NetApp SMI-S Provider Documentation

NetApp SMI-S Provider

NetApp
August 30, 2024

Table of Contents

NetApp SMI-S Provider Documentation

Welcome to the NetApp SMI-S Provider Information Library. Here you will find documentation of NetApp SMI-S Provider software including how to install and manage NetApp SMI-S Provider, a command-based interface that detects and manages NetApp storage systems.

Documentation for earlier releases of NetApp SMI-S Provider are available on the NetApp Support Site.

NetApp SMI-S Provider Release Notes

The NetApp SMI-S Provider Release Notes describe new features, upgrade notes, fixed issues, known limitations, and known issues.

NetApp SMI-S Provider overview

Overview

NetApp SMI-S Provider 5.2.5 enables you to manage and monitor storage systems and to manage LUNs and volumes of storage systems, CIMOM configuration settings, and CIM server users.

NetApp SMI-S Provider is a command-based interface that detects and manages platforms that run ONTAP software. SMI-S Provider uses Web-Based Enterprise Management (WBEM) protocols, which enable you to manage, monitor, and report on storage elements.

NetApp SMI-S Provider follows schemas standardized by two organizations:

- Distributed Management Task Force (DMTF)
- Storage Networking Industry Association (SNIA)

SMI-S Provider replaces the use of multiple managed-object models, protocols, and transports with a single object-oriented model for all components in a storage network.

New in this release

- There is no upgrade path available for SMI-S Provider 5.2.5.
- You must deploy SMI-S Provider 5.2.5 as a new installation.

For Windows users:

- This release is not compatible with Windows Server 2012 or System Center Virtual Machine Manager (SCVMM) 2012.
- SMI-S Provider 5.2.5 supports Windows Server 2016, Windows Server 2019, SCVMM 2016 and SCVMM 2019.

Uses of NetApp SMI-S Provider

NetApp SMI-S Provider makes it easier for you to manage and monitor storage systems and to manage LUNs and volumes of storage systems.

You can use NetApp SMI-S Provider to manage storage controllers using System Center 2016 - Virtual Machine Manager or System Center 2016 - Virtual Machine Manager.

NetApp SMI-S Provider sizing and performance

Knowing the maximum number of systems managed by NetApp SMI-S Provider helps you understand its performance capabilities.

Sizing

NetApp SMI-S Provider can manage up to the following numbers of objects in clustered Data ONTAP:

- 100 storage virtual machines (SVMs) (without indications)
- 10 Storage Virtual Machines (with indications)
- 1,500 LUNs (per FlexVol volume)
- 200 CIFS file shares (per FlexVol volume)

If the FlexVol contains both qtrees and volumes, the qtrees appear as directories. You should be careful to not delete the qtrees accidentally when deleting volumes.

Performance notice

For configurations with 5,000 FlexVol volumes or 300,000 Snapshot copies, you might experience performance issues with the following `cimcli` commands:

- `cimcli ei ONTAP_Snapshot -n root/ontap`
- `cimcli ei ONTAP_SnapshotBasedOnFlexVol -n root/ontap`
- `cimcli ei ONTAP_StorageVolumeStats -n root/ontap`

The Interoperability Matrix Tool (IMT) contains the latest information about sizing and performance.

NetApp SMI-S Provider components

NetApp SMI-S Provider consists of three components that enable you to manage and monitor storage systems: CIMOM, provider objects, and a repository.

- **CIMOM**

  This is the foundation for NetApp SMI-S Provider. CIMOM collects, validates, and authenticates each application request and then responds to the application. It becomes a conduit for each request by invoking the appropriate provider to handle each request.

- **Provider objects**

  When a host issues a command or query to SMI-S Provider, CIMOM loads a shared library object, invokes it to handle a request, and returns the resulting information to the host.

  Windows hosts use DLL objects.

- **Repository**

  CIMOM uses a flat-file database for its repository. It stores persistent data required at the CIM level.

NetApp SMI-S Provider protocols

NetApp SMI-S Provider uses CIM-XML encoding over HTTPS and Service Location Protocol (SLP).

- **CIM-XML encoding over HTTPS**

  Protocol that exchanges information between a Web-Based Enterprise Management (WBEM)-enabled

management client and the CIMOM server. CIM-XML encoding over HTTPS uses the CIM protocol as the payload and HTTPS as the transport. HTTP is also supported.

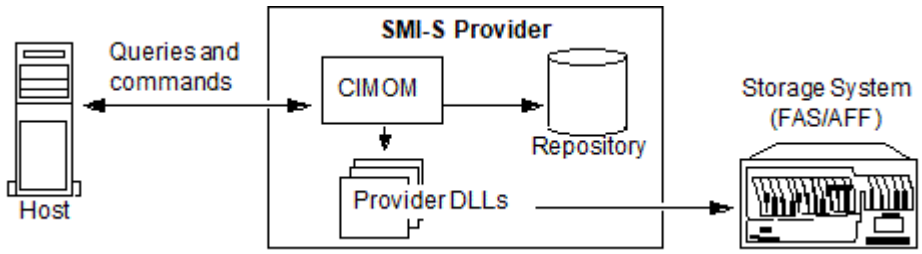
- **SLP**

  Discovery protocol that detects WBEM services within a LAN.

How NetApp SMI-S Provider interacts with a host

When a client application on a host discovers the CIMOM server by using SLP (CIM-XML encoding over HTTP), the client then queries the CIMOM for shared objects (objects modeled in the CIM language). The CIMOM loads shared objects and queries the storage system by using device-specific APIs for the requested information.

The following illustration shows how NetApp SMI-S Provider interacts with a WBEM management client when SMI-S Provider receives a query or command.

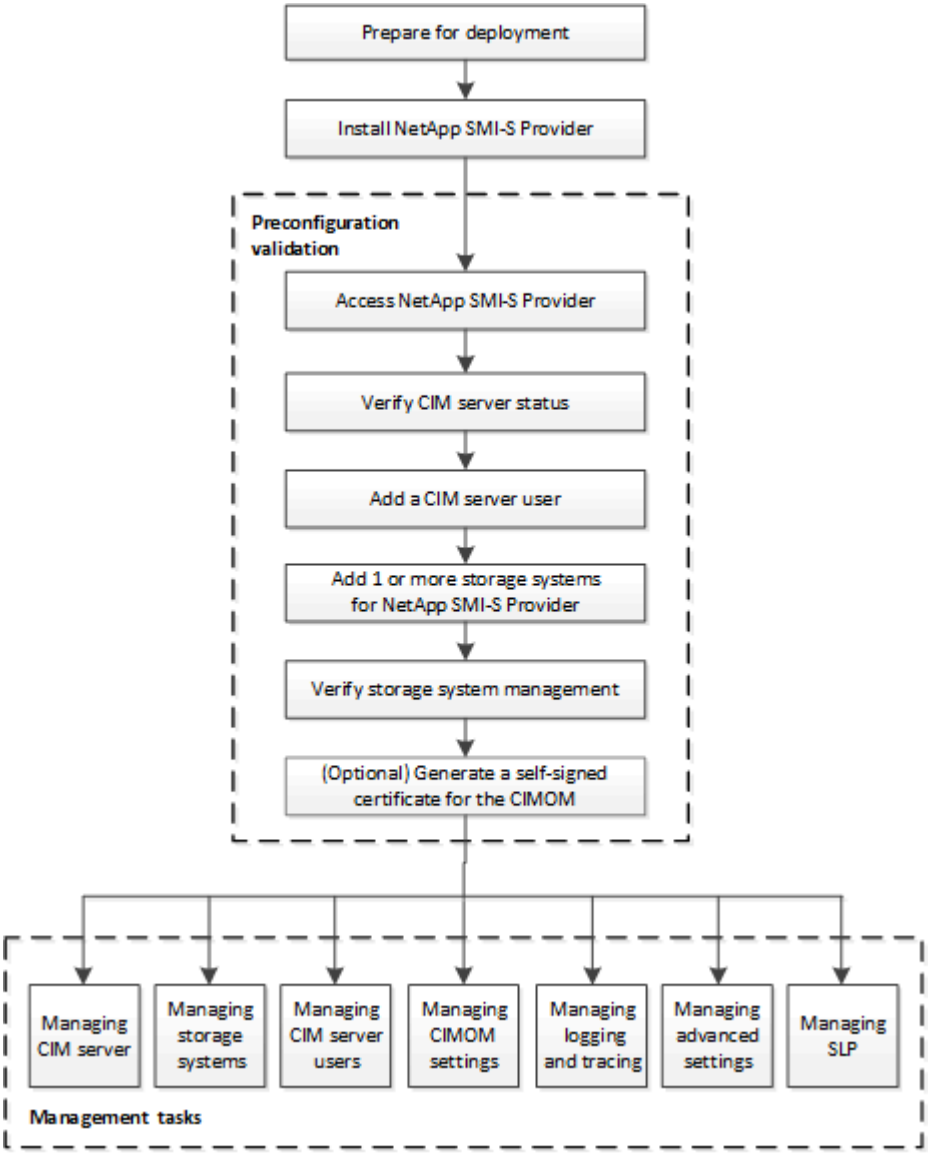


SMI-S profiles

SMI-S Provider uses profiles and subprofiles that comply with SMI-S v1.7. For information about SMI-S v1.7, see the SNIA: Technology Standards and Software page.

Deployment workflow

Before you can manage and monitor your storage systems using SMI-S Provider, you must install the SMI-S Provider software and validate your preliminary configuration.



Prepare for deployment

Overview

Before you deploy NetApp SMI-S Provider, you must verify that you have a supported operating system and platform, that you have the required licenses, and that your hosts meet the minimum requirements.

