Preconfiguration validation

NetApp SMI-S Provider

NetApp
February 12, 2024

This PDF was generated from https://docs.netapp.com/us-en/smis-provider/concept-preconfiguration-task-overview.html on February 12, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Preconfiguration validation . . . 1
- Overview . . . 1
- Verify the CIM server status . . . 1
- Add a CIM server user . . . 2
- Verify that the storage system is working correctly . . . 2
- Generate a self-signed certificate for the CIM server . . . 3

Preconfiguration validation

Overview

Before using SMI-S Provider for the first time, you must validate your preliminary configuration.

Perform the following tasks before using SMI-S Provider:

1. From NetApp SMI-S Provider, verify that the CIM server is started.
2. Add a CIM server user.
3. Verify management of the storage system by adding at least one storage system for SMI-S Provider.
4. **Optional:** Generate a self-signed certificate for the CIMOM.

By default, authentication is enabled for SMI-S Provider.

After you have successfully performed this validation, you can begin to manage your storage systems using NetApp SMI-S Provider.

Verify the CIM server status

After installing NetApp SMI-S Provider, you must verify that the CIM server automatically started after you access SMI-S Provider.

Before you begin

You must already have login credentials as Administrator.

Steps

1. Log in as Administrator.
2. Access NetApp SMI-S Provider by navigating to the directory where the executables reside:

If you are using…	Then do this…
Command prompt (with elevated administrative privileges)	Navigate to `C:\Program Files (x86)\NetApp\smis\pegasus\bin`
Start > **Programs** menu	Right-click **NetApp SMI-S Provider** and select `Run as Administrator`.

3. View the CIM server status:

   `smis cimserver status`

   If the CIM server has been started, the following message is displayed:

   ```
   NetApp SMI-S Provider is running.
   ```

Add a CIM server user

Before you can validate the storage system, you must add a CIM user authorized to use the CIM server.

Before you begin

- You must already have logged in as Administrator.
- You must already have accessed SMI-S Provider.

Steps

1. Create a local user account.
2. Add the user to the Administrators group.

   For more information, see *System documentation*.

3. Add a CIM server user:

   ```
   cimuser -a -u user_name
   ```

   For example, to add a CIM server user named “chris”:

   ```
   cimuser -a -u chris
   ```

4. When prompted, enter and reenter the password.

Verify that the storage system is working correctly

Before SMI-S Provider can be configured, you must add at least one storage system to the CIMOM repository, and then verify that the storage system is working correctly.

Before you begin

- You must already have logged in as Administrator.
- You must already have accessed SMI-S Provider.

Steps

1. Add at least one storage system to the CIMOM repository:

To add a storage system with an…	Enter this command…
HTTP connection between the provider and the storage system	`smis add storage_sys storage_sys_user`
HTTPS connection between the provider and the storage system	`smis addsecure storage_sys storage_sys_user`

   The command waits for up to 15 minutes for the provider to update the cache and respond.

2. Verify the output for the following commands:

For this command…	Verify that…
`smis list`	The number of items matches the number of storage systems being managed.
`smis disks`	The number of disks matches the total number of disks on all storage systems.
`smis luns`	The number of LUNs matches the total number of LUNs on all storage systems.
`smis pools`	The number of ONTAP_ConcretePools matches the total number of aggregates on all storage systems.
`smis volumes`	The number of volumes matches the total number of volumes on all storage systems.

Generate a self-signed certificate for the CIM server

By default, SSL authentication is enabled for the CIM server. During the SMI-S Provider installation, a self-signed certificate for the CIM server is installed in the `pegasus` directory. You can generate your own self-signed certificate and use it rather than the default certificate.

Before you begin

- You must already have logged in as Administrator.
- You must already have accessed SMI-S Provider.

Steps

1. Download the `openssl.cnf` file from the following location: http://web.mit.edu/crypto/openssl.cnf
2. Move the `openssl.cnf` file to the bin directory:

   `%PEGASUS_HOME%\bin\openssl.cnf`

3. Set the `OPENSSL_CONF` environmental variable to the location of the `openssl.cnf` file:

   `C:\ >set OPENSSL_CONF=%PEGASUS_HOME%\bin\openssl.cnf`

   This only sets the environment variable for the duration of the current Command Prompt session. If you want to permanently set the environment variable, you can use one of the following options:

   - Navigate to **Properties > Environmental Variables** and update the variable under **System**.
   - Use Command Prompt to permanently set the variable:

     `setx OPENSSL_CONF "%PEGASUS_HOME%\bin\openssl.cnf`.

     The variable is set when you open a new Command Prompt session.

4. Navigate to the `%PEGASUS_HOME%\bin` directory:

   C:\cd %pegasus_home%\bin

5. Generate a private key:

   openssl genrsa -out cimom.key 2048

6. Generate a certificate request:

   openssl req -new -key cimom.key -out cimom.csr

7. Enter your information for the certificate request when prompted.
8. Generate the self-signed certificate:

   openssl x509 -in cimom.csr -out cimom.cert -req -signkey cimom.key -days 1095

   You can provide a different number of days for which the certificate is valid.

9. Copy the `cimom.key` and `cimom.cert` files to the `pegasus` directory (Windows: `C:\Program Files (x86)\NetApp\smis\pegasus`).

Result

The certificate date range starts at the current date and runs for the number of days specified.

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.