IBM System Storage N series

Data ONTAP SMI-S Agent 5.0 Installation and Configuration Guide

GC52-1283-05

Contents

Preface

Supported features

IBM System Storage N series storage systems are driven by NetApp Data ONTAP software. Some features described in the product software documentation are neither offered nor supported by IBM. Please contact your local IBM representative or reseller for further details.

Information about supported features can also be found on the N series support website (accessed and navigated as described in *Websites* on page 8).

Websites

IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. The following web pages provide N series information:

- A listing of currently available N series products and features can be found at the following web page:
  www.ibm.com/storage/nas/
- The IBM System Storage N series support website requires users to register in order to obtain access to N series support content on the web. To understand how the N series support web content is organized and navigated, and to access the N series support website, refer to the following publicly accessible web page:
  www.ibm.com/storage/support/nseries/
  This web page also provides links to AutoSupport information as well as other important N series product resources.
- IBM System Storage N series products attach to a variety of servers and operating systems. To determine the latest supported attachments, go to the IBM N series interoperability matrix at the following web page:
  www.ibm.com/systems/storage/network/interophome.html
- For the latest N series hardware product documentation, including planning, installation and setup, and hardware monitoring, service and diagnostics, see the IBM N series Information Center at the following web page:
  publib.boulder.ibm.com/infocenter/nasinfo/nseries/index.jsp

Getting information, help, and service

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains

information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your IBM N series product, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure they are connected.
- Check the power switches to make sure the system is turned on.
- Use the troubleshooting information in your system documentation and use the diagnostic tools that come with your system.
- Refer to the N series support website (accessed and navigated as described in *Websites* on page 8) for information on known problems and limitations.

Using the documentation

The latest versions of N series software documentation, including Data ONTAP and other software products, are available on the N series support website (accessed and navigated as described in *Websites* on page 8).

Current N series hardware product documentation is shipped with your hardware product in printed documents or as PDF files on a documentation CD. For the latest N series hardware product documentation PDFs, go to the N series support website.

Hardware documentation, including planning, installation and setup, and hardware monitoring, service, and diagnostics, is also provided in an IBM N series Information Center at the following web page:

publib.boulder.ibm.com/infocenter/nasinfo/nseries/index.jsp

Hardware service and support

You can receive hardware service through IBM Integrated Technology Services. Visit the following web page for support telephone numbers:

www.ibm.com/planetwide/

Firmware updates

IBM N series product firmware is embedded in Data ONTAP. As with all devices, ensure that you run the latest level of firmware. Any firmware updates are posted to the N series support website (accessed and navigated as described in *Websites* on page 8).

Note: If you do not see new firmware updates on the N series support website, you are running the latest level of firmware.

Verify that the latest level of firmware is installed on your machine before contacting IBM for technical support.

How to send your comments

Your feedback helps us to provide the most accurate and high-quality information. If you have comments or suggestions for improving this document, please send them by email to *starpubs@us.ibm.com*.

Be sure to include the following:

- Exact publication title
- Publication form number (for example, GC26-1234-02)
- Page, table, or illustration numbers
- A detailed description of any information that should be changed

Data ONTAP SMI-S Agent overview

Data ONTAP SMI-S Agent enables you to manage and monitor storage systems and to manage LUNs and volumes of storage systems, CIMOM configuration settings, and CIM server users.

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

Data ONTAP SMI-S Agent follows schemas standardized by two organizations:

- Distributed Management Task Force (DMTF)
  For more information, see *http://www.dmtf.org/home*.
- Storage Networking Industry Association (SNIA)
  For more information, see *http://www.snia.org/home*.

Data ONTAP SMI-S Agent 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 and changed features in SMI-S Agent 5.0

SMI-S Agent 5.0 introduces new features and enhancements, such as CTP 1.6 compliance and support for clustered Data ONTAP.

SMI-S Agent 5.0 includes the following new features and enhancements:

- Support for SMI-S 1.5 and 1.6 via Conformance Testing Program (CTP) 1.5 and 1.6 compliance
- Support for thin provisioning for clustered Data ONTAP 8.2 (monitor, manage, and provision)
- Support for clustered Data ONTAP 8.2 for iSCSI, FCP and CIFS
  - CIFS support: monitor and manipulate file systems, file shares, and file share ACLs
- Support for SMB 3.0 (continuous availability support)
- Support for both indications and storage pools in Windows 8
- Support for AutoSupport (ASUP) reporting

SMI-S Agent 5.0 contains the following changed features:

- Users are no longer required to enter cimuser and cimpassword for every command

Known issues, limitations, and feature gaps for this release

You should be aware of some known issues and limitations in this release of Data ONTAP SMI-S Agent.

Known issues

The following are known issues in this release of SMI-S Agent:

Provider might not respond if the client host is not configured to receive indications	If the client host is not configured to receive indications, the provider might become unresponsive. As a workaround, you can configure the client host to receive indications or disable indications. This issue occurs only when the indications port 5990 is blocked on the client host machine.
Some features are not exposed	In this release, SMI-S Agent does not expose root volumes, file shares in root volumes, or shares that are mounted to an entire volume.

Limitations

The following are limitations in this release of SMI-S Agent:

No support for NAS performance statistics	NAS performance statistics are not supported in this release.
Limited support for concurrent clone operations	This release of SMI-S Agent does not support more than 24 concurrent clone operations. This applies only to thick provisioning.
Alert indications in clustered Data ONTAP	Alert Indications are disabled for clustered Data ONTAP 8.2.
Filesystem profiles support	NAS-related workflows of SCVMM 2012 SP1 are only supported in clustered Data ONTAP 8.2 and SCVMM 2012 SP1.
IPv6 not supported	IPv6 is not supported, therefore even if the filer or Vserver is registered with IPv4, but has other IPv6 addresses, registering will fail.

Uses of Data ONTAP SMI-S Agent

You can use Data ONTAP SMI-S Agent to perform the following tasks:

- Add a storage system to manage and monitor devices
- Delete a storage system
- Monitor logical unit numbers (LUNs), volumes, and disks of storage systems

- Provision LUNs and volumes for storage systems
- Manage the CIM server and its users
- Manage CIMOM configuration settings
- Set log levels for system messages sent from the CIMOM server
- Manage clustered Data ONTAP for iSCSI, FCP, and CIFS

Data ONTAP SMI-S Agent components

Data ONTAP SMI-S Agent consists of three components that allow you to manage and monitor storage systems.

CIMOM	This is the foundation for Data ONTAP SMI-S Agent. 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 Agent, CIMOM loads a shared library object, invokes it to handle a request, and returns the resulting information to the host. **Note:** Windows hosts use DLL objects. Linux hosts use SO objects.
Repository	CIMOM uses a flat-file database for its repository. It stores persistent data required at the CIM level.

Data ONTAP SMI-S Agent protocols

Data ONTAP SMI-S Agent uses CIM-XML encoding over HTTPS and Service Location Protocol (SLP).

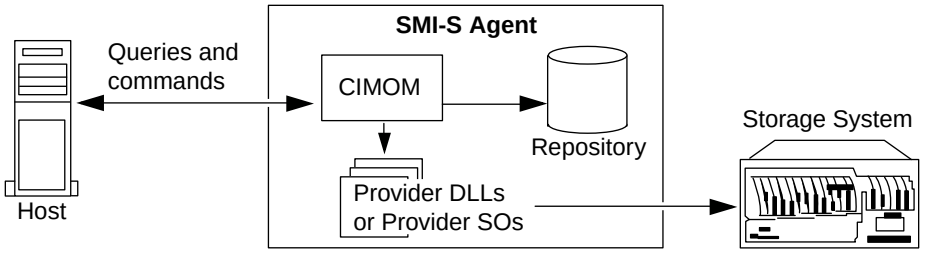
CIM-XML encoding over HTTPS	Protocol that exchanges information between a Web-Based Enterprise Management (WBEM)-enabled management client and the CIMOM server. CIM-XML encoding over HTTPS uses the CIM protocol as the payload and HTTPS as the transport. HTTP is also supported.
SLP	Discovery protocol that detects WBEM services within a LAN.

How Data ONTAP SMI-S Agent 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 Data ONTAP SMI-S Agent interacts with a WBEM management client when Data ONTAP SMI-S Agent receives a query or command.



SMI-S profiles

SMI-S Agent uses profiles and subprofiles that comply with SMI-S v1.6 via CTP 1.6.

For information about SMI-S v1.6, see Storage Management Initiative Specification (SMI-S) Releases.

Installing and uninstalling Data ONTAP SMI-S Agent

You can download and install Data ONTAP SMI-S Agent. If necessary, you can also uninstall the software.

Supported operating systems

Before installing SMI-S Agent, you must verify that the Windows and Linux hosts are running supported operating systems.