Supported operating system versions

Before installing SMI-S Provider, you must verify that the Windows host is running a supported operating system.

Operating system	Supported versions	Required client software
Windows	• Microsoft Windows Server 2016 • Microsoft Windows Server 2019	The Microsoft Visual C++ 2010 runtime libraries are automatically installed during the SMI-S Provider installation. To avoid potential issues related to runtime libraries, you must install Microsoft Visual C++ 2010 Redistributable Package (x86). from the following location: http://www.microsoft.com

SCVMM 2016 UR 2.1 requirement

System Center Virtual Machine Manager (SCVMM) 2016 Update Rollup (UR) 2.1 is required to manage NetApp File Server with NetApp SMI-S Provider 5.2.4 and later.

Without this UR, SCVMM 2016 displays the value of the `Total Capacity` and `Available Capacity` options as **`0 GB`** for the existing file shares in NetApp File Server.

To run SMI-S Provider, the provider host machine must meet the following specifications:

- The provider host machine cannot be used to host a Hyper-V node.
- SCVMM must not be running on the provider host machine.
- The provider host machine must not run other programs that are memory-intensive.
- The provider host machine must not run SMI-S providers from any other vendor.

The following hypervisors are supported:

- Microsoft Windows Server 2016 Hyper-V
- VMware ESX 5.0
- VMware ESX 5.1
- VMware ESX 5.5
- VMware ESX 6.0

Hardware requirements

You must verify that the Windows host meets the minimum hardware requirements before installing NetApp SMI-S Provider.

Hardware	Requirements
Memory	• 4 GB RAM (minimum) • 8 GB RAM (recommended)
Disk space	• 1 GB (minimum) • 4 GB (recommended) Enabling logging and tracing requires additional disk space of up to 1 GB, depending on the log and trace file rotation settings. You must have 100 MB temporary disk space available for installation.
CPU	• Dual-core 2.0 GHz (minimum) • Quad-core 2.0 GHz (recommended)

Required licenses

To use NetApp SMI-S Provider, you must have the required licenses.

The following licenses are required for NetApp SMI-S Provider:

- FCP, iSCSI, or both FCP and iSCSI licenses are required for creating LUNs on the storage systems.
- A CIFS license is required for creating file shares on supported ONTAP storage systems.
- A FlexClone license is required to create LUN clones on clustered storage systems running supported ONTAP versions.

Supported cluster platforms

NetApp SMI-S Provider supports cluster platforms that run Data ONTAP 8.3.2 and ONTAP 9 and later.

For NetApp SMI-S Provider to create clones of storage volumes (LUNs), you must have installed a FlexClone license on the storage system.

NetApp SMI-S Provider supports the following platforms:

- FAS series systems
- V-Series storage systems

Download the NetApp SMI-S Provider software package

Before installing NetApp SMI-S Provider, you must download the software package from the NetApp Support Site.

Before you begin

You must have created a NetApp Support Site account from NetApp Support.

Steps

1. Go to the **Downloads** > **Software** page at the NetApp Support Site.
2. Locate SMI-S Provider (formerly Data ONTAP SMI-S Agent) and select Windows operating system, and then click **Go!**.
3. Select the version to download by clicking **View & Download**.
4. From the **Software download** section, click **CONTINUE**.
5. Read and accept the End User License Agreement.
6. Select the software package file, and then save it to your desired location.

Install NetApp SMI-S Provider

Install NetApp SMI-S Provider on a Windows host

You can install NetApp SMI-S Provider software so that you can manage storage systems that run Data ONTAP. However, you cannot revert or downgrade to an earlier version. By default, the NetApp SMI-S Provider software is installed in the `C:\Program Files (x86)\NetApp\smis\pegasus` directory.

Before you begin

You must already have the following credentials and software:

- Login credentials for the Windows Administrator account
- NetApp SMI-S Provider software package

About this task

As a result of the installation process, the CIMOM service (named “NetApp SMI-S Provider” in Service Control Manager) and SLP daemon (named “Service Location Protocol” in Service Control Manager) run as automatic services that will automatically start even after a host reboot.

This installation procedure reflects a fresh install.

Steps

1. Log in as Administrator.
2. Navigate to the directory that contains the NetApp SMI-S Provider software package (`smisprovider-`*`version_number`*`.msi`), and then double-click the package name.
3. Complete the steps in the setup wizard.

Result

NetApp SMI-S Provider is started automatically toward the end of the installation process.

Uninstall NetApp SMI-S Provider

Uninstall NetApp SMI-S Provider from a Windows host

You can uninstall SMI-S Provider as needed. For example, depending on the version of your existing installation, you might need to uninstall the existing installation of SMI-S Provider before you can install the latest version.

About this task

If you plan to uninstall SMI-S Provider and want a clean reinstall, you must manually delete all of the content from the CIM server.

If you do not want a clean reinstall, SMI-S Provider retains the configuration, user, and other database files after the uninstall.

Steps

1. Log in as Administrator.
2. Uninstall NetApp SMI-S Provider from a Windows host by using the Windows Add/Remove Programs utility.

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.

Manage the CIM server

You can use SMI-S Provider to start, stop, and restart the CIM server and to review its status.

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in to the host system as Administrator.

Steps

1. Access NetApp SMI-S Provider.
2. Complete one of the following actions:

Action	Command	Additional information
Start the CIM server	`smis cimserver start`	After entering the command, a status message appears every three minutes. If an attempt to reach the CIM server fails, five more attempts are made to contact the server.
Stop the CIM server	`smis cimserver stop`	NA
Restart the CIM server	`smis cimserver restart`	NA
View the CIM server status	`smis cimserver status`	NA

Manage storage systems

You can use NetApp SMI-S Provider commands to add, delete, and list storage systems in the CIMOM repository. You can also list NFS and CIFS exports and exported LUNs for storage systems.

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in to the host system as Administrator.

About this task

For ONTAP, you must specify a management IP address for an SVM, not a cluster IP address, and you must provide the credentials for a vsadmin user. SMI-S Provider does not support cluster IP addresses or node management IP addresses, nor does it support node admin or node SVMs.

You should set the data protocol value to `none` for the management LIF when you add it to the SMI-S Provider.

Steps

1. Access NetApp SMI-S Provider.
2. Complete one of the following actions:

Action	Command	Additional information
Add a storage system with an HTTP connection between the provider and the storage system	**`smis add`** ***`storage_sys storage_sys_user`***	The command waits for up to 15 minutes for the provider to update the cache and respond.
Add a storage system with an 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.
List NFS and CIFS exports for a storage system	**`smis exports`**	None
List the storage systems for the CIMOM repository	**`smis list`**	You can run this command to verify the storage systems in the CIMOM repository before adding or deleting storage systems.
List exported LUNs for a storage system	**`smis luns`**	None

Action	Command	Additional information
Delete a storage system from the CIMOM repository	**smis delete *storage_sys***	If you no longer need to manage a storage system, you can delete it from the CIMOM repository. Because SMI-S Provider gathers information from all storage systems in the CIMOM repository, you should delete an unused storage system from the repository to maintain optimal performance.
List the current CIM server configuration information	**smis config show**	None
List the FC and iSCSI port information for storage system	**smis initiators**	None
List the storage pools for storage system	**smis pools**	None
List the traditional and flexible volumes for storage system	**smis volumes**	None

Manage CIM server users

Overview

You can use SMI-S Provider to add and remove CIM users that are authorized to use the CIM server. You can also list all current CIM users and modify their passwords.

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in to the host system as Administrator.

Steps

1. Access NetApp SMI-S Provider.
2. Create a local user account.
3. Add the user to the Administrators group.

   For more information, see *System documentation*.

4. Complete one of the following actions:

Action	Command	Additional information
Add a CIM server user	**`cimuser -a -u user_name`**	After entering the command, enter and reenter the password when prompted.
List the current users authorized to use the CIM server	**`cimuser -l`**	NA
Change the password for a CIM server user	**`cimuser -m -u user_name`**	After entering the command, enter and reenter the new and old password when prompted.
Remove a CIM server user not authorized to use the CIM server	**`cimuser -r -u user_name`**	NA

Types of CIM users and associated operations

When using SMI-S Provider, there are various types of user that you can assign to a user to control their access to the CIM server.

Starting with this release, the Domain user is allowed to modify the SMI-S Provider user database and other configuration settings as a Domain user of the Local Administrators group.

The following table lists the supported users of the CIM server and the operations that each type can perform.

Type of user	Operations
Domain administrator of the Administrators group	SMI-S Provider configuration and user management using `cimconfig` and `cimuser` commands. For example: • Add or remove a user to or from the trust store of SMI-S Provider. • Enable, disable, or change the log level and tracing configuration. • Enable or disable the authentication engine in SMI-S Provider. Storage management and verification using `smis` and `cimcli` commands. For example: • Add or remove storage controllers or SVMs to or from a SMI-S Provider repository or database or cache. • Refresh storage controllers or SVMs in SMI-S Provider cache. • Verify storage controller or SVM management. SCVMM discovery operations using the SCVMM GUI.
Domain user of the Local Administrators group	
Local user of the Local Administrators group	
Built-in Domain Administrator user	
Built-in Local Administrator user	
Domain user of the Users group	SCVMM discovery operations using the SCVMM GUI.
Local user of the Users group	

If you have SMI-S Provider on a Windows host and changed any “Administrator” user name, you must log out of the system and then log back in. The SMI-S Windows Service inherits authentication during this time; as a result, any change to the credentials are not recognized until the administrator logs out and then logs in again.

