Veritas InfoScale Operations Manager Patch 7.4.2.300

Last updated: 2021-02-26

VERITAS™

The truth in information.

Contents

Post installation tasks for the patch

After you install Patch 7.4.2.300 on a Veritas InfoScale Operations Manager (VIOM) Management Server and the managed hosts, update the following addons:

- Control Host (VRTSsfmch-7.4.2.300), which is applicable to the Management Server and the managed hosts. Update this addon if you have configured agentless hosts, virtualization servers like vCenter, HMC, and LPAR discoveries or storage arrays discoveries in the VIOM management console.
- Storage Insight addon (VRTSsfmsi-7.4.2.300), which is applicable to the Management Server only. Update this addon if you have configured storage array discoveries in the VIOM management console.

Removing or unconfiguring managed hosts using the API

VIOM now provides an API to remove or unconfigure managed hosts.

About VIOM web services APIs

The base URL to access the web service APIs is:

```
https://managementServerID:14161/vom/api
```

You can provide the host name, the fully qualified host name (FQHN), or the IP address of the Management Server as the value of *managementServerID*.

To fetch the attribute details of various InfoScale objects, use the `query` API as follows:

```
https://managementServerID:14161/vom/api/query
```

This API returns the URLs of all the `query` APIs that VIOM currently provides.

Note: To view the usage details of an API command, access the API by using a POST request or enter its URL directly in a browser.

For example:

- To view the URLs of all the APIs that allow you to perform VIOM operations, use the following URL:

  ```
  https://managementServerID:14161/vom/api/op
  ```

- To view the attribute details of all the managed hosts that are added to or configured on a Management Server, use the following URL:

  ```
  https://managementServerID:14161/vom/api/query/server/host
  ```

For details on VIOM API, refer to the *Veritas InfoScale Operations Manager User's Guide*.

To remove or unconfigure a managed host using the API

- Enter the following URL in a browser:

  ```
  https://managementServerID:14161/vom/api/op/infra/host/hostID/remove
  ```

You can identify the value of *hostID* for the managed host that you want to remove or unconfigure by using the `host` API that is described earlier.

To fetch the details of a managed host using the CLI

1. Before you can use the `query` API to fetch the details of a managed host, identify the session ID for the secure API login by using the following command:

   ```
   curl -g -k -d user="userName" -d password="userPassword" -d domain="managementServerID"
   https://managementServerID:14161/vom/api/login
   ```

   Specify the appropriate values of the username and password of the CMS.

   A sample session ID value is as follows:

   ```
   {"cookie":"JSESSIONID=2886C4EE175075D72C0AB91A1D9CF846;","current_server_time":"Mon Oct
   26 10:57:36 GMT-12:00 2020","max_active_interval":30,"expires_at":"Mon Oct 26 11:27:36
   GMT-12:00 2020"}
   ```

2. Fetch the host details by using the following command:

   ```
   curl -g -k -X POST -b "sessionID"
   https://managementServerID.com:14161/vom/api/query/server/host/
   ```

To remove or unconfigure a managed host using the CLI

- Run the following command to use the API to remove or unconfigure a managed host:

```
curl -g -k -X POST -b "sessionID"
https://managementServerID.com:14161/vom/api/op/infra/host/%7bhostID%7d/remove
```

Note:

- The `curl` command does not support the use of curly brackets, `{` and `}`. Replace `{` with `%7b` and `}` with `%7d` as the corresponding markup text.
- To be able to use this API with Google Chrome, install the RestMan addon.
- To be able to use this API with Mozilla FireFox, install the RESTClient addon.

Importing third-party certificates for xprtld

VIOM lets you import third-party certificates for the `xprtld` service on Management Servers that run on Linux. It also lets you import third-party certificates for the agents on AIX, Linux, and Solaris, provided that the agent version is 7.3.1 or later.

VIOM supports the use of a third-party certificate without a passphrase for `xprtld` that runs on port 5634. However, it only supports 2048-bit certificates.

To generate a third-party certificate for xprtld

1. Use the `openssl` command as follows to generate a private key and a certificate signing request (CSR):

```
openssl req -newkey rsa:2048 -nodes -keyout sfmAgentPrivateKeyFileName -out
sfmAgentCSRFileName
```

For example:

```
openssl req -newkey rsa:2048 -nodes -keyout sfm_agent.private.key -out sfm_agent.csr
```

2. The `openssl` command prompts you to provide some information that is to be added to the CSR. Specify the exact values that are provided in the following example:

```
Country Name (2 letter code) [XX]: .
State or Province Name (full name) []: .
Locality Name (eg, city) [Default City]: .
Organization Name (eg, company) [Default Company Ltd]: vx
Organizational Unit Name (eg, section) []: sfm_domain@nameOfCMS
Common Name (eg, your name or your server's hostname) []: sfm_agent
Email Address []: .
```

Note: The *nameOfCMS* value should match exactly with the value of the `cs_config_name` attribute that is present in the `/etc/default/sfm_resolv.conf` file on the Central Management Server (CMS).

