NetApp® SMI-S Provider 5.2.2

Installation and Configuration Guide

March 2016 | 215-10079_A0
doccomments@netapp.com

NetApp®

Contents

NetApp SMI-S Provider overview 6
New in this release 6
Uses of NetApp SMI-S Provider 6
NetApp SMI-S Provider sizing and performance 6
NetApp SMI-S Provider components 7
NetApp SMI-S Provider protocols 7
How NetApp SMI-S Provider interacts with a host 8
SMI-S profiles 8
Deployment workflow 9
Preparing for deployment 10
Supported operating system versions 10
Hardware requirements 11
Required licenses 11
Supported platforms 12
Downloading the NetApp SMI-S Provider software package 12
Installing NetApp SMI-S Provider 13
Installing NetApp SMI-S Provider on a Windows host 13
Installing NetApp SMI-S Provider on a Linux host 14
Upgrading NetApp SMI-S Provider 16
Prerequisites to upgrading 16
Upgrading NetApp SMI-S Provider on a Windows host 16
Upgrading NetApp SMI-S Provider on a Linux host 18
Uninstalling NetApp SMI-S Provider 20
Uninstalling NetApp SMI-S Provider from a Windows host 20
Uninstalling NetApp SMI-S Provider from a Linux host 20
Preconfiguration validation 21
Verifying the CIM server status 21
Adding a CIM server user 22
Verifying that the storage system is working correctly 22
Generating a self-signed certificate for the CIM server 23
Managing the CIM server 25
Managing storage systems 26
Managing CIM server users 28
Types of CIM users and associated operations 28
Managing CIMOM configuration settings 30
Managing logging and tracing 32
Configuring log settings 32
Logging levels 33
Managing tracing 33
Specifying trace settings 33
Specifying trace file size 35

Specifying the number of trace files saved 35
Enabling or disabling audit logging for SMI-S commands 36
Managing SMI-S Provider advanced settings 38
Specifying the SMI-S Provider automatic cache refresh interval 38
Specifying the concrete job lifetime value 38
Specifying the ONTAPI timeout value 39
Specifying the maximum number of threads per message service queue 39
Enabling or disabling authentication for NetApp SMI-S Provider 40
Enabling indications in SMI-S Provider 41
SMI-S Provider configuration settings when using ServiceNow 41
Managing SLP 43
Specifying SLP configuration options 43
slp.conf file management 43
CIMOM commands 45
cimconfig 45
CIM user commands 47
cimuser 47
SMI-S Provider commands 49
smis add 49
smis addsecure 51
smis cimom 52
smis cimserver 53
smis class 54
smis config show 55
smis crp 56
smis crsp 58
smis delete 59
smis disks 60
smis exports 60
smis initiators 61
smis licensed 62
smis list 62
smis luns 63
smis namespaces 64
smis pools 64
smis refresh 65
smis slpd 66
smis version 66
smis volumes 67
SLP commands 68
slptool 68
slptool findattrs 68
slptool findsrvs 69
Using System Center 2012 - Virtual Machine Manager 71
Remote replication overview 71

Remote replication requirements ... 72
Links to operations involved in configuring the SCVMM cloud fabric ... 72
Setting up cluster and SVM peering for disaster recovery ... 73
Troubleshooting SMI-S Provider ... 81
Possible errors while loading shared libraries ... 81
Access is denied error ... 81
Connection refused ... 82
Filer return: No ontap element in response ... 82
Clone/Snapshot operations are not allowed ... 82
ProviderLoadFailure ... 83
Warning 26130 ... 83
SnapMirror broken, a failover happened ... 84
EntityRef: expecting ';' error ... 84
HostAgentAccessDenied (ID: 26263) ... 85
Cannot connect to localhost:5988 ... 85
Cannot connect to localhost:5989 ... 86
SMI-S Provider crashes in Linux ... 86
Multiprocess mode disabled in Linux ... 87
SMI-S Provider crashes in Windows ... 87
Issue entering passwords containing special characters ... 87
Manually enabling ALUA in 7-Mode environments ... 88
Cloning technology used in SMI-S Provider ... 88
Confirming visibility of important objects ... 88
Requirement for using fileshares on Windows ... 89
Nondefault firewalls must have ports manually added as exceptions ... 89
Cannot add a storage system using a nondefault HTTP or HTTPS port ... 89
No response from the server ... 90
Runtime library issues ... 90
NetApp SMI-S Provider takes a long time to start ... 90
Total managed space for a storage pool (volume) discrepancy ... 91
During 7-Mode aggregate creation, SMI-S Provider incorrectly reports initial aggregate size ... 91
Network path not found ... 91
Insufficient system resources exist to complete the requested service ... 91
SMB share size dropping to 0 in SCVMM ... 92
SCVMM rescan operation failed to locate or communicate with SMI-S Provider ... 92
Relationship with destination <volume> already exists ... 93
Copyright information ... 94
Trademark information ... 95
How to send comments about documentation and receive update notifications ... 96
Index ... 97

NetApp SMI-S Provider overview

NetApp SMI-S Provider 5.2.2 (formerly *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.