Manage CIMOM configuration settings

You can use SMI-S Provider to manage the CIMOM configuration, such as enabling or disabling HTTP and HTTPS connections and changing HTTP and HTTPS port numbers. By default, HTTP connections are enabled, allowing clients to connect to the CIM server without using SSL encryption.

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in to the host system as Administrator.

About this task

If your environment requires encrypted traffic to and from the CIM server, you must first disable HTTP connections and then verify that HTTPS connections for the CIM server are enabled.

Steps

1. Access NetApp SMI-S Provider.
2. Complete one of the following actions:

Action	Command	Additional information
Enable the HTTP connection	**cimconfig -s enableHttpConnection=true -p**	NA
Disable the HTTP connection	**cimconfig -s enableHttpConnection=false -p**	NA
Enable the HTTPS connection	**cimconfig -s enableHttpsConnection=true -p**	NA
Disable the HTTPS connection	**cimconfig -s enableHttpsConnection=false -p**	NA
Modify the HTTP port number	**cimconfig -s httpPort=*new_port_number* -p**	By default, the HTTP port number is 5988. If you wanted to change it to 5555, for example, you would input this command: **cimconfig -s httpPort=5555 -p**

Action	Command	Additional information
Modify the HTTPS port number	**cimconfig -s httpsPort=*new_port_number* -p**	By default, the HTTP port number is 5989. If you wanted to change it to 5556, for example, you would input this command: **cimconfig -s httpsPort=5556 -p**

3. Restart the CIM server:

   smis cimserver restart

Manage logging and tracing

Overview

You can configure how SMI-S Provider manages log and trace files, such as specifying the levels of messages to be logged and the directory to which logs are saved. You also specify the components to be traced, the target to which trace messages are written, the level of tracing, and the trace file location.

Configure log settings

By default, all system messages are logged. In addition, by default, the system message logs are located in the `logs` directory in the directory in which NetApp SMI-S Provider is installed. You can change the location of and the level of system messages that are written to the CIM server log. For example, you can choose to have logs stored in a directory that you specify and have only fatal system messages written to the CIM server log.

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in to the host system as Administrator.

Steps

1. Access NetApp SMI-S Provider.
2. Complete one of the following actions:

Action	Command	Additional information
Change the system message logging level	**cimconfig -s logLevel=*new_log_level* -p**	If you wanted to change the logging level to “INFORMATION”, for example, you would input this command: **cimconfig -s logLevel=INFORMATION -p**
Change the system message log directory	**cimconfig -s logdir=new_log_directory -p** If the *new_log_directory* contains space, you must enclose it in quotation marks (**"***new log directory***"**).	If you wanted to change the log directory to “serverlogs”, for example, you would input this command: **cimconfig -s logdir=serverlogs -p**

3. Restart the CIM server:

   smis cimserver restart

Logging levels

You can specify the types of messages that are logged (for example, you want only fatal system messages to be logged).

You can configure the logging level to one of the following:

- **TRACE**

  Saves trace messages in the cimserver_standard log.

- **INFORMATION**

  Logs all (informational, warning, severe, and fatal) system messages.

- **WARNING**

  Logs warning, severe, and fatal system messages.

- **SEVERE**

  Logs severe and fatal system messages

- **FATAL**

  Logs only fatal system messages.

Manage tracing

You can configure how SMI-S Provider manages trace files, such as specifying the components to be traced, the target to which trace messages are written, the level of tracing, and the trace file location.

Specifying trace settings

Having tracing enabled is important for gathering information for troubleshooting. However, having tracing enabled can impact performance, so carefully consider what must be traced and how long you need tracing enabled.

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in to the host system as Administrator.

Steps

1. Access NetApp SMI-S Provider.
2. Specify various trace settings as applicable:

Action	Command
Specify the components to be traced	**cimconfig -s traceComponents=*components* -p**
Specify the trace facility	**cimconfig -s traceFacility=*facility* -p**
Specify the location of the trace file	**cimconfig -s traceFilePath=*path_name* -p**
Specify the trace level	**cimconfig -s traceLevel=*level* -p**

3. Restart the CIM server:

   smis cimserver restart

Trace setting values

You can specify the components to trace, the trace target, and the level of tracing. Optionally, you can change the name and location of the trace file if you do not want to use the default trace file name and location.

You can configure the following trace settings:

- **traceComponents**

  Specifies the components to be traced. By default, all components are traced.

- **traceFacility**

  Specifies the target to which trace messages are written:

  - File

    This is the default value, which specifies that trace messages are written to the file specified by the traceFilePath configuration option.

  - Log

    Specifies that trace messages are written to the cimserver_standard log file.

- **traceFilePath**

  Specifies the location of the trace file. By default, the trace is file is named `cimserver.trc` and is located in the `traces` directory.

- **traceLevel**

  Specifies the level of tracing. By default, tracing is disabled.

Trace level	Trace messages written
0	Tracing is disabled.
1	Severe and log messages.
2	Basic flow trace messages (low data detail)
3	Inter-function logic flow (medium data detail)
4	High data detail
5	High data detail + Method enter and exit

Specify trace file size

If tracing is enabled, the maximum trace file size is 100 MB by default. You can increase or decrease the maximum trace file size by setting the environment variable `PEGASUS_TRACE_FILE_SIZE`. The value of the trace file size can be 10 MB through 2 GB.

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in to the host system as Administrator.

Steps

1. Access NetApp SMI-S Provider.
2. Create a system or user environment variable named `PEGASUS_TRACE_FILE_SIZE` with the new trace file size in bytes.

   Windows documentation has more information about creating environment variables.

3. Restart the CIM server:

   ```
   smis cimserver restart
   ```

Specify the number of trace files saved

If tracing is enabled, seven trace files are saved by default. If you need more trace files saved, you can increase the maximum number of trace files saved by setting the environment variable `PEGASUS_TRACE_FILE_NUM`. If you increase the maximum number of trace files saved, you must ensure that the system has enough space on its hard drive to accommodate the trace files.

Before you begin

- You must already have login credentials as Administrator.

- You must already have logged in to the host system as Administrator.

About this task

If tracing is enabled, tracing information is written to the `cimserver.trc` file. The trace files are rotated. When `cimserver.trc` reaches the maximum trace file size, its contents are moved to the `cimserver.trc.n` file. By default, `n` is a value from 0 through 5. If you need more trace files saved, you increase the value of *n*.

Steps

1. Access NetApp SMI-S Provider.
2. Create a system or user environment variable named `PEGASUS_TRACE_FILE_NUM` with the new number of trace files saved.

   Windows documentation has more information about creating environment variables.

3. Restart the CIM server:

   `smis cimserver restart`

Enable or disable audit log for SMI-S commands

All incoming SMI-S commands are recorded in audit log files, which enables auditors to track activities of WBEM client operations and provider use. You can enable or disable the logging of these incoming commands by setting a dynamic configuration property.

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in to the host system as Administrator.

About this task

Audit log data can provide a record of access, activity, and configuration change for a CIM server. The contents of the audit file include what command was issued, by whom the command was issued, and what time the command was issued.

The dynamic configuration property `enableAuditLog` enables or disables audit logging at run time. By default, enableAuditLog is set to true.

The common practice is to leave audit logging enabled.

The audit log file (`cimserver_auditlog`) is stored in the pegasus log directory (`C:\Program Files (x86)\Netapp\smis\pegasus\logs`).

The maximum size of the audit log file is 10 MB. After reaching the maximum limit, the file is renamed `cimserver_auditlog.0`, and a new `cimserver auditlog` file is created to collect the newer audit logging information.

NetApp SMI-S Provider maintains the six most recent audit log files: `cimserver_auditlog.0` through `cimserver_auditlog.5`.

Steps

1. Access NetApp SMI-S Provider.
2. Set the audit logging of SMI-S commands at runtime:

Action	Command
Enable SMI-S audit logging	`cimconfig -s enableAuditLog=true`
Disable SMI-S audit logging	`cimconfig -s enableAuditLog=false`

Manage SMI-S Provider advanced settings

Overview

You can manage advanced settings for SMI-S Provider, such as specifying the SMI-S cache refresh interval, ONTAPI timeout, and maximum number of threads per message service queue.

Specify the SMI-S Provider automatic cache refresh interval

By default, SMI-S Provider automatically retrieves information from storage systems every five minutes (300 seconds). You can set the automatic cache refresh interval (`CACHE_REFRESH_SEC` environment variable) to a value from 300 through 86400 seconds (24 hours).

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in to the host system as Administrator.

About this task

If you want to manually refresh the state of the storage system at any time, you can use the `smis refresh` command.

Steps

1. Access NetApp SMI-S Provider.
2. Create a system or user environment variable named `CACHE_REFRESH_SEC` with the new refresh interval value (in seconds).

   For information about creating environment variables, see your Windows documentation.

3. Restart the CIM server:

   ```
   smis cimserver restart
   ```

Specify the concrete job lifetime value

SMI-S Provider tracks the progress of asynchronous operations by creating *concrete jobs*. You can increase the concrete job lifetime from the default of 60 minutes (3600 seconds) to a value through 86400 seconds (24 hours).

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in to the host system as Administrator.

Step

1. Create a system or user environment variable named `JOB_LIFETIME_SEC` with the new lifetime value (in

seconds).

For information about creating environment variables, see your Windows documentation.

Specify the ONTAPI timeout value

SMI-S Provider makes ONTAP API (ONTAPI) calls to storage systems. By default, the ONTAPI timeout is 300 seconds. You can set the timeout to a value from 60 to 300 seconds.

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in to the host system as Administrator.

Step

1. Create a system or user environment variable named `ONTAPI_TIMEOUT_SEC` with the new timeout value (in seconds).

   For information about creating environment variables, see your Windows documentation.