Operating system	Supported versions

Linux	• Red Hat Enterprise Linux 5 Advanced Platform for x86 (32-bit and 64-bit)
	• Red Hat Enterprise Linux v6 (32-bit and 64-bit)
	  • For 64-bit, install 32-bit libraries: gcc, libc, and libz
	• SUSE Linux Enterprise Server, version 10 (32-bit)
	• SUSE Linux Enterprise Server, version 11 with SP1 (64-bit)
	  • Install 32-bit libraries: gcc, libc, and libz

Windows	• Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012

Any operating system that is supported by your hypervisor system will function.

Note: If you need to operate on a 32-bit Windows system, install the agent normally, and it will run in 32-bit.

To run SMI-S Agent, the agent host machine must meet certain specifications:

- The agent host machine cannot be used to host a Hyper-V node.
- System Center Virtual Machine Manager (SCVMM) must not be running on the agent host machine.
- The agent host machine must not run other programs that are memory-intensive.
- The agent host machine must not run SMI-S providers from any other vendor.

Hardware requirements

You must verify that Windows and Linux hosts meet minimum hardware requirements before installing Data ONTAP SMI-S Agent.

Hardware	Requirements
Memory	You must always meet the minimum memory requirements for the host operating system. • 4 GB RAM (minimum) • 8 GB RAM (recommended)
Disk space	• 1 GB (minimum) • 4 GB (recommended)
CPU	• Dual-core 2.0 GHz (minimum) • Quad-core 2.0 GHz (recommended)

Note: Enabling logging and tracing requires additional disk space of up to 1 GB, depending on the log and trace file rotation settings.

Client software requirements

Before you install Data ONTAP SMI-S Agent, you must first install required software.

Operating system	Required client software
Linux	• Install the `uncompress` utility in the `/usr/bin` directory.
Windows	Microsoft Visual C++ 2010 runtime libraries are automatically installed during the Data ONTAP SMI-S Agent installation. To avoid potential issues related to runtime libraries, install the following software package: • Microsoft Visual C++ 2010 Redistributable Package (x86), available at *http://www.microsoft.com*.

Supported platforms

SMI-S Agent supports platforms running Data ONTAP 7.3.5+, 8.0.x, and 8.1.x (operating in 7-Mode only), and Data ONTAP 8.2.x.

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

SMI-S Agent supports the following platforms:

- N series filers
- N series gateways

Where to get SMI-S Agent

You can obtain the product software either from the physical media kit or from software updates available for download (if no media kit is requested or available). Downloads are available only to entitled IBM N series customers who have completed the registration process on the N series support website (accessed and navigated as described in *Websites* on page 8).

Software available from the N series support website

N series content, including software downloads, is available on the N series support website (accessed and navigated as described in *Websites* on page 8).

Installing SMI-S Agent on a Windows host

You can install the SMI-S Agent software so that you can manage storage systems that run Data ONTAP. If you are installing on a Windows 2008 R2 or Windows 2012 platform, the SMI-S Agent software is by default installed in the *system_drive*`:\Program Files (x86)\ontap\smis` directory.

Before you begin

You must already have the following credentials and software:

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

About this task

As a result of the installation process, the CIMOM service (named “Data ONTAP SMI-S Agent” in Service Control Manager) and SLP daemon (named “Service Location Protocol” in Service Control Manager) run as automatic services that are automatically started after a host reboot.

Upgrading to the latest version of SMI-S Agent is not supported. You must uninstall the previous version and install the new version.

Steps

1. Uninstall the installed version of SMI-S Agent.
2. If you are upgrading from SMI-S Agent 4.1 to SMI-S Agent 5.0, delete the `smis` folder located at *`installation_directory`*`\ontap\smis`.
3. Check the publication matrix page for important alerts, news, interoperability details, and other information about the product before beginning the installation.
4. Obtain the product software by inserting the physical media kit or from the version you downloaded.
5. Launch the software installation program from where you downloaded the software, and then follow the prompts.
6. Navigate to the directory that contains the SMI-S Agent software package, and double-click the package name.
7. Complete the steps in the setup wizard.

Result

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

After you finish

After upgrading to SMI-S Agent 5.0, filer credentials are cleared, and you must re-add the storage systems to the CIMOM repository.

Installing SMI-S Agent on a Linux host

You can install the SMI-S Agent software so that you can manage platforms that run Data ONTAP. By default, the SMI-S Agent software is installed in the `/usr/ontap/smis` directory.

Before you begin

You must already have the following credentials and software:

- Login credentials for the root account
- SMI-S Agent software package

Steps

1. Check the publication matrix page for important alerts, news, interoperability details, and other information about the product before beginning the installation.
2. Obtain the product software by inserting the physical media kit or from the version you downloaded.
3. Log in as root.
4. Navigate to the directory that contains the SMI-S Agent software package by entering the following command:

   cd *directory_name*
5. Do one of the following:
   - To extract the tar file into a temporary directory and delete all temporary files, including the install script, enter the following command:

     tar xvf smisagent-5.0.tar
   - To extract the tar file into a temporary directory without deleting the temporary files, enter the following command:

     tar xvf smisagent-5.0.tar -k
6. To install the software package, enter one of the following commands:
   - To install the software package and automatically delete all temporary files, including `install_smisproxy`:

     ./install_smisproxy
   - To install the software package without deleting the temporary files:

     ./install_smisproxy -k
   - To reinstall the software package and overwrite the previously installed version of the SMI-S Agent:

     ./install_smisproxy -f
   - To reinstall the software package and keep the SLP configuration files:

     ./install_smisproxy -f -s

Uninstalling SMI-S Agent from a Windows host

You must uninstall the existing version of SMI-S Agent to upgrade to the latest version.

Steps

1. Uninstall SMI-S Agent from a Windows host by using the Windows Add/Remove Programs utility.

2. If you are upgrading from SMI-S Agent 4.1 to SMI-S Agent 5.0, delete the `smis` folder located at *`installation_directory`*`\ontap\smis`.

Uninstalling SMI-S Agent from a Linux host

Uninstalling SMI-S Agent from Linux requires you to use the CLI.

Before you begin

The compress or gzip program must be installed for you to use the following `uninstall_smisproxy` script options:

- `-i` (interactive mode)
- `-s` *`path`* (silent mode with the option to save agent log files)

Steps

1. Log in as root.
2. Enter the following command:

   ***`installation_directory`*`/ontap/smis/pegasus/bin/uninstall_smisproxy`**

Preconfiguration task overview

Before using SMI-S Agent, verify that the CIM server is started, add at least one storage system to the CIMOM repository, and verify that the storage system is working correctly. Optionally, you can also enable authentication for SMI-S Agent and generate a self-signed certificate for the CIMOM.

Perform the following tasks before using SMI-S Agent:

1. Access SMI-S Agent.
2. Verify that the CIM server is started.
3. Add a storage system to the CIMOM repository.
4. Verify that the storage system is working correctly.
5. (Optional) Enable authentication for SMI-S Agent.
6. (Optional) Generate a self-signed certificate for the CIMOM.

Related tasks

Accessing SMI-S Agent on page 21
Verifying the CIM server status on page 22
Adding storage systems to the CIMOM repository on page 22
Verifying that the storage system is working correctly on page 24
Enabling authentication for SMI-S Agent on page 24
Generating a self-signed certificate for the CIM server (Linux) on page 25
Generating a self-signed certificate for the CIM server (Windows) on page 26

Accessing SMI-S Agent

For Linux platforms, you access SMI-S Agent from the shell. For Windows platforms, you can open a command prompt to access SMI-S Agent, or you can access SMI-S Agent from the Start menu.

Before you begin

You must have login credentials as root (Linux) or Administrator (Windows). If you have User Account Control (UAC) enabled on Windows, make sure you have Administrator credentials.

Steps

1. Log in as root (Linux) or Administrator (Windows).
2. Do one of the following:

Platform	Description
Linux	From a command prompt with elevated administrative privileges, navigate to *installation_directory*/ontap/smis/pegasus/bin.
Windows	From a command prompt with elevated administrative privileges, navigate to *installation_directory*\ontap\smis\pegasus\bin) or, from the Start > Programs menu, right-click Data ONTAP SMI-S Agent and select Run as Administrator.

Verifying the CIM server status

After installing SMI-S Agent, you must verify that the CIM server automatically started.

Before you begin

You must already have login credentials as root (Linux) or Administrator (Windows).

Steps

1. Log in as root or Administrator.
2. Enter the following at the command prompt:

   smis cimserver status

   If the CIM server has been started, you see the following message:

   ```
   Data ONTAP SMI-S Agent is running.
   ```

Adding storage systems to the CIMOM repository

Before you configure SMI-S Agent, you must add at least one storage system to the CIMOM repository.