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

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

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

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

New in this release

NetApp SMI-S Provider 5.2.2 includes new support enhancements and critical bug fixes.

- Product name change to NetApp SMI-S Provider
- Support for Data ONTAP 8.3.2
- Bug fixes

Uses of NetApp SMI-S Provider

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

You can use NetApp SMI-S Provider to perform the following tasks:

- Manage storage controllers using System Center 2012 - Virtual Machine Manager or System Center 2012 R2 - Virtual Machine Manager
- Monitor storage controllers using ServiceNow
- Monitor storage controllers using Tivoli Storage Productivity Center (TPC)
- Manage and monitor using additional SMI-S based products

NetApp SMI-S Provider sizing and performance

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

Sizing

NetApp SMI-S Provider can manage up to the following numbers of objects:

- **Data ONTAP operating in 7-Mode**

  - 30 storage systems (without indications)
  - 10 storage systems (with indications)
  - 1,500 LUNs (per FlexVol)
- **Clustered Data ONTAP**
  - 100 Storage Virtual Machines (without indications)
  - 10 Storage Virtual Machines (with indications)
  - 1,500 LUNs (per FlexVol volume)
  - 200 CIFS file shares (per FlexVol volume)

Performance notice

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

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

For the latest information about sizing and performance, check the Interoperability Matrix Tool (IMT).

Related information

NetApp Interoperability Matrix Tool

NetApp SMI-S Provider components

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

CIMOM

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

Provider objects

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

> **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.

NetApp SMI-S Provider protocols

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

CIM-XML encoding over HTTPS

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

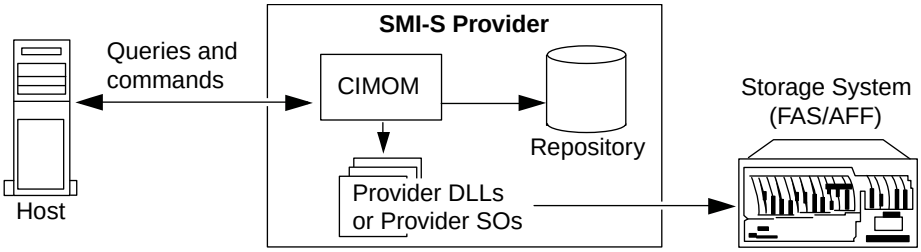
SLP

Discovery protocol that detects WBEM services within a LAN.

How NetApp SMI-S Provider interacts with a host

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

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



SMI-S profiles

SMI-S Provider uses profiles and subprofiles that comply with SMI-S v1.6.1.