Specify the maximum number of threads per message service queue

By default, SMI-S Provider allows 80 threads per message service queue. You can specify the maximum thread value as 1 through 5000. Increasing the maximum number of threads can impact the SMI-S Provider machine's performance, so carefully consider whether you need to increase this value.

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in to the host system as Administrator.

About this task

If your trace file shows many lines of `insufficient resources` output, you must increase the number of threads in increments of 500.

If you set the maximum number of threads to fewer than 20, using the **`cimcli -n root/ontap niall`** command, the provider becomes unresponsive and returns the `Insufficient threadpool` message in the trace file. If this occurs, you must increase the number of threads in increments of 500 and then restart the provider.

Steps

1. Access NetApp SMI-S Provider.
2. Create a system or user environment variable named `PEGASUS_MAX_THREADS_PER_SVC_QUEUE` with the new maximum thread value.

   For information about creating environment variables, see your Windows documentation.

3. Restart the CIM server:

```
smis cimserver restart
```

Enable or disable authentication for NetApp SMI-S Provider

By default, authentication is enabled for SMI-S Provider. If authentication causes errors on your system, you can optionally disable it. If authentication has been disabled and you want to reenable it, you can do so.

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in as Administrator.
- Any client, including System Center Virtual Machine Manager (SCVMM), must be connected to the provider using cimuser and cimpassword.

Steps

1. Access NetApp SMI-S Provider.
2. Set the authentication for SMI-S Provider:

Action	Command
Enable authentication if previously disabled	`cimconfig -p -s enableAuthentication=true`
Disable authentication	`cimconfig -p -s enableAuthentication=false`

   CIMOM does not use Windows authentication.

3. Restart NetApp SMI-S Provider:

```
smis cimserver restart
```

Enable indications in SMI-S Provider

Alert, FileSystem Quota, and Lifecycle indications are disabled by default. You can enable these indications by setting the environment variable `PEGASUS_DISABLE_INDICATIONS` to `false`.

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in to the host system as Administrator.

About this task

When `PEGASUS_DISABLE_INDICATIONS` is set to `false`, then Alert (`ONTAP_AlertIndication`),

FileSystem Quota (`ONTAP_FSQuotaIndication`), and Lifecycle indications are enabled on NetApp SMI-S Provider.

Steps

1. Access NetApp SMI-S Provider.
2. Set the `PEGASUS_DISABLE_INDICATIONS` environment variable to `false`.
3. Restart the CIM server:

   ```
   smis cimserver restart
   ```

Manage SLP

Overview

The SLP service broadcasts WBEM services. When the SLP service is enabled, client applications can discover the CIMOM server. You can also specify SLP configuration settings using the `slp.conf` file.

If the SLP service is not already enabled, you can start the SLP service by using the `smis slpd start` command. To stop the SLP service, use the `smis slpd stop` command.

Specify SLP configuration options

You can edit the `slp.conf` configuration file to manage the service location protocol daemon (SLPD) service.

slp.conf file management

The `slp.conf` configuration file provides additional options that enable you to manage a service location protocol daemon (SLPD) server.

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\cfg`

Privilege level

A user with a valid user name and password

Description

The `slp.conf` configuration file enables you to change the number of interfaces a host listens to for SLP requests and the number of IP addresses a host uses for multicasting.

Use a text editor to open the `slp.conf`.

Parameters

- **`interfaces`**

  Specifies the maximum number of IP addresses a host can listen to for SLP requests.

- **`multicast`**

  Specifies the maximum number of IP addresses a host might use for multicasting. Use this parameter when configuring interfaces for SLP multicast traffic on multihomed systems.

- **`BroadcastOnly`**

  Forces the use of the broadcast option, instead of using the multicast option, when sending messages over SLP.

- **securityEnabled**

  Enables security for received URLs and attribute lists.

Example

The following is an abbreviated example of the `slp.conf` configuration file:

```
#####################################################################
# OpenSLP configuration file
# Format and contents conform to specification in IETF RFC 2614 so
the comments use the language of the RFC. In OpenSLP, SLPD
operates as an SA and a DA. The SLP UA functionality is
encapsulated by SLPLIB.
#####################################################################

#--------------------------------------------------------------------
# Static Scope and DA Configuration
#--------------------------------------------------------------------
# This option is a comma delimited list of strings indicating the
only scopes a UA or SA is allowed when making requests or
registering or the scopes a DA must support. (default value is
"DEFAULT");net.slp.useScopes = myScope1, myScope2, myScope3

# Allows administrator to force UA and SA agents to use specific
DAs. If this setting is not used dynamic DA discovery will be used
to determine which DAs to use. (Default is to use dynamic DA
discovery)
```

CIMOM commands

cimconfig

You can use the `cimconfig` command to configure CIMOM settings, such as enabling and disabling HTTP and HTTPS and changing the HTTP and HTTPS port numbers. After entering the `cimconfig` command or creating an environment variable for the NetApp SMI-S Provider configuration value, you must restart the CIM server by using the `smis cimserver restart` command.

Syntax

`cimconfig` *options*

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

Administrator (Windows)

Options

- **-c**

  Specifies that the configuration setting applies to the current CIMOM configuration.

- **-d**

  Specifies that the configuration setting applies to the default CIMOM configuration.

- **-g**

  Gets the value of a specified configuration property.

- **-h, --help**

  Displays help for the `cimconfig` command.

- **-l**

  Lists all CIMOM configuration properties.

- **-p**

  Specifies that the configuration setting is applied when the CIM server is next started.

- **-s**

  Sets the specified configuration property value.

- **-u**

  Resets the configuration property to its default value.

- **--version**

  Displays the version of the CIM server.

Example

Change the maximum log file size to 15000 KB:

```
cimconfig -s maxLogFileSizeKBytes=15000
Current value for the property maxLogFileSizeKBytes is set to "15000" in
CIMServer.
smis cimserver restart
```

CIM user commands

cimuser

You can use the `cimuser` command to add, remove, delete, modify, and list CIM server users, as well as manage their passwords.

Syntax

`cimuser` *options*

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

Administrator (Windows)

Options

- **-a**

  Adds a CIM user.

- **-h, --help**

  Displays help for the `cimuser` command.

- **-l**

  Lists CIM users.

- **-m**

  Modifies a CIM user's password. The password can be between 4 through 32 characters long.

- **-n**

  Creates a new password for the specified user. The password can be between 4 through 32 characters long.

- **-r**

  Removes a specified CIM user.

- **-u**

  Specifies a CIM user name.

- **--version**

  Displays the version of the CIM server.

- **-w**

Specifies the password for the specified user.

Example

Create a CIM user named sydney with a password of password1:

```
cimuser -a -u sydney -w password1
User added successfully.
```

SMI-S Provider commands

Overview

You can use the `smis` commands to manage storage systems and to display information about the CIM object manager.

Help is available for the `smis` command by using the `-help` option.

- **smis `-help`**

  Displays a command summary.

- **smis `-help` examples**

  Displays usage examples.

- **smis `-help` *`subcommand`***

  Displays help for the specified subcommand.

The default timeout value for the smis tool is 180 seconds.

smis add

The `smis add` command adds a storage system with an HTTP connection to your configuration to enable you to manage and monitor the device. Unless is it necessary, you should use `smis addsecure` instead of `smis add`.

Syntax

```
smis add

storage_sys storage_sys_user
[-t {http | https}]
```

Operating systems using languages other than U.S. English cannot use the `add` command.

Location

```
C:\Program Files (x86)\NetApp\smis\pegasus\bin
```

Privilege level

Administrator (Windows)

Parameters

- ***`storage_sys`***

  Name or IP address of the storage system that you are adding

If you are specifying the IP address, you can use IPv4 or IPv6. Both compressed and full IPv6 addressees are supported, for example **1001:0002:0000:0000:0000:0000:0003:0004** or **1001:2::3:4**.

- ***storage_sys_user***

  User name of the administrator who manages the storage system that you are adding

- ***storage_sys_pwd***

  Optional: password of the administrator who manages the storage system that you are adding

  As a best practice, do not use this parameter for security reasons. This parameter is provided only for automation and backward compatibility.

- **[-t {http | https}]**

  Protocol to be used: HTTPS (default) or HTTP

Storage system-agent and agent-client protocol

The `smis add` and `smis addsecure` commands determine the protocol used between the storage system and the provider. The `[-t {`**`http | https`**`}]` parameter determines the protocol used between the provider and the client.

The `smis addsecure` command and the `[-t {`**`https`**`}]` parameter connects using SSL encryption, and unencrypted traffic is not allowed. The `smis add` command and the `[-t {`**`http`**`}]` parameter connects without using SSL encryption, and unencrypted traffic is allowed.

You should consider your environment's security needs before disabling SSL-encrypted connections.

Example

Add a storage system using IPv4 with an IP address of 10.32.1.4 over HTTP:

```
smis add 10.32.1.4 user2
```

A confirmation message appears that the storage system was successfully added. If an error occurred, an error message appears.

Example

Add a storage system using IPv6 over HTTP:

```
smis add 1001:0002:0000:0000:0000:0000:0003:0004 user2
smis add 1001:2::3:4 user2
```

A confirmation message appears that the storage system was successfully added. If an error occurred, an error message appears.

Example

Add a storage system with an IP address of 10.32.1.4 over HTTP on a non-English-language system:

```
cimcli -n root/ontap ci ontap_filerdata hostname="10.32.1.4"
username="vsadmin" password="PasSw0Rd" port=80 comMechanism="HTTP"
--timeout 180
```

smis addsecure

The `smis addsecure` command adds a storage system with an HTTPS connection to your configuration to enable you to manage and monitor the device. Unless is it necessary, you should use `smis addsecure` instead of `smis add`.