Step

1. Enter one of the following at the command prompt:

To add a storage system with an...	Enter this command...
HTTP connection between the agent and the storage system	**smis add *storage_sys storage_sys_user storage_sys_pwd***
HTTPS connection between the agent and the storage system	**smis addsecure *storage_sys storage_sys_user storage_sys_pwd***

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

For clustered Data ONTAP, the IP address specified must be for a virtual storage server (Vserver), not a cluster, and the credentials must be for a vsadmin user. Data ONTAP SMI-S Agent 5.0 does not support cluster IP addresses or node management IP addresses, nor does it support not admin or node Vservers (only cluster Vservers).

Examples: Adding a storage system

To add a storage system with an IP address of 10.32.1.4 over HTTP, enter the following command:

```
smis add 10.32.1.4 root PasSw0Rd
```

To add a storage system with an IP address of 10.32.1.4 over HTTPS, enter the following command:

```
smis addsecure 10.32.1.4 root PasSw0Rd
```

Note: Operating systems using languages other than U.S. English cannot use the `add` or `addsecure` commands.

To add a storage system with an IP address of 10.32.1.4 over HTTP on a non-English-language system, enter the following command:

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

To add a storage system with an IP address of 10.32.1.4 over HTTPS on a system using languages other than U.S. English, enter the following command:

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

Note: Only for clustered Data ONTAP, replace "root" with "vsadmin".

After you finish

When operating in a cluster environment (Data ONTAP 8.2 or later), make sure that you have correctly followed the guidelines for setting up your virtual storage servers (Vservers) in the *Clustered Data ONTAP System Administration Guide for Vserver Administrators*. Data ONTAP SMI-S Agent 5.0 only supports cluster Vservers, not admin or node Vservers.

Related tasks

Deleting storage systems from the CIMOM repository on page 31
Listing storage systems in the CIMOM repository on page 31

Related references

Issue entering passwords containing special characters on page 88

Verifying that the storage system is working correctly

After adding a storage system to the CIMOM repository, you can verify whether the storage system is working correctly by using `smis` commands such as `smis list`, `smis disks`, `smis luns`, `smis pools`, and `smis volumes`.

Steps

1. Enter the following command:

   `smis luns`

2. Verify the command output:

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.

Enabling authentication for SMI-S Agent

By default, authentication is not enabled for SMI-S Agent. You can optionally enable authentication.

Before you begin

You must have login credentials as root (Linux) or Administrator (Windows). Any client, including System Center Virtual Machine Manager (SCVMM), should connect to the agent using cimuser and cimpassword.

Steps

1. Log in as root (Linux) or Administrator (Windows).
2. Navigate to the `bin` directory in the directory in which SMI-S Agent was installed.
3. At a command prompt, verify that SMI-S Agent is running by entering the following command:

   `smis cimserver status`

4. Enable authentication by entering the following command:

   cimconfig -p -s enableAuthentication=true

   CIMOM does not use Windows authentication.

5. Restart SMI-S Agent with the following commands:

   smis cimserver stop

   smis cimserver start

   On Windows systems, the following commands also work:

   net stop cimserver

   net start cimserver

6. Add a CIM server user by entering the following command:

   cimuser -a -u Administrator -w *password*

Generating a self-signed certificate for the CIM server (Linux)

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

About this task

For this certificate, Common Name does not have to match the connecting server name exactly, because that requirement might preclude using a common certificate on multiple machines and lead to difficulty diagnosing connection issues.

The administrator must be an existing local or domain user on the machine.

Steps

1. Navigate to the pegasus bin directory at installation_directory/ontap/smis/pegasus/bin.
2. At a command prompt, navigate to the OpenSSL bin directory.
3. Generate a private key by entering the following command:

   openssl genrsa -out cimom.key 2048

4. Generate a certificate request by entering the following command:

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

5. Enter your information for the certificate request when prompted.

6. Generate the self-signed certificate by using the following command:

   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.

7. Copy the `cimom.key` and `cimom.cert` files to the *`installation_directory`*`/ontap/smis/pegasus` directory.

Result

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

Generating a self-signed certificate for the CIM server (Windows)

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

Steps

1. Navigate to the pegasus bin directory at `installation_directory\ontap\smis\pegasus\bin`.
2. Generate a private key by entering the following command:

   openssl genrsa -out cimom.key 2048

3. Generate a certificate request by entering the following command:

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

4. Enter your information for the certificate request when prompted.
5. Generate the self-signed certificate by using the following command:

   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.

6. Copy the `cimom.key` and `cimom.cert` files to the *`installation_directory`*`\ontap\smis\pegasus` directory.

Managing the CIM server

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

Stopping and starting the CIM server

You can use SMI-S Agent to stop and start the CIM server.

Before you begin

You must already have login credentials as root (Linux) or Administrator (Windows).

Steps

1. Log in to the host system as root or Administrator.
2. Enter the following commands: **`smis cimserver stop`** and **`smis cimserver start`**.

   After entering the **`smis cimserver start`** 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.

Related tasks

Restarting the CIM server on page 27
Reviewing the CIM server status on page 28

Restarting the CIM server

You can use SMI-S Agent to restart the CIM server. After entering the `cimconfig` command or creating an environment variable for an SMI-S Agent configuration value, you must restart the CIM server (using the `smis cimserver restart` command).

Before you begin

Make sure that you have login credentials as root (Linux) or Administrator (Windows).

Steps

1. Log in as root or Administrator.
2. Enter the following at the command prompt:

   `smis cimserver restart`

Related tasks

Stopping and starting the CIM server on page 27
Reviewing the CIM server status on page 28

Reviewing the CIM server status

You can use SMI-S Agent to review whether the CIM server is running.

Before you begin

Make sure that you have login credentials as root (Linux) or Administrator (Windows).

Steps

1. Log in as root or Administrator.
2. Enter the following at the command prompt:

   ```
   smis cimserver status
   ```

Related tasks

Stopping and starting the CIM server on page 27
Restarting the CIM server on page 27

Managing storage systems

You can use SMI-S Agent 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. Performing these tasks from the SMI-S Agent CLI enables you to quickly manage and verify whether storage systems are running properly.

Adding storage systems to the CIMOM repository

Before you configure SMI-S Agent, you must add at least one storage system to the CIMOM repository.

Step

1. Enter one of the following at the command prompt:

To add a storage system with an...	Enter this command...
HTTP connection between the agent and the storage system	**`smis add`** ***`storage_sys storage_sys_user storage_sys_pwd`***
HTTPS connection between the agent and the storage system	**`smis addsecure`** ***`storage_sys storage_sys_user storage_sys_pwd`***

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

For clustered Data ONTAP, the IP address specified must be for a virtual storage server (Vserver), not a cluster, and the credentials must be for a vsadmin user. Data ONTAP SMI-S Agent 5.0 does not support cluster IP addresses or node management IP addresses, nor does it support not admin or node Vservers (only cluster Vservers).

Examples: Adding a storage system

To add a storage system with an IP address of 10.32.1.4 over HTTP, enter the following command:

```
smis add 10.32.1.4 root PasSw0Rd
```

To add a storage system with an IP address of 10.32.1.4 over HTTPS, enter the following command:

```
smis addsecure 10.32.1.4 root PasSw0Rd
```

Note: Operating systems using languages other than U.S. English cannot use the `add` or `addsecure` commands.

To add a storage system with an IP address of 10.32.1.4 over HTTP on a non-English-language system, enter the following command:

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

To add a storage system with an IP address of 10.32.1.4 over HTTPS on a system using languages other than U.S. English, enter the following command:

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

Note: Only for clustered Data ONTAP, replace "root" with "vsadmin".

After you finish

When operating in a cluster environment (Data ONTAP 8.2 or later), make sure that you have correctly followed the guidelines for setting up your virtual storage servers (Vservers) in the *Clustered Data ONTAP System Administration Guide for Vserver Administrators*. Data ONTAP SMI-S Agent 5.0 only supports cluster Vservers, not admin or node Vservers.

Related tasks

Deleting storage systems from the CIMOM repository on page 31
Listing storage systems in the CIMOM repository on page 31

Related references

Issue entering passwords containing special characters on page 88

Listing NFS and CIFS exports for storage systems

You can get a list of NIFS and CIFS exports for storage systems.

Step

1. Enter the following at the command prompt:

   ```
   smis exports
   ```

Listing storage systems in the CIMOM repository

You can verify the storage systems in the CIMOM repository before adding or deleting storage systems.

Step

1. Enter the following at the command prompt:

   ```
   smis list
   ```

Example: Listing storage systems in the CIMOM repository

To list storage systems, enter the following command:

```
smis list
```

Related tasks

Adding storage systems to the CIMOM repository on page 22
Deleting storage systems from the CIMOM repository on page 31

Listing exported LUNs for storage systems

You can list exported LUNs for storage systems.