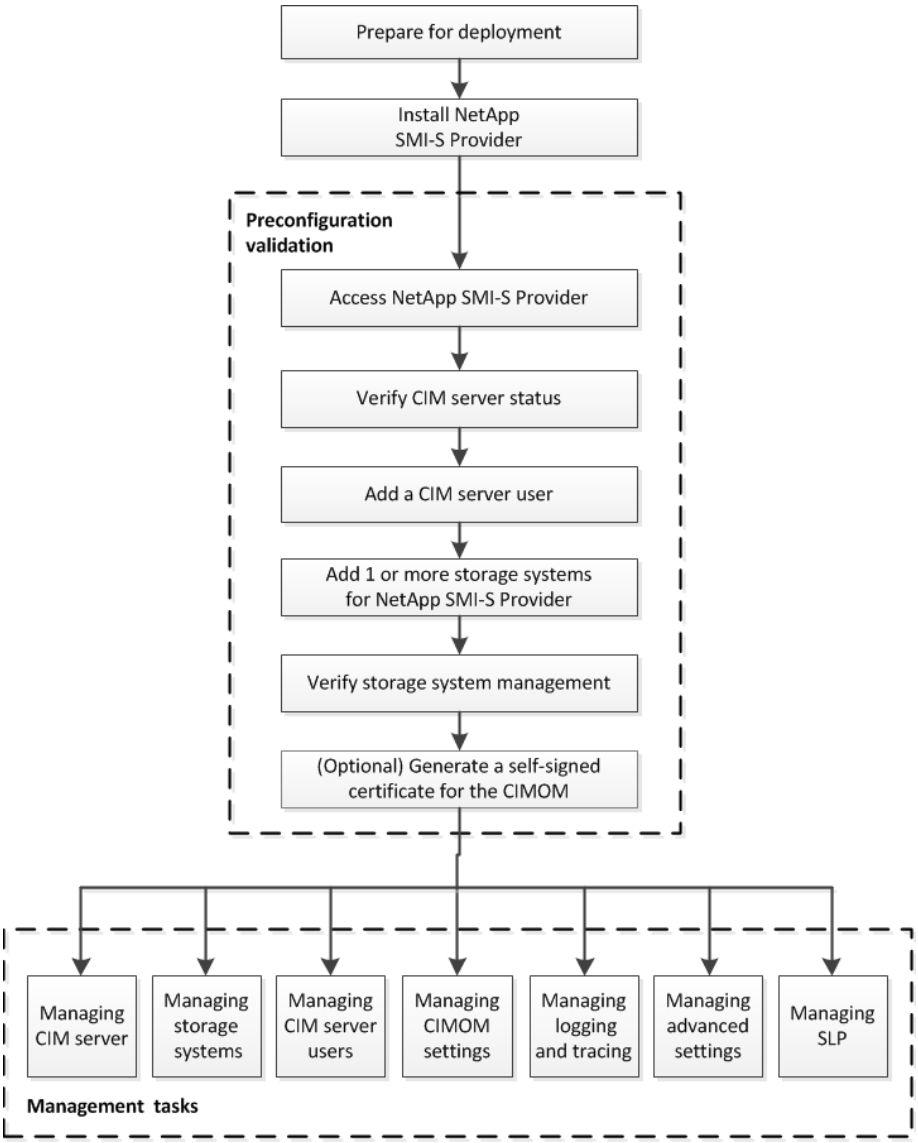
For information about SMI-S v1.6.1, see the SNIA: Technology Standards and Software page.

Related information

SNIA: Technology Standards and Software

Deployment workflow

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



Preparing for deployment

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

Supported operating system versions

Before installing SMI-S Provider, you must verify that the Windows and Linux hosts are running supported operating systems (including Windows and Linux VMs).

Operating system	Supported versions	Required client software
Linux	• SUSE Linux Enterprise Server, version 10.x (32-bit and 64-bit) • SUSE Linux Enterprise Server, version 11.x (32-bit and 64-bit) • Red Hat Enterprise Linux 5.x for x86 (32-bit and 64-bit) • Red Hat Enterprise Linux 6.x for x86 (32-bit and 64-bit) • Red Hat Enterprise Linux 7 (64-bit)	Install the `uncompress` utility in the `/usr/bin` directory.
Windows	• Microsoft Windows Server 2008 R2 Enterprise Edition (64-bit) • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2	Microsoft Visual C++ 2010 runtime libraries are automatically installed during the NetApp SMI-S Provider installation. To avoid potential issues related to runtime libraries, install Microsoft Visual C++ 2010 Redistributable Package (x86) (available at http://www.microsoft.com).

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

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

The following hypervisors are supported:

- Microsoft Windows Server 2008 R2 Hyper-V
- Microsoft Windows Server 2012 R2 Hyper-V
- VMware ESX 3.5

- VMware ESX 4.0
- VMware ESX 4.1
- VMware ESX 5.0
- VMware ESX 5.1
- VMware ESX 5.5
- VMware ESX 6.0

Hardware requirements

You must verify that Windows and Linux hosts meet minimum hardware requirements before installing NetApp SMI-S Provider.

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

Required licenses

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

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

- A SnapMirror license is required on both source and destination clusters to use remote replication.
- FCP, iSCSI, or both FCP and iSCSI licenses are required for creating LUNs on the storage systems.
- A CIFS license is required for creating file shares on supported clustered Data ONTAP storage systems.
- A FlexClone license is required to create LUN clones on 7-Mode storage systems running supported Data ONTAP versions.
- A FlexClone license is required to create LUN clones on clustered storage systems running supported Data ONTAP versions.
- A FlexClone license is required for remote replication test failover.

Supported platforms

NetApp SMI-S Provider supports platforms that run Data ONTAP.

- 7-Mode platforms running Data ONTAP 8.1.x, and 8.2.x
- Cluster platforms running Data ONTAP 8.2.x and 8.3.x

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

NetApp SMI-S Provider supports the following platforms:

- FAS series systems
- V-Series storage systems

Downloading the NetApp SMI-S Provider software package

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

Before you begin

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

Steps

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

Installing NetApp SMI-S Provider

You can install NetApp SMI-S Provider on a Windows or Linux host. However, you cannot revert or downgrade to an earlier version.