Syntax

```
smis addsecure

storage_sys storage_sys_user
[-t {http | https}]
```

> Operating systems using languages other than U.S. English cannot use the `addsecure` command.

Location

```
C:\Program Files (x86)\NetApp\smis\pegasus\bin
```

Privilege level

Administrator (Windows)

Parameters

- ***storage_sys***

  Name or IP address of the storage system that you are adding

  If you are specifying the IP address, you can use IPv4 or IPv6. Both compressed and full IPv6 addressees are supported, for example `1001:0002:0000:0000:0000:0000:0003:0004` or `1001:2::3:4`.

- ***storage_sys_user***

  User name of the administrator who manages the storage system that you are adding

- ***storage_sys_pwd***

  Optional: password of the administrator who manages the storage system that you are adding

  As a best practice, do not use this parameter for security reasons. This parameter is provided only for automation and backward compatibility.

- **[-t {http | https}]**

  Protocol to be used: HTTPS (default) or HTTP

Storage system-agent and agent-client protocol

The `smis add` and `smis addsecure` commands determine the protocol used between the storage system and the provider. The `[-t {http | https}]` parameter determines the protocol used between the provider and the client.

The `smis addsecure` command and the `[-t {https}]` parameter connects using SSL encryption, and unencrypted traffic is not allowed. The `smis add` command and the `[-t {http}]` parameter connects without using SSL encryption, and unencrypted traffic is allowed.

You should consider your environment's security needs before disabling SSL-encrypted connections.

Example

Add a storage system using IPv4 with an IP address of 10.32.1.4 over HTTPS:

```
smis addsecure 10.32.1.4 user2 password2
```

A confirmation message appears that the storage system was successfully added. If an error occurred, an error message appears.

Example

Add a storage system using IPv6 over HTTPS:

```
smis addsecure 1001:0002:0000:0000:0000:0000:0003:0004 user2 password2
smis addsecure 1001:2::3:4 user2 password2
```

A confirmation message appears that the storage system was successfully added. If an error occurred, an error message appears.

Example

Add a storage system with an IP address of 10.32.1.4 over HTTPS on a non-English-language system:

```
cimcli -n root/ontap ci ontap_filerdata hostname="10.32.1.4"
username="vsadmin" password="PasSw0Rd" port=443 comMechanism="HTTPS"
--timeout 180
```

smis cimom

The `smis cimom` command describes the CIM object manager.

Syntax

smis cimom `[-t {http | https}]`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

- **`[-t {http | https}]`**

  Protocol to be used: HTTPS (default) or HTTP

Example

The `smis cimom` command and its output:

```
smis cimom
PG_ObjectManager.CreationClassName="PG_ObjectManager",
Name="PG:1297121114307-10-229-89-243",
SystemCreationClassName="PG_ComputerSystem",SystemName="10.1.2.3"
```

smis cimserver

The `smis cimserver` command starts, stops, restarts, or gets the status of the CIM server.

Syntax

`smis cimserver`

`{`**`start`** | **`stop`** | **`restart`** | **`status`**`}`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

Administrator (Windows)

Parameters

- **start**

  Start the CIM server.

- **stop**

  Stop the CIM server.

- **restart**

  Restart the CIM server.

- **status**

  Get the status of the CIM server.

smis class

The `smis class` command lists information about a specified class or all classes.

Syntax

`smis class`

name_space {**niall** | {**ei** | **ni** | **gi** | **gc**} *class_name*}} [-t {**http** | **https**}]

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

- ***name_space***

  Name space supported by the CIMOM

- **niall**

  Enumerate all instance names

- **ei**

  Enumerate instances for a class

- **ni**

  Enumerate instance names for a class

- **gi**

  Get instances for a class

- **gc**

  Get class for a class name

- ***class_name***

  Name of the class for which you want information

- **[-t {http | https}]**

  Protocol to be used: HTTPS (default) or HTTP

Example

The `smis class` command and its abbreviated output:

```
smis class root/ontap gi CIM_StorageVolume
1:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID="P3Lf
GJdC-
mN5",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:01350
27815"
2:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID="P3Lf
GJcmzpHt",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:
0135027815"
3:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID="P3Lf
GJc30t26",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:
0135027815"
4:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID="P3Lf
GJcSgbiT",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:
0135027815"
5:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID="P3Lf
GJcSgrA9",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:
0135027815"
```

smis config show

The `smis config show` command lists the current CIM server configuration information.

Syntax

`smis config show`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

Administrator (Windows)

Example

The `smis config show` and its output:

```
smis config show
slp:
Current value: true

tracelevel:
Current value: 4

traceComponents:
Current value: XmlIO,Thread, IndicationGeneration, DiscardedData,
CMPIProvider, LogMessages, ProviderManager, SSL, Authentication,
Authorization

traceFilePath:
Current value: traces/cimserver.trc

enableAuditLog:
Current value: true

logLevel:
Current value: WARNING

sslKeyFilePath:
Current value: cimom.key

sslCertificateFilePath:
Current value: cimom.cert

passwordFilePath:
Current value: cimserver.passwd

enableHttpConnection:
Current value: true

enableHttpsConnection:
Current value: true

httpPort:
Current value: 5988

httpsPort:
Current value: 5989

enableAuthentication:
Current value: true
```

smis crp

The `smis crp` command describes CIM-registered profiles supported by NetApp SMI-S Provider, including NetApp SMI-S Provider profiles.

Syntax

smis crp

`[-t {`**`http`** | **`https`**`}]`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

- **`[-t {http | https}]`**

  Protocol to be used: HTTPS (default) or HTTP

Example

The `smis crp` command and its output:

```
smis crp

PG_RegisteredProfile.InstanceID="SNIA:Profile Registration:1.4.0"
PG_RegisteredProfile.InstanceID="SNIA:SMI-S:1.4.0"
PG_RegisteredProfile.InstanceID="SNIA:SMI-S:1.5.0"
PG_RegisteredProfile.InstanceID="SNIA:SMI-S:1.6.0"
PG_RegisteredProfile.InstanceID="SNIA:Server:1.4.0"
PG_RegisteredProfile.InstanceID="SNIA:Server:1.5.0"
PG_RegisteredProfile.InstanceID="SNIA:Server:1.6.0"
PG_RegisteredProfile.InstanceID="DMTF:Profile Registration:1.4.0"
PG_RegisteredProfile.InstanceID="DMTF:Indications:1.4.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Indication:1.4.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Indication:1.5.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Indication:1.6.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Software:1.4.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Software:1.5.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Software:1.6.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Object Manager Adapter:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:iSCSI Target Ports:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:iSCSI Target Ports:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Software:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Disk Drive Lite:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Disk Drive Lite:1.5.0"
```

```
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Disk Drive Lite:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Multiple Computer
System:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Access Points:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Target Port:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Initiator Ports:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Initiator Ports:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Initiator Ports:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Masking and Mapping:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Masking and Mapping:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Extent Composition:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Extent Composition:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Extent Composition:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Server
Performance:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Server
Performance:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Physical Package:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Physical Package:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Services:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Services:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Services:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Health:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FileSystem:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Storage:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Export:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Export
Manipulation:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Export
Manipulation:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File System
Manipulation:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Filesystem
Manipulation:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Server
Manipulation:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FileSystem Quotas:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Job Control:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Job Control:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Location:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:NAS Network Port:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Replication Services:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Replication Services:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Capacity Utilization:1.4.0"
```

smis crsp

The `smis crsp` command describes CIM-registered subprofiles supported by NetApp SMI-S Provider, including NetApp SMI-S Provider subprofiles.

Syntax

smis crsp

`[-t {`**`http`** | **`https`**`}]`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

- **`[-t {http | https}]`**

  Protocol to be used: HTTPS (default) or HTTP

Example

The `smis crsp` command and its abbreviated output:

```
smis crsp

PG_RegisteredSubProfile.InstanceID="SNIA:Indication:1.4.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Indication:1.5.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Indication:1.6.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Software:1.4.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Software:1.5.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Software:1.6.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Object Manager Adapter:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:iSCSI Target Ports:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:iSCSI Target Ports:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Software:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Disk Drive Lite:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Disk Drive Lite:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Disk Drive Lite:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Multiple Computer
System:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Access Points:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Target Port:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Initiator Ports:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Initiator Ports:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Initiator Ports:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Masking and Mapping:1.6.0"
```

```
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Masking and Mapping:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Extent Composition:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Extent Composition:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Extent Composition:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Server
Performance:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Server
Performance:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Physical Package:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Physical Package:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Services:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Services:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Services:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Health:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FileSystem:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Storage:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Export:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Export
Manipulation:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Export
Manipulation:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File System
Manipulation:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Filesystem
Manipulation:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Server
Manipulation:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FileSystem Quotas:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Job Control:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Job Control:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Location:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:NAS Network Port:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Replication Services:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Replication Services:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Capacity Utilization:1.4.0"
```

smis delete

The `smis delete` command deletes a storage system.

Syntax

`smis delete`

`storage_sys`

`[-t {`**`http`** | **`https`**`}]`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

Administrator (Windows)

Parameters

- ***storage_sys***

  Name or the IP address of the storage system that you are adding

- **[-t {http | https}]**

  Protocol to be used: HTTPS (default) or HTTP

Example

Delete a storage system labeled mgt-1:

```
smis delete mgt-1
```

If no error message appears, the storage system was successfully deleted.

smis disks

The`smis disks` command displays disk information for storage systems. `smis disks` only functions when used with Data ONTAP 7-Mode controllers.