Step

1. Enter the following at the command prompt:

   ```
   smis luns
   ```

Deleting storage systems from the CIMOM repository

If you no longer need to manage a storage system, you can delete it from the CIMOM repository. Because SMI-S Agent gathers information from all storage systems in the CIMOM repository, you should delete an unused storage system from the repository to maintain optimal performance.

Step

1. Enter the following at the command prompt:

   ```
   smis delete storage_sys
   ```

Example: Deleting a storage system

To delete a storage system with an IP address of 10.32.1.4, enter the following command:

```
smis delete 10.32.1.4
```

Related tasks

Adding storage systems to the CIMOM repository on page 22
Listing storage systems in the CIMOM repository on page 31

Managing CIM server users

You can use SMI-S Agent 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.

Adding CIM server users

You can use SMI-S Agent to authorize CIM users to use the CIM server.

Before you begin

You must already have login credentials as root (Linux) or Administrator (Windows).

Steps

1. Log in as root or Administrator.
2. For Windows, create a local user account, and add the user to the Administrators group.

   For more information, see your system documentation.
3. Enter the following at the command prompt:

   `cimuser -a -u user_name -w password`

> **Example: Adding a CIM server user**
>
> To add a CIM server user named chris, enter the following command:
>
> **`cimuser -a -u chris -w PaSsWoRd`**

Related tasks

Removing CIM server users on page 35
Listing CIM server users on page 34
Managing CIM server user passwords on page 34

Listing CIM server users

If you want to check the current CIM users that are authorized to use the CIM server, you can use the `cimuser -l` command.

Before you begin

You must already have login credentials as root (Linux) or Administrator (Windows).

Steps

1. Log in as root or Administrator.
2. Enter the following at the command prompt:

   `cimuser -l`

Related tasks

Adding CIM server users on page 33
Removing CIM server users on page 35
Managing CIM server user passwords on page 34

Managing CIM server user passwords

After adding CIM users, you can modify their passwords if you need to reset the passwords.

Before you begin

You must already have login credentials as root (Linux) or Administrator (Windows).

Steps

1. Log in as root or Administrator.
2. Enter the following at the command prompt:

   `cimuser -m -u user_name -w old_password -n new_password`

Example: Modifying a CIM server user's password

To change the password for the CIM server user named chris, enter the following command:

`cimuser -m -u chris -w PaSsWoRd -n pAsSw0rD`

Related references

Issue entering passwords containing special characters on page 88

Removing CIM server users

You can use SMI-S Agent to remove CIM server users so that they are not authorized to use the CIM server.

Before you begin

You must have login credentials as root (Linux) or Administrator (Windows).

Steps

1. Log in as root or Administrator.
2. Enter the following at the command prompt:

   `cimuser -r -u` ***`user_name`***

Example: Removing a CIM server user

To remove the CIM server user named chris, enter **`cimuser -r -u chris`**.

Related tasks

Adding CIM server users on page 33
Listing CIM server users on page 34
Managing CIM server user passwords on page 34

Managing CIMOM configuration settings

You can use SMI-S Agent to manage the CIMOM configuration, such as enabling or disabling HTTP and HTTPS connections and changing HTTP and HTTPS port numbers.

Enabling HTTP connections

By default, HTTP connections are enabled. Enabling HTTP connections allows clients to connect to the CIM server without using SSL encryption. Unencrypted traffic is allowed. If your environment requires encrypted traffic to and from the CIM server, disable HTTP connections and verify that HTTPS connections for the CIM server are enabled.

Steps

1. Access SMI-S Agent.
2. Enter the following command:
   ```
   cimconfig -s enableHttpConnection=true -p
   ```
3. Restart the CIM server by entering the following command:
   ```
   smis cimserver restart
   ```

Related tasks

Disabling HTTP connections on page 36
Enabling HTTPS connections on page 37
Disabling HTTPS connections on page 37

Disabling HTTP connections

By default, HTTP connections are enabled, which allows clients to connect to the CIM server without using SSL encryption. Unencrypted traffic will be allowed. If your environment requires encrypted traffic to and from the CIM server, disable HTTP connections and verify that HTTPS connections for the CIM server are enabled.

Steps

1. Access SMI-S Agent.
2. Enter the following command:
   ```
   cimconfig -s enableHttpConnection=false -p
   ```
3. Restart the CIM server by entering the following command:

```
smis cimserver restart
```

Related tasks

Enabling HTTP connections on page 36
Enabling HTTPS connections on page 37
Disabling HTTPS connections on page 37

Enabling HTTPS connections

By default, HTTPS connections are enabled, which allows clients to connect to the CIM server using SSL encryption. If you previously disabled HTTPS connections and want to allow SSL-encrypted traffic, you can enable HTTPS connections again.

Steps

1. Access SMI-S Agent.
2. Enter the following command:

   ```
   cimconfig -s enableHttpsConnection=true -p
   ```

3. Restart the CIM server by entering the following command:

   ```
   smis cimserver restart
   ```

Related tasks

Disabling HTTPS connections on page 37
Enabling HTTP connections on page 36
Disabling HTTP connections on page 36

Disabling HTTPS connections

By default, HTTPS connections are enabled, which allows clients to connect to the CIM server using SSL encryption. You can disable HTTPS connections so that unencrypted traffic is allowed. You should consider your environment's security needs before disabling HTTPS connections.

Steps

1. Access SMI-S Agent.
2. Enter the following command:

   ```
   cimconfig -s enableHttpsConnection=false -p
   ```

3. Restart the CIM server by entering the following command:

   ```
   smis cimserver restart
   ```

Related tasks

Enabling HTTPS connections on page 37
Enabling HTTP connections on page 36
Disabling HTTP connections on page 36

Changing the HTTP port number

By default, the HTTP port number is 5988. You can change the HTTP port number.

Steps

1. Access SMI-S Agent.
2. Enter the following command:

   cimconfig -s httpPort=*new_port_number* -p
3. Restart the CIM server by entering the following command:

   smis cimserver restart

Example: Changing the HTTP port number

To change the HTTPS port number to 5555, enter the following command:

```
cimconfig -s httpPort=5555 -p
smis cimserver restart
```

Related tasks

Changing the HTTPS port number on page 38

Changing the HTTPS port number

By default, the HTTPS port number is 5989. You can change the HTTPS port number.

Steps

1. Access SMI-S Agent.
2. Enter the following command:

   cimconfig -s httpsPort=*new_port_number* -p
3. Restart the CIM server by entering the following command:

   smis cimserver restart

Example: Changing the HTTPS port number

To change the HTTPS port number to 5556, enter the following commands:

```
cimconfig -s httpsPort=5556 -p
smis cimserver restart
```

Related tasks

Changing the HTTP port number on page 38

Managing logging and tracing

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

Configuring log settings

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.

Changing the system message log directory

By default, the system message logs are located in the `logs` directory in the directory in which SMI-S Agent is installed. If you prefer to have logs saved to a directory that you specify, you can use the `cimconfig` command.

Steps

1. Access SMI-S Agent.
2. Enter the following command:

   `cimconfig -s logdir=`*`new_log_directory`*` -p`

   If the *`new_log_directory`* contains space, you must enclose it in quotation marks: *`"new log directory"`*.
3. Restart the CIM server:

   `smis cimserver restart`

Example: Changing the system message log directory

To change the directory in which logs are stored to `serverlogs`, enter the following commands:

```
cimconfig -s logdir=serverlogs -p
smis cimserver restart
```

Related tasks

Changing the system message logging level on page 41

Related references

Logging levels on page 41

Changing the system message logging level

By default, all system messages are logged. Using the `cimconfig` command, you can change the logging level so that fewer messages are logged. For example, you can specify that only severe and fatal system messages are logged.

Steps

1. Access SMI-S Agent.
2. Enter the following command:

   `cimconfig -s logLevel=`*`new_log_level`*` -p`
3. Restart the CIM server:

   `smis cimserver restart`

> **Example: Changing the system message logging level**
>
> To change the logging level to INFORMATION, enter the following commands:
>
> **`cimconfig -s logLevel=INFORMATION -p`**
>
> **`smis cimserver restart`**

Related tasks

Changing the system message log directory on page 40

Related references

Logging levels on page 41

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.

Related tasks

Changing the system message log directory on page 40
Changing the system message logging level on page 41

Managing tracing

You can configure how SMI-S Agent 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.

