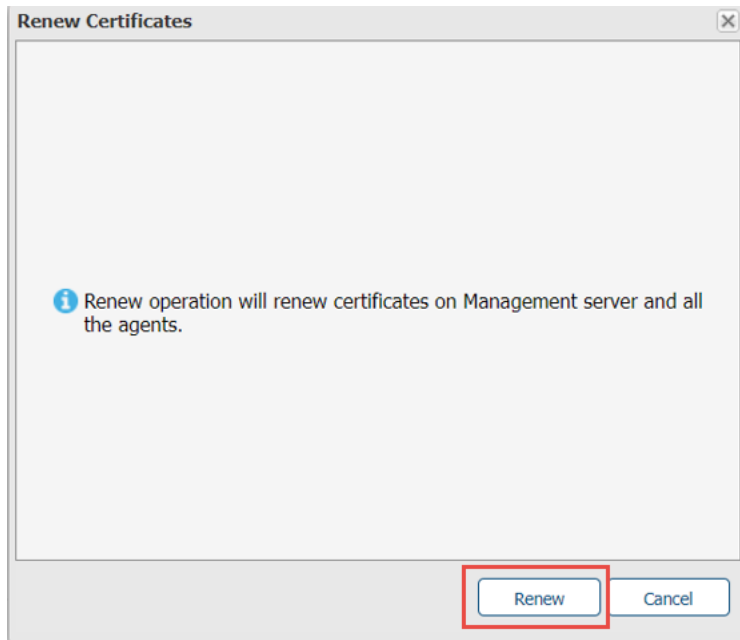
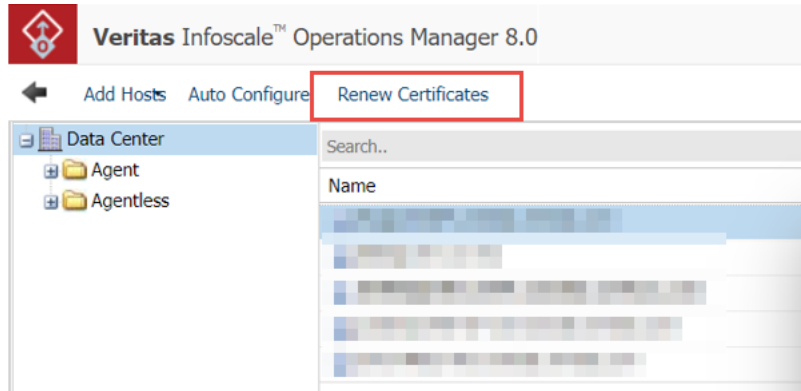
“VIOM certificates will be expired within %days_remaining% days. Renew certificates”

Whenever you see the fault in VIOM GUI, you need to perform renew certificates operation to renew the certificates. If you fail to renew the certificates in 120 days, then VIOM Management Server and Agents may stopped working.

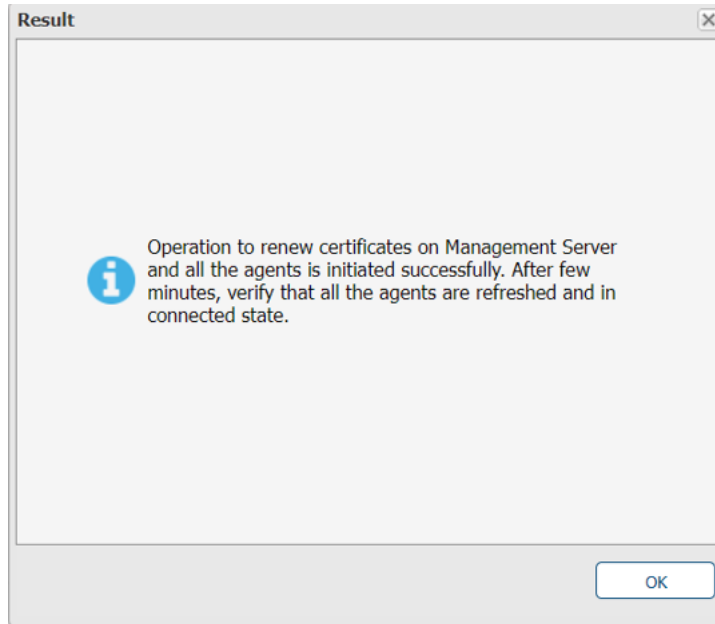
To renew certificates

You can start the certificate renewal process when your certificates are about to expire by performing the following steps:

1. On the VIOM Console, click **Settings > Host**.
2. Click the **Renew Certificate** option at the top of the menu bar. The **Renew Certificates** pop-up window opens.



3. Click the **Renew** button to renew the certificates.



Once Management Server and Agents certificates are successfully renewed, the fault disappears.

Note: While performing certificate renew operation, VIOM validates whether all the agents are in the connected and reachable state. In case if any Agent is not connected or not reachable then you must need to fix the communication issue to renew the certificates.

4. If you are using third party certificates for `sfm_agent` then VIOM will detect it. In this case, renew certificate operation will renew certificates on Management Server only and you have to manually run the `import_sfm_agent_certificate.pl` script to update `sfm_agent` certificates for VIOM Agents.

Implementing US Executive Order (EO) requirements

VIOM supports Event log management requirements (EL1) by US executive order.

If you want to implement the EO, you need to do the following steps manually:

1. In the `/opt/VRTSsfmcs/webgui/tomcat/conf/server.xml` file (Linux), inside `"Valve className="org.apache.catalina.valves.AccessLogValve"` tag, change the directory and log statement pattern as mentioned below:

- Change the directory tag to `directory="${web.log.dir}"`
- Change the pattern tag as follows:


```
pattern="%{yyyy-MM-dd}tT%{HH:mm:ss.SSSXXX}t ${hostName}
SourceIP=%a DestinationIP=%A &quot;%r&quot; %b StatusCode=%s
ResponseTime=%F milliseconds SessionID=%S
IncomingHeaders=&quot;%{User-Agent}i %{Content-Type}i %
{Accept}i %{Accept-Encoding}i %{Accept-Language}i %{Accept-
Charset}i&quot; OutgoingHeaders=&quot;%{Content-Type}o %
{Content-Length}o %{Server}o&quot;;"
```
- Add `maxDays` tag as follows:


```
maxDays="30"
```

Note: For Windows the file path is `C:\Program Files\Veritas\VRTSsfmcs\webgui\tomcat\conf\server.xml`

2. Restart **Web server**.

After you restart the Web server, you can see the new logs inside the `/var/opt/VRTSsfmcs/logs` directory.

Implementation of new VVR faults

VIOM Implements the following two new VVR faults:

- **SRL Disabled**
If RVG volume is SRL and state is 'DISABLED' then **SRL for RVG %obj_name%** is **disabled** fault gets raised. This is a part of VVR discovery.
- **RLINK detached**
If the Rlink state for RVG is 'DETACHED' then **Rlink for RVG %obj_name%** is **detached** fault gets raised. This is a part of VVR discovery.