Specify the exact values that are provided in the following example for this additional information that is also to be sent with the CSR:

```
A challenge password []: .
An optional company name []: .
```

3. Send the CSR file—for example, `sfm_agent.csr`—to your certificate signing authority and ask them to provide the corresponding certificate. The certificate should be provided in the `pem` format, along with the intermediate CA certificate and the root CA certificate, and it should support SSL clients. Veritas recommends that you assign a validity of 10 years to the certificate, or the maximum duration possible.
4. Optionally, run the following command to verify the purpose of the certificate, including the support for SSL clients:

```
openssl x509 -purpose -noout -in sfmAgentCertFileName
```

For example:

```
openssl x509 -purpose -noout -in sfm_agent.cert.pem
Certificate purposes:
SSL client : Yes
SSL client CA : No
SSL server : Yes
SSL server CA : No
Netscape SSL server : Yes
Netscape SSL server CA : No
```

5. Ensure that you have the following files ready before you import the certification on a Management Server:

File	Sample file name
Private key file for `sfm_agent`	`sfm_agent.private.key`
Certificate file for `sfm_agent`	`sfm_agent.cert.pem`
Certificate file for intermediate CA	`intermediate.cert.pem`
Certificate file for root CA	`ca.cert.pem`

To import a third-party certificate on a Management Server and on the agents

1. Copy all the files that are mentioned in the last step of the previous procedure on the Management Server at the appropriate location, for example: `/viom/certs/`.
2. Run the following command to import the certificates:

```
/opt/VRTSsfmh/bin/perl /opt/VRTSsfmh/util/import_sfm_agent_certificate.pl
--import_sfm_agent_cert --sfm_agent_certificate=/viom/certs/sfmAgentCertificateFileName
--sfm_agent_privatekey=/viom/certs/sfmAgentPrivateKeyFileName
--subCA_certificate=/viom/certs/intermediateCertificateFileName
--rootCA_certificate=/viom/certs/caCertificateFileName
```

For example:

```
/opt/VRTSsfmh/bin/perl /opt/VRTSsfmh/util/import_sfm_agent_certificate.pl
--import_sfm_agent_cert --sfm_agent_certificate=/viom/certs/sfm_agent.cert.pem
--sfm_agent_privatekey=/viom/certs/sfm_agent.private.key
--subCA_certificate=/viom/certs/intermediate.cert.pem
--rootCA_certificate=/viom/certs/ca.cert.pem
```

The certificates are imported on the agents automatically.

3. Follow the instructions and provide the appropriate input at the prompts that the command displays.

   You may encounter certain situations that you can address as follows:

   - The certificate import process restarts all the VIOM services on the Management Server and the `xprtld` service on all the managed hosts. After the certificate is successfully imported, if a managed host does not yet use the new certificate, check whether that host is registered on multiple Management Servers. If so, unconfigure the managed host from the Management Servers other than the one on which this new certificate was installed, and then restart the `xprtld` service on the host.
   - The certificate cannot be imported on the managed hosts that are on VIOM 7.3 or an earlier version. Upgrade such hosts to VIOM 7.3.1 or a later supported version (refer to the VIOM Hardware and Software Compatibility Lists document), and then run the command to import the certificate again.
   - The certificate cannot be imported on managed hosts that are unreachable from the Management Server. After the import process is complete, address the connectivity issue for the managed hosts that were unreachable. Then, add the managed hosts to the Management Server again; the new certificate gets automatically installed on the managed hosts.

Known issues in this patch

Issue 1: After you install Patch 7.4.2.300, the discovery of fabrics or switches from Brocade and Cisco may fail due to incorrect credentials.

Workaround: Reconfigure the fabrics and switches so that they can be discovered successfully.

Issue 2: After you install Patch 7.4.2.300, the two-factor authentication (2FA) for any existing credentials fails.

Workaround: Reset the pin; the new pin is then accepted by 2FA.

ABOUT VERITAS TECHNOLOGIES LLC

Veritas Technologies empowers businesses of all sizes to discover the truth in information—their most important digital asset. Using the Veritas platform, customers can accelerate their digital transformation and solve pressing IT and business challenges including multi-cloud data management, data protection, storage optimization, compliance readiness and workload portability—with no cloud vendor lock-in. Eighty-six percent of Fortune 500 companies rely on Veritas today to reveal data insights that drive competitive advantage. Learn more at veritas.com or follow us on Twitter at @veritastechllc.

Veritas World Headquarters
2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
www.veritas.com

For specific country offices
and contact numbers,
please visit our website.

VERITAS
The truth in information.