Steps

1. Access SMI-S Agent.
2. To specify the components to be traced, enter the following command:

   cimconfig -s traceComponents=*components* -p
3. To specify the trace facility, enter the following command:

   cimconfig -s traceFacility=*facility* -p
4. To specify the location of the trace file, enter the following command:

   cimconfig -s traceFilePath=*path_name* -p
5. To specify the trace level, enter the following command:

   cimconfig -s traceLevel=*level* -p
6. To restart the CIM server, enter the following command:

   smis cimserver restart

Related tasks

Specifying trace file size on page 44
Specifying the number of trace files saved on page 44

Related references

Trace setting values on page 43

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

Related tasks

Specifying trace settings on page 42
Specifying trace file size on page 44
Specifying the number of trace files saved on page 44

Specifying 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.

Steps

1. Do one of the following:

If you are using...	Then do this...
Linux	Set the `PEGASUS_TRACE_FILE_SIZE` environment variable to the new trace file size in bytes.
Windows	Create a system or user environment variable named `PEGASUS_TRACE_FILE_SIZE` with the new trace file size in bytes. (For information about creating environment variables, see your Windows documentation.)

2. Restart the CIM server by using the `smis cimserver restart` command.

Example: Specifying the trace file size (Linux)

To specify the trace file size on Linux, enter the following commands:

```
export PEGASUS_TRACE_FILE_SIZE=20971520
smis cimserver restart
```

Related tasks

Specifying trace settings on page 42
Specifying the number of trace files saved on page 44

Related references

Trace setting values on page 43

Specifying 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.

About this task

If tracing is enabled, tracing information is written to the cimserver.trc file. The trace files are rotated. When the cimserver.trc file reaches the maximum trace file size, its contents are moved to

the cimserver.trc.*n* file. By default, *n* is a value from zero through five. If you need more trace files saved, you increase the value of *n*.

Steps

1. Do one of the following:

If you are using...	Then do this...
Linux	Set the `PEGASUS_TRACE_FILE_NUM` environment variable to the new number of trace files saved.
Windows	Create a system or user environment variable named `PEGASUS_TRACE_FILE_NUM` with the new number of trace files saved. (For information about creating environment variables, see your Windows documentation.)

2. Restart the CIM server by using the `smis cimserver restart` command.

Example: Specifying the number of trace files saved (Linux)

To specify the number of trace files saved, enter the following commands:

```
export PEGASUS_TRACE_FILE_NUM=10
smis cimserver restart
```

Related tasks

Specifying trace settings on page 42
Specifying trace file size on page 44

Related references

Trace setting values on page 43

Enabling or disabling audit logging for SMI-S commands

All incoming SMI-S commands are recorded in audit log files. You can enable or disable the logging of these incoming commands by setting a dynamic configuration property.

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 audit log enables auditors to track activities of WBEM client operations and provider usages.

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.

Step

1. To enable or disable audit logging of SMI-S commands at runtime, reset the dynamic configuration property as follows:
   - To enable SMI-S audit logging, enter `cimconfig -s enableAuditLog=true`.
   - To disable SMI-S audit logging, enter `cimconfig -s enableAuditLog=false`.

Result

The audit log file, `cimserver_auditlog`, is stored in the `/usr/ontap/smis/pegasus/logs` directory in Linux and the `C:\Program Files (x86)\ontap\smis\pegasus\logs` directory in Windows.

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.

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

Managing SMI-S Agent advanced settings

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

Specifying the SMI-S Agent cache refresh interval

By default, SMI-S Agent gets information from storage systems every 5 minutes (300 seconds). You can set the cache refresh interval to a value from 300 through 86400 seconds (24 hours).

Steps

1. Do one of the following:

If you are using...	Then do this...
Linux	Set the `CACHE_REFRESH_SEC` environment variable to the new refresh interval value (in seconds).
Windows	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.)

2. Restart the CIM server by using the `smis cimserver restart` command.

Specifying the concrete job lifetime value

Some storage system operations, such as aggregate creation and cloning or splitting a LUN, are asynchronous. SMI-S Agent tracks the progress of these operations by creating "concrete jobs". By default, SMI-S Agent keeps concrete job information for 60 minutes (3600 seconds) after the completion of the job. You can set the concrete job lifetime to a value from 3600 through 86400 seconds (24 hours).

Step

1. Do one of the following:

If you are using...	Then do this...
Linux	Set the `JOB_LIFETIME_SEC` environment variable to the new lifetime value (in seconds).

If you are using...	Then do this...
Windows	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.)

Specifying the ONTAPI timeout value

SMI-S Agent makes ONTAP API (ONTAPI) calls to storage systems. By default, the ONTAPI timeout is 60 seconds. You can increase or decrease the timeout value.

Step

1. Do one of the following:

If you are using...	Then do this...
Linux	Set the `ONTAPI_TIMEOUT_SEC` environment variable to the new timeout value (in seconds).
Windows	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.)

Related references

Filer return: No ontap element in response on page 90

Specifying the maximum number of threads per message service queue

By default, SMI-S Agent 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 Agent machine's performance, so carefully consider whether you need to increase this value.

About this task

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

If you set the maximum number of threads to less than 20, using the command **`cimcli -n root/ontap niall`** causes the agent to become unresponsive and to return the message `Insufficient threadpool` in the trace file. If this occurs, increase the number of threads in increments of 500 and restart the agent.

Steps

1. Do one of the following:

If you are using...	Then do this...
Linux	Set the `PEGASUS_MAX_THREADS_PER_SVC_QUEUE` environment variable to the new maximum thread value.
Windows	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.)

2. Restart the CIM server by using the `smis cimserver restart` command.

Disabling indications in SMI-S Agent

When `PEGASUS_DISABLE_INDICATIONS` is set to *`true`*, then Alert, FileSystem Quota, and Lifecycle indications are disabled on SMI-S Agent. Indications support is only available for Windows.

Steps

1. Set the `PEGASUS_DISABLE_INDICATIONS` environment variable to *`true`*.
2. Restart SMI-S Agent.

   `ONTAP_AlertIndication`, `ONTAP_FSQuotaIndication`, and Lifecycle indications are disabled on SMI-S Agent.

Managing SLP

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.

Specifying SLP configuration options

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

Editing the slp.conf file

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

Location

- Linux—*`installation_directory`*`/ontap/smis/pegasus/cfg`
- Windows—*`installation_directory`*`\ontap\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:

```
bin::> vi slp.conf
#####################################################################
# 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

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.

cimconfig command options

You can use the `cimconfig` command to manage CIMOM configuration settings. After entering the `cimconfig` command or creating an environment variable for an SMI-S Agent configuration value, you must stop and then restart the CIM server (using the `smis cimserver stop` and `smis cimserver start` commands).

Syntax

```
cimconfig options
```

Location

- Linux—*installation_directory*`/ontap/smis/pegasus/bin`
- Windows—*installation_directory*`\ontap\smis\pegasus\bin`

Privilege level

Root or sudo (Linux) or 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

The following example changes the maximum log file size to 15000 KB:

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

CIM user commands

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

cimuser command options

You can use the `cimuser` options to add, remove, modify, and list CIM server users.

Syntax

```
cimuser options
```

Location

- Linux—*installation_directory*`/ontap/smis/pegasus/bin`
- Windows—*installation_directory*`\ontap\smis\pegasus\bin`

Privilege level

Root or sudo (Linux) or 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

The following example creates a CIM user named sydney with a password of password1:

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

SMI-S Agent commands

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

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

`smis -help`

Displays command summary.

`smis -help examples`

Displays usage examples.

`smis -help` *`subcommand`*

Displays help for the specified subcommand.

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` by default instead of `smis add`.

Syntax

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

Location

- Linux—*`installation_directory`*`/ontap/smis/pegasus/bin`
- Windows—*`installation_directory`*`\ontap\smis\pegasus\bin`

Privilege level

Root or sudo (Linux) or Administrator (Windows)

Parameters

`storage_sys`

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

`storage_sys_user`

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

storage_sys_pwd

Password of the administrator who manages the storage system that you are adding

[-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 agent. The [`-t {http | https}`] parameter determines the protocol used between the agent and the client.

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

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

Example

The following is an example of the `smis add` command:

```
bin::>smis add 10.32.1.4 user2 password2
```

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

Related references

Issue entering passwords containing special characters on page 88

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` by default instead of `smis add`.

Syntax

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

Location

- Linux—*installation_directory*`/ontap/smis/pegasus/bin`

- Windows—*installation_directory*\ontap\smis\pegasus\bin

Privilege level

Root or sudo (Linux) or Administrator (Windows)

Parameters

storage_sys

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

storage_sys_user

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

storage_sys_pwd

Password of the administrator who manages the storage system that you are adding

[-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 agent. The [`-t {http | https}`] parameter determines the protocol used between the agent and the client.

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

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

Example

The following is an example of the `smis addsecure` command:

```
bin::>smis addsecure 10.32.1.4 user2 password2
```

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

Related references

Issue entering passwords containing special characters on page 88

smis cimom

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

Syntax

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

Location

- Linux: *`installation_directory`*`/ontap/smis/pegasus/bin`
- Windows: *`installation_directory`*`\ontap\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 following is an example of the `smis cimom` command and its output:

```
bin::>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 status of the CIM server.