Syntax

smis disks

`[-t {`**`http`** `|` **`https`**`}]`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

- **[-t {http | https}]**

  Protocol to be used: HTTPS (default) or HTTP

Example

The `smis disks` command and its abbreviated output:

```
smis disks
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.00.3",S
ystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:0135027815"
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.00.5",S
ystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:0135027815"
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.00.7",S
ystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:0135027815"
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.00.6",S
ystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:0135027815"
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.00.1",S
ystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:0135027815"
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.00.8",S
ystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:0135027815"
```

smis exports

The `smis exports` command displays Network Attached Storage (NAS) exports for storage systems.

Syntax

smis exports `[-t {`**`http`** `|` **`https`**`}]`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

- **`[-t {http | https}]`**

  Protocol to be used: HTTPS (default) or HTTP

Example

The `smis exports` command and its output:

```
smis exports
ONTAP_LogicalFile.CreationClassName="ONTAP_LogicalFile",CSCreationClassNam
e="ONTAP_StorageSystem",CSName="ONTAP:68f6b3c0-923a-11e2-a856-
123478563412",FSCreationClassName="ONTAP_LocalFS",FSName="/vol/NAS_vol/Tes
tCFS0528",Name="/vol/NAS_vol/TestCFS0528"
ONTAP_Qtree.CreationClassName="ONTAP_Qtree",CSCreationClassName="ONTAP_Sto
rageSystem",CSName="ONTAP:68f6b3c0-923a-11e2-a856-
123478563412",FSCreationClassName="ONTAP_LocalFS",FSName="nilesh_vserver_r
ootvol",Id="nilesh_vserver_rootvol:0",Name=""
ONTAP_Qtree.CreationClassName="ONTAP_Qtree",CSCreationClassName="ONTAP_Sto
rageSystem",CSName="ONTAP:68f6b3c0-923a-11e2-a856-
123478563412",FSCreationClassName="ONTAP_LocalFS",FSName="NAS_vol",Id="NAS
_vol:0",Name=""
ONTAP_Qtree.CreationClassName="ONTAP_Qtree",CSCreationClassName="ONTAP_Sto
rageSystem",CSName="ONTAP:68f6b3c0-923a-11e2-a856-
123478563412",FSCreationClassName="ONTAP_LocalFS",FSName="NAS_vol",Id="NAS
_vol:1",Name=""
```

smis initiators

The `smis initiators` command displays Fibre Channel and iSCSI port information for storage systems.

Syntax

smis initiators

`[-t {`**`http`** | **`https`**`}]`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

- **`[-t {http | https}]`**

  Protocol to be used: HTTPS (default) or HTTP

Example

The `smis initiators` command and its abbreviated output:

```
smis initiators
ONTAP_StorageHardwareID.InstanceID="ONTAP:0084259609:iqn.1991-
05.com.microsoft:sf-tpc1"
ONTAP_StorageHardwareID.InstanceID="ONTAP:0084259609:21:00:00:e0:8b:86:f2:
89"
ONTAP_StorageHardwareID.InstanceID="ONTAP:0084259609:iqn.1991-
05.com.microsoft:went2k3x32-01"
```

smis licensed

The `smis licensed` command lists the licensed features for storage systems.

Syntax

smis licensed

`[-t {`**`http`** | **`https`**`}]`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

- **`[-t {http | https}]`**

  Protocol to be used: HTTPS (default) or HTTP

Example

The `smis licensed` command and its abbreviated output:

```
smis licensed
ONTAP_SoftwareIdentity.InstanceID="ONTAP:0084259609:cifs"
ONTAP_SoftwareIdentity.InstanceID="ONTAP:0084259609:cluster"
ONTAP_SoftwareIdentity.InstanceID="ONTAP:0084259609:fcp"
ONTAP_SoftwareIdentity.InstanceID="ONTAP:0084259609:iscsi"
ONTAP_SoftwareIdentity.InstanceID="ONTAP:0084259609:nfs"
```

smis list

The `smis list` command displays storage systems that are added.

Syntax

smis list

`[-t {**http** | **https**}]`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

- **[-t {http | https}]**

  Protocol to be used: HTTPS (default) or HTTP

Example

The `smis list` command and its output:

```
smis list
ONTAP_FilerData.hostName="10.16.180.122",port=80
```

smis luns

The `smis luns` command displays LUN information for storage systems.

Syntax

smis luns

`[-t {**http** | **https**}]`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

- **[-t {http | https}]**

  Protocol to be used: HTTPS (default) or HTTP

Example

The `smis luns` command and its abbreviated output:

```
smis luns
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID
="ef805c0d-5269-47c6-ba0fd9cdbf5e2515",
SystemCreationClassName="ONTAP_StorageSystem",SystemNa
me="ONTAP:68f6b3c0-923a-11e2-a856-123478563412"
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID
="f81cb3bf-2f16-467c-8e30-88bae415ab05",SystemCreationClassName="ONT
AP_StorageSystem",SystemName="ONTAP:68f6b3c0-923a-11e2-
a856-123478563412"
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID
="684f5fb9-0fdd-4b97-8678-188774bdcdd0",SystemCreationClassName="ONT
AP_StorageSystem",SystemName="ONTAP:68f6b3c0-923a-11e2-
a856-123478563412"
```

smis namespaces

The `smis namespaces` command lists the registered namespaces for the CIMOM.

Syntax

smis namespaces

`[-t {`**`http`** | **`https`**`}]`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

- **`[-t {http | https}]`**

  Protocol to be used: HTTPS (default) or HTTP

Example

The `smis namespaces` command and its abbreviated output:

```
smis namespaces
interop
root/ontap
```

smis pools

The `smis pools` command lists the storage pools for storage systems.

Syntax

`smis pools`

`[-t {`**`http`** | **`https`**`}]`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

- **`[-t {http | https}]`**

  Protocol to be used: HTTPS (default) or HTTP

Example

The `smis pools` command and its abbreviated output:

```
smis pools
ONTAP_ConcretePool.InstanceID="ONTAP:0084259609:d46de7f0-3925-11df-8516-
00a0980558ea"
ONTAP_ConcretePool.InstanceID="ONTAP:0084259609:51927ab0-28b5-11df-92b2-
00a0980558ea"
ONTAP_DiskPrimordialPool.InstanceID="ONTAP:0084259609:Spare"
ONTAP_DiskPrimordialPool.InstanceID="ONTAP:0084259609:Other"
ONTAP_DiskPrimordialPool.InstanceID="ONTAP:0084259609:Present"
```

smis refresh

By default, SMI-S Provider automatically gets information from storage systems every 60 minutes (3600 seconds). You can use the `smis refresh` command to manually refresh a particular storage system.

Syntax

`smis refresh` *`storage_system_ip`*

`[-t {`**`http`** | **`https`**`}]`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

- ***storage_system_ip***

  Refreshes a specific storage system.

- **[-t {http | https}]**

  Protocol to be used: HTTPS (default) or HTTP

Example

The `smis refresh` command and its output:

```
smis refresh 10.32.1.4
Return Value= 0
```

smis slpd

The `smis slpd` command starts or stops the SLP daemon.

Syntax

`smis slpd`

{**start** | **stop**}

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

Administrator (Windows)

Example

Start the SLP daemon:

```
smis slpd start
SLPD started.
```

Stop the SLP daemon:

```
smis slpd stop
SLPD (15564) was successfully stopped.
```

smis version

The `smis version` command displays the version of NetApp SMI-S Provider.

Syntax

`smis version`

`[-t {`**`http`** | **`https`**`}]`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

- **`[-t {http | https}]`**

  Protocol to be used: HTTPS (default) or HTTP

Example

The `smis version` command and its output:

```
smis version
ONTAP_SMIAgentSoftware.InstanceID="ONTAP5.2.2"
```

smis volumes

The `smis volumes` command lists the traditional and flexible volumes for storage systems.

Syntax

`smis volumes`

`[-t {`**`http`** | **`https`**`}]`

> For clustered Data ONTAP, you must use the `smis pools` command instead of the `smis volumes` command.

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

- **[-t {http | https}]**

  Protocol to be used: HTTPS (default) or HTTP

Example

The `smis volumes` command and its abbreviated output:

```
smis volumes
ONTAP_LogicalDisk.CreationClassName="ONTAP_LogicalDisk",DeviceID="d46de7f0
-3925-
11df-8516-
00a0980558ea",SystemCreationClassName="ONTAP_StorageSystem",SystemName
="ONTAP:0084259609"
ONTAP_LogicalDisk.CreationClassName="ONTAP_LogicalDisk",DeviceID="397cd140
-3a45-
11df-8516-
00a0980558ea",SystemCreationClassName="ONTAP_StorageSystem",SystemName
="ONTAP:0084259609"
ONTAP_LogicalDisk.CreationClassName="ONTAP_LogicalDisk",DeviceID="69c472c0
-4b27-
11df-8517-
00a0980558ea",SystemCreationClassName="ONTAP_StorageSystem",SystemName
="ONTAP:0084259609"
ONTAP_LogicalDisk.CreationClassName="ONTAP_LogicalDisk",DeviceID="6c7ea0b0
-3927-
11df-8516-
00a0980558ea",SystemCreationClassName="ONTAP_StorageSystem",SystemName
="ONTAP:0084259609"
```

SLP commands

slptool

You can use the `slptool` command to display information about WBEM services.

Syntax

`slptool [options] *subcommand*`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

Administrator (Windows)

Options

- **-i**

  Specifies one or more interfaces.

- **-l**

  Specifies a language tag.

- **-s**

  Specifies a list of scopes (separated by commas).

- **-u**

  Specifies one interface.

- **-v**

  Displays the version of `slptool` and OpenSLP.

slptool findattrs

The `slptool findattrs` command finds WBEM attributes that run on a network.