Syntax

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

Location

- Linux—*`installation_directory`*`/ontap/smis/pegasus/bin`

- Windows—*installation_directory*\ontap\smis\pegasus\bin

Privilege level

Root or sudo (Linux) or 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.

Example

The following command starts the CIM server:

```
bin::>smis cimserver start
Data ONTAP SMI-S Agent started.
```

The following command stops the CIM server:

```
bin::>smis cimserver stop
Data ONTAP SMI-S Agent stopped.
```

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

- Linux—*installation_directory*/ontap/smis/pegasus/bin
- Windows—*installation_directory*\ontap\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 following is an example of the `smis class` command and its abbreviated output:

```
bin::>smis class root/ontap gi CIM_StorageVolume
1:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID="P3LfGJ
dC-mN5",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:
0135027815"
2:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID="P3LfGJ
cmzpHt",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:
0135027815"
3:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID="P3LfGJ
c30t26",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:
0135027815"
4:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID="P3LfGJ
cSgbiT",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:
0135027815"
5:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID="P3LfGJ
```

```
cSgrA9",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

- Linux—*installation_directory*`/ontap/smis/pegasus/bin`
- Windows—*installation_directory*`\ontap\smis\pegasus\bin`

Privilege level

Root or sudo (Linux) or Administrator (Windows)

Example

The following example is an example of the `smis config show` output:

```
[root@smis-rhel5x64-07 ~]# smis config show
slp:
Current value: true

tracelevel:
Current value: 4

traceComponents:
Current value:
XmlIO,Thread,IndicationGeneration,DiscardedData,CMPIProvider,LogMess
ages,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 SMI-S Agent, including Data ONTAP profiles.

Syntax

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

Location

- Linux—*`installation_directory`*`/ontap/smis/pegasus/bin`
- Windows—*`installation_directory`*`\ontap\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 following is an example of the `smis crp` command and its output:

```
[root@smis-rhel5x64-07 ~]# smis crp
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_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"
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:Capacity Utilization:1.4.0"
ONTAP_RegisteredProfile.InstanceID="ONTAP:SCNAS:1.6.0"
ONTAP_RegisteredProfile.InstanceID="ONTAP:SCNAS:1.5.0"
ONTAP_RegisteredProfile.InstanceID="ONTAP:SCNAS:1.4.0"
ONTAP_RegisteredProfile.InstanceID="ONTAP:Array:1.6.0"
ONTAP_RegisteredProfile.InstanceID="ONTAP:Array:1.5.0"
ONTAP_RegisteredProfile.InstanceID="ONTAP:Array:1.4.0"
ONTAP_RegisteredProfile.InstanceID="ONTAP:NAS Head:1.6.0"
ONTAP_RegisteredProfile.InstanceID="ONTAP:NAS Head:1.5.0"
ONTAP_RegisteredProfile.InstanceID="ONTAP:NAS Head:1.4.0"
```

```
ONTAP_RegisteredProfile.InstanceID="ONTAP:Storage Virtualizer:1.6.0"
ONTAP_RegisteredProfile.InstanceID="ONTAP:Storage Virtualizer:1.5.0"
ONTAP_RegisteredProfile.InstanceID="ONTAP:Storage Virtualizer:1.4.0"
ONTAP_RegisteredProfile.InstanceID="ONTAP:Thin Provisioning:1.6.0"
ONTAP_RegisteredProfile.InstanceID="ONTAP:Thin Provisioning:1.5.0"
ONTAP_RegisteredProfile.InstanceID="ONTAP:Thin Provisioning:1.4.0"
```

smis crsp

The `smis crsp` command describes CIM registered subprofiles supported by Data ONTAP SMI-S Agent, including Data ONTAP subprofiles.

Syntax

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

Location

- Linux—*`installation_directory`*`/ontap/smis/pegasus/bin`
- Windows—*`installation_directory`*`\ontap\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 following is an example of the `smis crsp` command and its abbreviated output:

```
[root@smis-rhel5x64-07 ~]# 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"
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:Capacity Utilization:1.4.0"
```

smis delete

The `smis delete` command deletes a storage system.

Syntax

```
smis delete storage_sys  [-t {http | https}]
```

Location

- Linux—*installation_directory*`/ontap/smis/pegasus/bin`
- Windows—*installation_directory*`\ontap\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Note: To add a storage system with the `smis add` command, you should log in as a system administrator.

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

The following is an example of the `smis delete` command:

```
bin::>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.

Syntax

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

Location

- Linux—*installation_directory*`/ontap/smis/pegasus/bin`
- Windows—*installation_directory*`\ontap\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 following is an example of the `smis disks` command and its abbreviated output:

```
bin::>smis disks
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.
00.3",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:
0135027815"
```

```
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.
00.5",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:
0135027815"
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.
00.7",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:
0135027815"
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.
00.6",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:
0135027815"
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.
00.1",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:
0135027815"
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.
00.8",SystemCreationClassName="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

- Linux—*`installation_directory`*`/ontap/smis/pegasus/bin`
- Windows—*`installation_directory`*`\ontap\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 following example displays abbreviated output from the `smis exports` command:

```
[root@smis-rhel5x64-07 ~]# smis exports
ONTAP_LogicalFile.CreationClassName="ONTAP_LogicalFile",CSCreationClassName=
"ONTAP_StorageSystem",CSName="ONTAP:68f6b3c0-923a-11e2-
a856-123478563412",FSCreationClassName="ONTAP_LocalFS",FSName="/vol/NAS_vol/
TestCFS0528",Name="/vol/NAS_vol/TestCFS0528"
ONTAP_Qtree.CreationClassName="ONTAP_Qtree",CSCreationClassName="ONTAP_Stora
geSystem",CSName="ONTAP:68f6b3c0-923a-11e2-
```

```
a856-123478563412",FSCreationClassName="ONTAP_LocalFS",FSName="nilesh_vserve
r_rootvol",Id="nilesh_vserver_rootvol:0",Name=""
ONTAP_Qtree.CreationClassName="ONTAP_Qtree",CSCreationClassName="ONTAP_Stora
geSystem",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_Stora
geSystem",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

- Linux—*`installation_directory`*`/ontap/smis/pegasus/bin`
- Windows—*`installation_directory`*`\ontap\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 following example displays abbreviated output from the `smis initiators` command:

```
bin::>smis initiators
ONTAP_StorageHardwareID.InstanceID="ONTAP:0084259609:iqn.
1991-05.com.microsoft:s
f-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

- Linux—*`installation_directory`*`/ontap/smis/pegasus/bin`
- Windows—*`installation_directory`*`\ontap\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 following is an example of the `smis licensed` command and its abbreviated output:

```
bin::>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

- Linux—*installation_directory*/ontap/smis/pegasus/bin
- Windows—*installation_directory*\ontap\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 following is an example of the `smis list` command and its output:

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

smis luns

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

Syntax

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

Location

- Linux—*installation_directory*/ontap/smis/pegasus/bin
- Windows—*installation_directory*\ontap\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 following example displays abbreviated output from the `smis luns` command:

```
[root@smis-rhel5x64-07 ~]# smis luns
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID
="ef805c0d-5269-47c6-ba0f-
d9cdbf5e2515",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

- Linux—*installation_directory*`/ontap/smis/pegasus/bin`
- Windows—*installation_directory*`\ontap\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 following is an example of the `smis namespaces` command and its abbreviated output:

```
bin::>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

- Linux—*installation_directory*`/ontap/smis/pegasus/bin`
- Windows—*installation_directory*`\ontap\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 following is an example of the `smis pools` command and its abbreviated output:

```
bin::>smis pools
ONTAP_ConcretePool.InstanceID="ONTAP:
0084259609:d46de7f0-3925-11df-8516-00a09805
58ea"
ONTAP_ConcretePool.InstanceID="ONTAP:
0084259609:51927ab0-28b5-11df-92b2-00a09805
58ea"
ONTAP_DiskPrimordialPool.InstanceID="ONTAP:0084259609:Spare"
ONTAP_DiskPrimordialPool.InstanceID="ONTAP:0084259609:Other"
ONTAP_DiskPrimordialPool.InstanceID="ONTAP:0084259609:Present"
```

smis slpd

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

Syntax

```
smis slpd  {start | stop}]
```

Location

- Linux—*`installation_directory`*`/ontap/smis/pegasus/bin`
- Windows—*`installation_directory`*`\ontap\smis\pegasus\bin`

Privilege level

Root or sudo (Linux) or Administrator (Windows)

Note: To add a storage system with the `smis add` command, you should log in as a system administrator.

Example

The following example starts the SLP daemon:

```
bin::>smis slpd start
SLPD started.
```

The following example stops the SLP daemon:

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

smis version

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

Syntax

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

Location

- Linux—*installation_directory*/ontap/smis/pegasus/bin
- Windows—*installation_directory*\ontap\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 following example displays output from the `smis version` command:

```
bin::>smis version
ONTAP_SMIAgentSoftware.InstanceID="ONTAP5.0"
```

smis volumes

The `smis volumes` command lists the traditional and flexible volumes for storage systems. `smis volumes` only functions in Data ONTAP operating in 7-mode.

Syntax

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

Location

- Linux—*installation_directory*/ontap/smis/pegasus/bin
- Windows—*installation_directory*\ontap\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 following is an example of the `smis volumes` command and its abbreviated output:

```
bin::>/smis volumes
ONTAP_LogicalDisk.CreationClassName="ONTAP_LogicalDisk",DeviceID="d46de7f0-3
925-
11df-8516-00a0980558ea",SystemCreationClassName="ONTAP_StorageSystem",System
Name
="ONTAP:0084259609"
ONTAP_LogicalDisk.CreationClassName="ONTAP_LogicalDisk",DeviceID="397cd140-3
a45-
11df-8516-00a0980558ea",SystemCreationClassName="ONTAP_StorageSystem",System
Name
="ONTAP:0084259609"
ONTAP_LogicalDisk.CreationClassName="ONTAP_LogicalDisk",DeviceID="69c472c0-4
b27-
11df-8517-00a0980558ea",SystemCreationClassName="ONTAP_StorageSystem",System
Name
="ONTAP:0084259609"
ONTAP_LogicalDisk.CreationClassName="ONTAP_LogicalDisk",DeviceID="6c7ea0b0-3
927-
11df-8516-00a0980558ea",SystemCreationClassName="ONTAP_StorageSystem",System
Name
="ONTAP:0084259609"
```

SLP commands

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

slptool command options

You can use these options with the `slptool` command.

Syntax

```
slptool [options] subcommand
```

Location

- Linux—*installation_directory*`/ontap/smis/pegasus/bin`
- Windows—*installation_directory*`\ontap\smis\pegasus\bin`

Privilege level

Root or sudo (Linux) or 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

- Linux—*installation_directory*`/ontap/smis/pegasus/bin`
- Windows—*installation_directory*`\ontap\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

service

Specifies the service type.

Example

The following example displays abbreviated output from the `slptool findattrs` command:

```
[root@smis-rhel5x64-07 ~]# 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=Basic
Read,Basic Write,Schema Manipulation,Instance
Manipulation,Association Traversal,Qualifier
Declaration,Indications),(MultipleOperationsSupported=TRUE),
(AuthenticationMechanismsSupported=Basic),
(AuthenticationMechanismDescriptions=Basic),
(CommunicationMechanism=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

- Linux—*installation_directory*`/ontap/smis/pegasus/bin`
- Windows—*installation_directory*`\ontap\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

service

Specifies the service type.

Example

The following is an example of the `slptool findsrvs` command and its output:

```
bin::>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
```

Using System Center 2012 - Virtual Machine Manager SP1

You can use System Center 2012 - Virtual Machine Manager (SCVMM) SP1 to manage SMI-S Agent functions, including establishing an iSCSI session and allocating storage to host pools. SMI-S Agent cannot run on the same machine as SCVMM.

Related information

Technical Documentation Download for System Center 2012 – Virtual Machine Manager

Configuring an SMI-S Provider for iSCSI Target Server

Lifecycle indications tracked in SCVMM 2012 SP1

SMI-S Agent tracks certain lifecycle indications every five minutes. Lifecycle indications capture any out-of-band operations and report them to the clients. You can use these indications to monitor SMI-S Agent operations.

In SCVMM 2012 SP1, lifecycle indications for creation, modification, and deletion of objects are tracked every five minutes.

The following CIM classes are tracked:

- `CIM_DiskDrive`
- `CIM_StoragePool`
- `CIM_StorageVolume`
- `CIM_SCSIProtocolController`
- `CIM_ProtocolControllerForUnit`
- `CIM_SCSIProtocolEndpoint`
- `CIM_FCPort`
- `CIM_ComputerSystem`
- `CIM_StorageHardwareID`
- `CIM_AuthorizedSubject`

Discovering SMI-S Agent in SCVMM 2012 SP1

To interact with SMI-S Agent through System Center 2012 - Virtual Machine Manager (SCVMM) SP1, you must first discover the agent.

Before you begin

You must have SCVMM SP1 installed on the designated server per Microsoft best practices.

Steps

1. Open SCVMM 2012 SP1.
2. In the bottom left pane, select **Fabric**.
3. From the top left pane, expand the **Storage** option.
4. Under **Storage** options, click **Providers**.
5. On the top bar, click **Add Resources** then select **Storage Devices**
6. Select `Add a storage device that is managed by an SMI-S provider`.
7. From the **Protocol** drop-down menu, select **SMI-S CIMXML**.
8. Enter the IP address of the server running the SMI-S Agent.

   Port number is 5988 by default, but you may select another specific port or check `Use Secure Sockets Layer connection`.
9. On the **Run As Account** tab, click **Browse**.
10. Select one of the following:
    - Select an account that already has local administrative privileges on the SMI-S Agent server.
    - Create a new account and add those privileges.

Result

SCVMM SP1 discovers the SMI-S Agent list of controllers and the subsequent list of storage pools. For the latest information, consult your System Center user manual.

After you finish

You must define a set of service levels.

Related information

Technical Documentation Download for System Center 2012 – Virtual Machine Manager

Allocating storage to host pools using SCVMM 2012 SP1

You can use System Center 2012 - Virtual Machine Manager to allocate storage to host pools.

Before you begin

You must have System Center 2012 - Virtual Machine Manager SP1 installed on the designated server per Microsoft best practices.

Steps

1. Open System Center 2012 - Virtual Machine Manager (SCVMM) SP1.
2. In the bottom left pane, select **Fabric**.

   The Fabric pane loads in the top left.
3. From the **Fabric** pane, expand **Storage** > **Arrays**.
4. Select **Allocate Capacity**.
5. Choose the host group.
6. Click the **Allocate storage pools** option.

   The storage aggregate pools are listed.
7. Select a storage aggregate pool.
8. Click **Add** to allocate the selected storage pool.
9. Click **OK** to go back to **Allocate Storage Capacity** window.
10. Click **Allocate logical units**.

    The available logical units are listed.
11. Select an available logical unit.
12. Click **Add** to allocate the selected logical units.
13. Click **OK**.

Related information

Technical Documentation Download for System Center 2012 – Virtual Machine Manager

Establishing an iSCSI session using SCVMM 2012 SP1

You can use System Center 2012 - Virtual Machine Manager to establish an iSCSI session with a host.

Before you begin

You must have System Center 2012 - Virtual Machine Manager SP1 installed on the designated server per Microsoft best practices.

Steps

1. Open System Center 2012 - Virtual Machine Manager (SCVMM) SP1.
2. In the bottom left pane, select **VMs and Services**.

   The VMs and Services pane loads in the top left.
3. From the **VMs and Services** pane, expand **All Hosts**.
4. Right-click the selected server name.
5. Select **Properties**.
6. In the **Properties** window, select **Storage**.
7. Click the **Add iSCSI Array** option.
8. Enter the storage array details, target portal, and initiator IP.
9. Click **Create**.

Related information

Technical Documentation Download for System Center 2012 – Virtual Machine Manager:

Troubleshooting SMI-S Agent

If you encounter a problem with SMI-S Agent, use error messages to help with troubleshooting.

Possible errors while loading shared libraries

Message The server displays the following message on Linux systems:

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

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

For example, you might receive the message `Cimserver not running` when executing `cimserver`, or you might receive the message `/usr/ontap/smis/pegasus/bin/cimcli: symbol lookup error: /usr/ontap/smis/pegasus/bin/cimcli: undefined symbol: _ZN7Pegasus16StringConversion21decimalStringToUint64EPKcRy` when executing `cimcli`.

These examples are not all-inclusive, and the error messages received might vary, even for the same executable.

Description This message (and similar messages) occurs when the LD_LIBRARY_PATH environment variable 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/ontap/smis/pegasus/lib`

`setenv LD_LIBRARY_PATH $LD_LIBRARY_PATH:/usr/ontap/smis/pegasus/lib`

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 Agent unable to communicate with removed SMI-S client

- SMI-S client unable to receive indications from SMI-S Agent

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.