Syntax

`slptool findattrs *service*`

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

- ***service***

  Specifies the service type.

Example

The `slptool findattrs` command and its abbreviated output:

```
slptool findattrs service:wbem
(template-url-syntax=http://10.229.90.227:5988),(service-id=PG:10-229-90-
227),(service-hi-name=Pegasus),(service-hi-description=Pegasus CIM Server
Version 2.12.0),(template-type=wbem),(template-version=1.0),(template-
description=This template describes the attributes used for advertising
Pegasus CIM
Servers.),(InteropSchemaNamespace=interop),(FunctionalProfilesSupported=Ba
sic Read,Basic Write,Schema Manipulation,Instance Manipulation,Association
Traversal,Qualifier
Declaration,Indications),(MultipleOperationsSupported=TRUE),(Authenticatio
nMechanismsSupported=Basic),(AuthenticationMechanismDescriptions=Basic),(C
ommunicationMechanism=CIM-
XML),(ProtocolVersion=1.0),(Namespace=root/PG_Internal,interop,root/ontap,
root),(RegisteredProfilesSupported=SNIA:Server,SNIA:Array,SNIA:NAS
Head,SNIA:Software,SNIA:Profile Registration,SNIA:SCNAS,SNIA:Storage
Virtualizer,SNIA:Indication)
```

slptool findsrvs

The `slptool findsrvs` command finds WBEM services that run on a network.

Syntax

`slptool findsrvs` *service*

Location

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

- ***service***

  Specifies the service type.

Example

The `slptool findsrvs` command and its output:

```
slptool findsrvs service:wbem
service:wbem:http://10.60.167.143:5988,65535
service:wbem:http://10.60.167.246:5988,65535
service:wbem:https://10.60.167.143:5989,65535
service:wbem:https://10.60.167.246:5989,65535
service:wbem:http://10.60.167.151:5988,65535
service:wbem:http://10.60.167.250:5988,65535
service:wbem:https://10.60.167.151:5989,65535
service:wbem:https://10.60.167.250:5989,65535
service:wbem:http://10.60.167.141:5988,65535
service:wbem:https://10.60.167.141:5989,65535
service:wbem:http://10.60.167.147:5988,65535
service:wbem:https://10.60.167.147:5989,65535
service:wbem:http://10.60.167.139:5988,65535
service:wbem:http://[fe80::7804:75ad:ab59:28c]:5988,65535
service:wbem:http://[fe80::3cb1:12da:f5c3:5874]:5988,65535
service:wbem:http://[2001::4137:9e76:3cb1:12da:f5c3:5874]:5988,65535
service:wbem:https://10.60.167.139:5989,65535
service:wbem:https://[fe80::7804:75ad:ab59:28c]:5989,65535
service:wbem:https://[fe80::3cb1:12da:f5c3:5874]:5989,65535
service:wbem:https://[2001::4137:9e76:3cb1:12da:f5c3:5874]:5989,65535
```

Troubleshoot SMI-S Provider

Overview

If you encounter a problem with NetApp SMI-S Provider, you should use any error messages that you receive to help with troubleshooting.

Access is denied error

- **Message**

  `Access is denied.`

- **Description**

  This message occurs in two possible situations:

  - If you are not logged in as Administrator when accessing SMI-S Provider from the Start menu shortcut
  - If the SMI-S Provider directory is not pointing to `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

- **Corrective action**

  Complete the action that corresponds to the situation:

  - Log in with Administrator-level privileges and reopen SMI-S Provider from the Start menu, or right-click and select **Run as administrator**.
  - Log in with Administrator-level privileges and manually change the directory to `C:\Program Files (x86)\NetApp\smis\pegasus\bin`.

Possible errors while loading shared libraries

- **Messages**

  `Error while loading shared libraries: libssl.so 1.0.0: cannot open shared object file: No such file or directory.`

  The `smis cimserver` status shows the cimserver is running properly, but all other `/usr/netapp/smis/pegasus/bin/cim` commands show various failure messages.

  For example, you might receive the message `cimserver not running` when executing the `cimserver`, or you might receive the message `/usr/netapp/smis/pegasus/bin/ cimcli: symbol lookup error: /usr/netapp/smis/pegasus/bin/cimcli: undefined symbol: _ZN7Pegasus16StringConversion21decimalStringToUint64EPKcRy` when executing cimcli. These examples are not all-inclusive.

- **Description**

  This message (and similar messages) occur when the `LD_LIBRARY_PATH` environment is not set to the installation directory.

- **Corrective action**

  Enter one of the following commands to set the `LD_LIBRARY_PATH` environment variable to the installation directory:

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/netapp/smis/pegasus/lib

setenv LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/netapp/smis/pegasus/lib
```

Connection refused

- **Message**

  `Connection refused`

- **Cause**

  The CIM server has not been started.

- **Corrective action**

  Navigate to the `bin` directory in the directory in which you installed NetApp SMI-S Provider, and enter the following command to verify that the CIM server is started:

  `smis cimserver status`

  If the CIM server is not running, enter the following command:

  `smis cimserver start`

Filer return: No ontap element in response

- **Message**

  `Filer return: No ontap element in response.`

- **Description**

  This message occurs when the ONTAPI API times out. The default ONTAPI API timeout is 60 seconds, which might be too short in some scenarios.

- **Corrective action**

  Change the ONTAPI API timeout to a value greater than 60 seconds by setting the environment variable `ONTAPI_TIMEOUT_SEC`, and then restart SMI-S Provider.

Clone/Snapshot operations are not allowed

- **Message**

  `Clone/Snapshot operations are not allowed while LUN clone split operations are`

`going on in the volume. Please wait for some time and try again.`

- **Description**

  This error occurs if you attempt to execute Snapshot operations during a LUN clone split. You cannot perform Snapshot operations in a volume where a LUN is being split, if that LUN clone split is running in the background.

- **Corrective action**

  Try your Snapshot operations after the LUN is split.

Warning 26130

Message

`Warning (26130) Storage pool has been allocated to host group where none of hosts in host group has access to storage array.`

Description

This error occurs when you allocate storage capacity and grant an array access to hosts that are in a host group. With this warning, it is impossible to put virtual machines on the storage systems.

Corrective action

1. On each host machine, add the IP address of each storage system to the iSCSI Initiator application.
2. If required, on each storage system, for each host machine, create one unique igroup linked with the proper iSCSI node name from the corresponding host machine.
3. For each host machine connected to Data ONTAP, open the MPIO application and add the following hardware ID:
   - For clustered Data ONTAP, enter **`NETAPP LUN C-Mode`**.
4. Reboot the host machines.
5. Remove the provider.
6. Set the storage pool again.

HostAgentAccessDenied (ID: 26263)

Message

`Registration of storage provider` *`smis_provider_machine`* `for user` *`name`* `failed from` *`SCVMM_ (machine)`* `with error code HostAgentAccessDenied. Specify valid provider, port and user credentials for storage discovery. ID: 26263`

Description

This message occurs when a user is specified in SCVMM to connect to SMI-S Provider but is not part of the SMIS trust store.

To enable communication between SCVMM and SMI-S Provider, a valid CIM user (Local Administrator user or Domain user of the Local Administrators group) must be added to the SMIS trust store using the `cimuser` command.

Corrective action

Add the Local Administrator user (on the SMI-S Provider machine) to the CIM server database using the `cimuser` command: `cimuser -a -u admin user -w password`. You must then use that administrative user when adding NetApp SMI-S Provider to SCVMM.

If the domain controller takes too long to authenticate the Domain user, you must use the Local Administrator user on the SMI-S Provider machine.

If the error persists, you can disable authentication in SMI-S Provider.

Cannot connect to localhost:5988

- **Message**

  `Cannot connect to localhost:5988. Connection failed. Trying to connect to localhost:5988`

- **Description**

  This message occurs when HTTPS connections are disabled or the HTTPS port is not set to 5988, or if the provider has stopped working and remains in a hanging state.

- **Corrective action**

  Verify that the values of `enableHttpsConnection` and `httpsPort` are correct:

  ```
  cimconfig -g enableHttpConnection

  cimconfig -g enableHttpsConnection

  cimconfig -g httpPort

  cimconfig -g httpsPort
  ```

  If `enableHttpConnection` or `enableHttpsConnection` is not set to `true`, enter the following commands:

  ```
  cimconfig -s enableHttpConnection -p

  smis cimserver restart
  ```

  If `httpPort` is not set to 5988, enter the following commands:

  ```
  cimconfig -s httpPort=5988 -p

  smis cimserver restart
  ```

  If the provider has stopped working and remains in a hanging state, open Task Manager and end the

process, and then restart the provider.

Cannot connect to localhost:5989

- **Message**

  `Cannot connect to localhost:5989. Connection failed. Trying to connect to localhost:5989`

- **Description**

  This message occurs when HTTPS connections are disabled or the HTTPS port is not set to 5989, or if the provider has stopped working and remains in a hanging state.

- **Corrective action**

  Verify that the values of `enableHttpsConnection` and `httpsPort` are correct:

  ```
  cimconfig -g enableHttpsConnection

  cimconfig -g httpsPort
  ```

  If `enableHttpsConnection` is not set to “true”, enter the following commands:

  ```
  cimconfig -s enableHttpsConnection -p

  smis cimserver restart
  ```

  If `httpsPort` is not set to 5989, enter the following commands:

  ```
  cimconfig -s httpsPort=5989 -p

  smis cimserver restart
  ```

  If the provider has stopped working and remains in a hanging state, open Task Manager and end the process, and then restart the provider.

SMI-S Provider crashes in Windows

- **Issue**

  SMI-S Provider crashes in Windows.

- **Cause**

  This issue occurs for a variety of reasons, documented in files generated at the time of the crash.

- **Corrective action**

  Restart the provider and send the following information to technical support for further analysis:

  - Dump file from the `C:\Program Files (x86)\NetApp\smis\pegasus\pegasus\logs` directory

- Log files from the `C:\Program Files (x86)\NetApp\smis\pegasus\pegasus\logs` directory
- Trace files from the `C:\Program Files (x86)\NetApp\smis\pegasus\pegasus\traces` directory

  Messages similar to the following also appear in the trace file:

  ```
  23-May-2013 20:46:36.874 INFO cimserver: createMiniDump: SMI-S Agent has
  crashed, attempting to generate a dump file

  23-May-2013 20:46:37.14 INFO cimserver: createMiniDump: Process dumped to
  C:\Program Files (x86)\netapp\smis\pegasus\logs\SMI-S Agent-8be55da-
  2011_05_23-20_46_36.dmp
  ```

- The files `version.txt` and `cimserver_current.conf` from the `C:\Program Files (x86)\NetApp\smis\pegasus\pegasus` directory

Issue entering passwords containing special characters

- **Issue**

  In English-language operating systems, using a password that contains special characters with the `smis` command does not work in a Windows environment. This issue has not been tested with non-English operating systems.

- **Cause**

  In Windows, the following characters, plus any spaces, are considered special characters and cause password input to fail if the password is not enclosed in quotation marks:

  , & ' < > ; | = ^ "

- **Corrective action**

  If a password contains spaces or special characters, enclose it in double quotes (" ") when you use it in the `smis` command. Note that the quote character (") is a special character and should never be used in your password.

Issuing passwords with special characters

```
smis add 1.2.3.4 Administrator "pass word"

smis add 1.2.3.4 Administrator "pass&word"
```

Clone technology used in SMI-S Provider

You must have a FlexClone license for SMI-S Provider to create LUN clones.

SMI-S Provider creates LUN clones on that storage system using only FlexClone technology. If you do not have a FlexClone license, SMI-S Provider does not generate clones using LUN clone technology, and it generates the following error message:

`FlexClone license is not enabled on the storage system.`

If you have LUN clones that were created using LUN clone technology, and the Data ONTAP version is then upgraded to 7.3.1 or later, you cannot use SMI-S Provider to split those clones. They must be managed by the storage system administrator.

Confirm visibility of important objects

After adding a managed storage system, you should confirm that you can see all the important logical and physical objects in NetApp SMI-S Provider.

You can use the `smis` command to see the objects that are in the NetApp SMI-S Provider CIMOM repository. For example, use `smis list` to display added storage systems, and use `smis luns` to display LUN information.

Requirement for using fileshares on Windows

When using fileshares (CIFS shares) on Windows, the volume on which the fileshare is created must be an NTFS-only volume.

If you want to create a fileshare and use it on Windows, the volume where the fileshare is created must be an NTFS-only volume. This is to avoid problems with the credentials that access the fileshare.

From System Center 2016 Virtual Machine Manager (SCVMM), you can create virtual machines (VMs) only on fileshares that were created on NTFS-only volumes. Mixed and UNIX-style volumes are not supported.

Creating a volume to be used for CIFS shares and SCVMM

When creating a volume to be used for CIFS shares and System Center Virtual Machine Manager (SCVMM), the volume has to be of NTFS type. To create the volume with NTFS, enter the following: *`vol create -vserver <vserver_name> -volume <volume_name> -aggregate <aggr_name> -size<volume_size> -security-style ntfs`*

Nondefault firewalls must have ports manually added as exceptions

- **Issue**

  If you are using a firewall other than the default Windows firewall, you might experience the following issues:

  - SMI-S Provider is unable to communicate with a removed SMI-S client.
  - The SMI-S client is unable to receive indications from SMI-S Provider.

- **Cause**

  This issue occurs when you use a firewall other than the default Windows firewall without first manually adding the necessary ports as exceptions.

- **Corrective action**

Add ports 427, 5988, and 5989 as exceptions to your firewall.

Cannot add a storage system using a nondefault HTTP or HTTPS port

- **Issue**

  You cannot add a storage system running HTTP or HTTPS on a nondefault port.

- **Cause**

  By default, NetApp SMI-S Provider uses port 80 for communicating with storage systems over HTTP and port 443 for communicating over HTTPS.

- **Corrective action**

  Use the following command to add a storage system that uses a port other than 80 for HTTP traffic or port 443 for HTTPS traffic:

  `cimcli ci -n root/ontap ONTAP_FilerData hostName=`*`storage_sys_ip_address`*
  `port=`*`non_default_port`* `userName=`*`storage_sys_user`* `password=`*`storage_sys_pwd`*
  `comMechanism=HTTP -u` *`agent_user`* `-p` *`agent_pwd`*`-llocalhost:5989 -s`

  `-u`, `-p`, `-l`, and `-s` are optional parameters.

Adding a storage system that uses port 8000 for HTTP traffic

```
cimcli ci -n root/ontap ONTAP_FilerData hostName=10.60.167.12 port=8000
userName=root password=netapp1! comMechanism=HTTP -u root -p netapp1! -l
localhost:5989 -s --timeout 180
```

No response from the server

- **Issue**

  The server does not respond when queried.

- **Cause**

  This issue occurs when there is no storage system added to the CIMOM repository.

- **Corrective action**

  Enter the following command to verify that a storage system is added:

  `smis list`

  If there is no storage system listed, add a storage system by entering the following command:

  `smis add` *`storage_sys storage_sys_user storage_sys_pwd`*

Runtime library issues

- **Issue**

  You encounter runtime library issues.

- **Corrective action**

  Install the Microsoft Visual C++ 2010 Redistributable Package (x86) from www.microsoft.com.

NetApp SMI-S Provider takes a long time to start

- **Description**

  On Windows systems, with storage systems that are already under management, when you start NetApp SMI-S Provider using the `smis cimserver` command, the command does not return until the provider local cache is populated. It waits a maximum of 15 minutes while the cache is populated, and you cannot use NetApp SMI-S Provider until it returns.

  Using the `smis cimserver` command is the recommended method of starting NetApp SMI-S Provider.

Total managed space for a storage pool (volume) discrepancy

- **Issue**

  If you are using another storage management tool, such as FilerView, you might notice a different size reported for the total managed space for a storage pool (volume) than the size returned by SMI-S Provider.

- **Cause**

  This discrepancy occurs because the size returned by SMI-S Provider includes the WAFL and Snapshot reserve, while FilerView and other tools show only the usable space, excluding WAFL and Snapshot reserve.

- **Corrective action**

  This is an expected behavior; no corrective action.

Network path not found

- **Message**

  ```
  Network path not found
  ```

- **Description**

  This message reflects a DNS issue and occurs during VM deployment on an SMB share when the host does not have a record on the DNS server.

  Typically, the domain DNS server should automatically update the host record within 24 to 48 hours when a

new host is configured in the domain. However, this update does not always automatically happen.

- **Corrective action**
  - If you are a domain administrator, manually update the DNS host record.
  - If you are not a domain administrator, update the host file (`C:\Windows\System32\drivers\etc\hosts`).

    The host file does not have a file extension (`.txt`).

Insufficient system resources exist to complete the requested service

- **Message**

  `Insufficient system resources exist to complete the requested service`

- **Description**

  This message occurs when the maximum limit on user sessions from the same user per connection has been reached when provisioning a large number of VMs on a single file share in SCVMM.

  SCVMM creates one TCP connection per Hyper-V host, and each connection creates many sessions with two users: the computer name (COMPUTER$) of the Hyper-V host and the SCVMM “Run As account”. The number of sessions with COMPUTER$ is exactly one more than number of virtual hard disks deployed in that Hyper-V host.

  The default value of `Max Same User Session Per Connection` is 50. This limit blocks a large-scale VM deployment with SCVMM. If you deploy more than 50 VMs per Hyper-V host, then you encounter this issue.

- **Corrective action**

  Increase the counter that controls the maximum number of sessions on the same connection for CIFS protocol. For example, the following command changes the maximum user sessions on the same connection from the default 50 to 100:

  `SVM::*> cifs op modify -max-same-user-sessions-per-connection 100`

SMB share size dropping to 0 in SCVMM

- **Issue**

  New or existing SMB 3.0 share size can drop to 0 in System Center Virtual Machine Manager (SCVMM).

- **Cause**

  This issue occurs when quota reinitialization takes a long time in Data ONTAP due to heavy I/O, new or existing SMB 3.0 share size can drop to 0 in SCVMM. Because of this, new VMs cannot be provisioned on the new or existing SMB 3.0 shares.

- **Corrective action**

a. Turn off the quotas.
b. Add one default quota rule of type “tree” on each volume hosting SMB shares.
c. Turn on the quotas for those volumes to which you added a default quota rule and restart SMI-S Provider.

SCVMM rescan operation failed to locate or communicate with SMI-S Provider

- **Issue**

  In rare instances, SCVMM is not able to locate SMI-S Provider.

- **Cause**

  This issue can occur if the security infrastructure is updated with new GPOs. When they take effect after the reboot of SMI-S Provider host, SCVMM host might not trust the SMI-S Provider or the host.

- **Corrective action**
  a. Uninstall SMI-S Provider and install it again.
  b. Run the rescan operation in SCVMM for the SMI-S Provider.

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

http://www.netapp.com/us/legal/copyright.aspx

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/us/media/patents-page.pdf

Privacy policy

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Notice

Notice files provide information about third-party copyright and licenses used in NetApp software.

Notice for NetApp SMI-S Provider

Copyright information

Trademark information