Access is denied error

Message When you try to access SMI-S Agent from the Start menu on Windows platforms, you receive the following message:

```
Access is denied.
```

Description This message occurs in two situations:

- If you are not logged in as Administrator when accessing SMI-S Agent from the Start menu shortcut
- If the SMI-S Agent directory is not pointing to `program files (x86)/ontap/smis/pegasus/bin`

Corrective action To resolve this issue, complete the action that corresponds to the situation:

- Log in with Administrator-level privileges and reopen SMI-S Agent from the Start menu, or right-click and select **Run as administrator**.
- Log in with Administrator-level privileges and manually change the directory to `program files x86/ontap/smis/pegasus/bin`.

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, SMI-S Agent 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 -l localhost:5989
-s
```

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

Example:

```
cimcli ci -n root/ontap ONTAP_FilerData hostName=10.60.167.12
port=8000 userName=root password=ibm1! comMechanism=HTTP -u
root -p ibm1! -l localhost:5989 -s --timeout 180
```

Cannot connect to localhost:5988

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

Description This message occurs if HTTPS connections are disabled or the HTTPS port is not set to 5988, or if the agent 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 agent has stopped working and remains in a hanging state, open Task Manager and end the process, and then restart the agent.

Cannot connect to localhost:5989

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

Description This message occurs if HTTPS connections are disabled or the HTTPS port is not set to 5989, or if the agent 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 agent has stopped working and remains in a hanging state, open Task Manager and end the process, and then restart the agent.

Connection refused error

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 SMI-S Agent, 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
```

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 international (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.

Example:

```
smis add 1.2.3.4 root "pass word"
```

Example:

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

Related tasks

Adding storage systems to the CIMOM repository on page 22
Managing CIM server user passwords on page 34

Related references

smis add on page 56
smis addsecure on page 57

Guidelines for handling SMI-S Agent crashes in Linux

Issue

If SMI-S Agent crashes, there is information you can gather to help find the cause. When SMI-S Agent crashes, it generates a core file in the `/usr/ontap/smis/pegasus/bin` directory.

Cause

The cause of your crash can be found using one of the logs below.

Corrective action

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

- Core file from the `/usr/ontap/smis/pegasus/bin` directory or the /root directory
- Log files from the `/usr/ontap/smis/pegasus/logs` directory
- Trace files from the `/usr/ontap/smis/pegasus/traces` directory
- The files `version.txt` and `cimserver_current.conf` from the `/usr/ontap/smis/pegasus` directory

Guidelines for handling SMI-S Agent crashes in Windows

Issue

If SMI-S Agent crashes, it generates a dump file in the *`installation_directory`*`\ontap\smis\pegasus\logs` 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)\ontap\smis\pegasus\logs\SMI-S
Agent-8be55da-2011_05_23-20_46_36.dmp
```

When running Windows Server 2012, the agent might not generate a dump file. If the agent does not generate a dump file, it can be found under the Windows Error Reporting tool .

Cause The cause of your crash can be found using one of the logs below.

Corrective action Restart the agent and send the following information to technical support for further analysis:

- Dump file from the *`installation_directory`*`\ontap\smis\pegasus\logs` directory
- Log files from the *`installation_directory`*`\ontap\smis\pegasus\logs` directory
- Trace files from the *`installation_directory`*`\ontap\smis\pegasus\traces` directory
- The files `version.txt` and `cimserver_current.conf` from the *`installation_directory`*`\ontap\smis\pegasus` directory

Multiprocess mode disabled in Linux

Description SMI-S Agent does not currently support multiprocess mode in Linux.

Filer return: No ontap element in response

Message `Filer return: No ontap element in response`.

Description Your system returns this error if your 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 Agent.

Related tasks

Specifying the ONTAPI timeout value on page 48

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*.

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.

SMI-S Agent takes a long time to start

Description	On both Windows and Linux systems, with storage systems that are already under management, when you start SMI-S Agent using the `smis cimserver` command,

the command does not return until the agent's local cache is populated. It waits a maximum of 15 minutes while the cache is populated, and you cannot use SMI-S Agent until it returns.

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

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 Agent.
Cause	This discrepancy occurs because the size returned by SMI-S Agent 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.

ProviderLoadFailure

Your agent might return the error `ProviderLoadFailure` due to missing library files on RHEL6x64.

Message

```
[root@smis-rhelx64-03 ~]# /usr/ontap/smis/pegasus/bin/smis list
cimcli CIMException: Cmd= ni Object= ONTAP_FilerData Code= 1
CIM_ERR_FAILED: ProviderLoadFailure:
(/usr/ontap/smis/pegasus/lib/
libONTAP_FilerData.so:ONTAP_FilerData):Cannot load library, error:
libz.so.1: cannot open shared object file: No such file or directory
```

Description

This error occurs because of missing library files on RHEL6x64.

Corrective action

1. Try setting the `LD_LIBRARY_PATH` using:

   `LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/ontap/smis/pegasus/lib`

2. Enter the following commands:

   `ldd /usr/ontap/smis/pegasus/bin/cimserver`

   `ldd /usr/ontap/smis/pegasus/bin/cimcli`

   `ldd /usr/ontap/smis/pegasus/lib/libONTAP_FilerData.so`

3. Check the logs for any binaries that are not found on the `ldd` command.
4. If they are not found, look online and download correct binaries.

Warning 26130

Warning 26130 occurs during storage capacity allocation through zoning.

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 device hardware ID:
   - For clustered Data ONTAP, enter **`NETAPP LUN C-Mode`**.
   - For Data ONTAP operating in 7-Mode, enter **`NETAPP LUN`**.
4. Reboot the host machines.
5. Remove the provider.
6. Try setting the storage pool again.

Best practices for using SMI-S Agent

To use SMI-S Agent most effectively, follow recommended best practices.

Manually enabling ALUA

Because SMI-S Agent 5.0 does not automatically enable the ALUA property on the FC and iSCSI igroups it creates, if you are using Data ONTAP MPIO DSM 3.4 or later for Windows MPIO, you must manually enable ALUA on those igroups.

The ALUA property does not need to be manually enabled for Data ONTAP MPIO DSM 3.4 or Microsoft DSM.

Data ONTAP MPIO DSM 3.4 does not support clustered Data ONTAP 8.2.x LUNs. Use Data ONTAP MPIO DSM 3.5 for clustered LUNs.

Cloning technology used in SMI-S Agent

SMI-S Agent creates LUN clones using FlexClone technology.

SMI-S Agent creates LUN clones on that storage system using only FlexClone technology. If you do not have a FlexClone license, SMI-S Agent 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 Agent to split those clones. They must be managed by the storage system administrator.

Confirming 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 SMI-S Agent.

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

Related concepts

SMI-S Agent commands on page 56

Starting and stopping SMI-S Agent

To ensure that all the configuration settings are correctly set and that the agent's cache is in good health, start and stop SMI-S Agent using the `smis cimserver` command.

Related references

smis cimserver on page 59

Starting SMI-S Agent in Windows

To access SMI-S Agent from the Start menu in Windows, you must be logged in as Administrator.

If you are not logged in as a user with administrator privileges, and you start SMI-S Agent by using "Run as" to run the Start menu shortcut as Administrator, the application cannot access the `%PEGASUS_HOME%\bin` directory.

Using SMI-S Agent across different domains

If your storage systems and SMI-S Agent are installed in different domains, authentication must be enabled before you can use SMI-S Agent.

Related tasks

Enabling authentication for SMI-S Agent on page 24

Requirement for using fileshares in Windows

When using fileshares (CIFS shares) in Windows, the volume where the fileshare will be created must be an NTFS-only volume.

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

From System Center Virtual Machine Manager (SCVMM) 2012 SP1, you can only create virtual machines (VMs) on fileshares that were created in NTFS-only volumes. Mixed and Unix style volumes are not supported.

Creating a volume to be used for CIFS shares and System Center Virtual Machine Manager (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, type the following:

```
vol create -vserver <vserver_name> -volume <volume_name> -aggregate
<aggr_name> -size<volume_size> -security-style ntfs
```

Copyright and trademark information

References in this documentation to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's or NetApp's intellectual property rights may be used instead of the IBM or NetApp product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM and NetApp, are the user's responsibility.

No part of this document covered by copyright may be reproduced in any form or by any means— graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

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

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, FAServer, FastStak, FilerView, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service

Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, SnapDirector, SnapDrive, SnapFilter, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. NetCache is certified RealSystem compatible.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, N.Y. 10504-1785
U.S.A.

For additional information, visit the web at:
http://www.ibm.com/ibm/licensing/contact/

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Index

T

U

V

W

NA 210-06075_A0, Printed in USA

GC52-1283-05