Installing NetApp SMI-S Provider on a Windows host

You can install NetApp SMI-S Provider software so that you can manage storage systems that run Data ONTAP. By default, the NetApp SMI-S Provider software is installed in the `C:\Program Files (x86)\NetApp\smis\pegasus` directory.

Before you begin

You must already have the following credentials and software:

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

About this task

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

This installation procedure reflects a fresh install. If you are upgrading your existing version of NetApp SMI-S Provider, refer to the associated "Upgrading" topic in this guide and the *NetApp SMI-S Provider Release Notes* for more information.

NetApp SMI-S Provider 5.2.2 Release Notes

Steps

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

Result

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

Related tasks

Upgrading NetApp SMI-S Provider on a Windows host on page 16

Related references

Types of CIM users and associated operations on page 28

Installing NetApp SMI-S Provider on a Linux host

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

Before you begin

You must already have the following credentials and software:

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

About this task

This installation procedure reflects a fresh install. If you are upgrading your existing version of SMI-S Provider, refer to the associated "Upgrading" topic in this guide and the *NetApp SMI-S Provider Release Notes* for more information.

NetApp SMI-S Provider 5.2.2 Release Notes

Steps

1. Log in as root.
2. Navigate to the directory that contains the NetApp SMI-S Provider software package (`smisprovider-`*`version_number`*`.tar`), and do one of the following:
   - Extract the tar file into a temporary directory and delete all temporary files, including the install script (`install_smisprovider`):

     `tar -xvf smisprovider-`*`version_number`*`.tar`

   - Extract the tar file into a temporary directory without deleting the temporary files:

     `tar -xvf smisprovider-`*`version_number`*`.tar -k`

3. Install the software package:
   - To install the software package and automatically delete all temporary files, including the install script:

     `./install_smisprovider`

   - To install the software package without deleting the temporary files:

     `./install_smisprovider -k`

   - To reinstall the software package and overwrite the previously installed version of NetApp SMI-S Provider:

     `./install_smisprovider -f`

   - To reinstall the software package and keep the SLP configuration files:

     `./install_smisprovider -f -s`

Result

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

Related tasks

Upgrading NetApp SMI-S Provider on a Linux host on page 18

Related references

Types of CIM users and associated operations on page 28

Upgrading NetApp SMI-S Provider

When a new version of SMI-S Provider becomes available, you can upgrade your existing installation to benefit from new and enhanced functionality.

Before upgrading your existing installation, review the *NetApp SMI-S Provider Release Notes* for supported upgrade paths and possible additional notes regarding the upgrade process.

NetApp SMI-S Provider 5.2.2 Release Notes

Prerequisites to upgrading

Due to the change in the path of the installation directory and to avoid losing configuration, database, and repository files, there are some issues that you must consider before upgrading to SMI-S Provider 5.2.2.

If you have SMI-S Provider installed in a Windows environment and SMI-S Provider 5.2.1P1 is your current version, then you can perform an in-place upgrade, without needing to uninstall the existing version.

If you are upgrading SMI-S Provider in a Windows environment from a version earlier than 5.2.1P1, you should first upgrade to SMI-S Provider 5.2.1P1 before upgrading to SMI-S Provider 5.2.2. This two-phase upgrade automatically provides a smooth transition to SMI-S Provider 5.2.2.

Manual Intervention

If you are upgrading SMI-S Provider in a Linux environment, you must manually copy configuration and database files (`cfilers.dat`, `identity.dat`, `hwidcache.dat`, and `cimserver.passwd`) from their current location to the new SMI-S Provider 5.2.2 installation directory. The same is applicable to Windows environment only if you are upgrading from a version earlier than 5.2.1P1 and you choose not to use the recommended two-phase upgrade.

If indications are enabled in SMI-S Provider and clients are subscribed for indications, all indication subscriptions in the SMI-S Provider repository will be lost during the upgrade process. Manually copying these subscriptions might lead to repository corruption. You must re-subscribe to get indications using the client after the upgrade installation process is complete.

For most clients, re-subscribing for indications means removing and re-adding SMI-S Provider to their management. If you are managing SMI-S Provider with Microsoft System Center Virtual Machine Manager, you can re-subscribe for indications by restarting the storage service using the `Restart-Service MsStrgSvc` command and rescan SMI-S Provider in Microsoft System Center Virtual Machine Manager. This avoids the need to remove and re-add SMI-S Provider under the management of Microsoft System Center Virtual Machine Manager Server.

Upgrading NetApp SMI-S Provider on a Windows host

You can upgrade your existing version of SMI-S Provider.

Before you begin

You must already have the following credentials and software:

- Login credentials for the Windows Administrator account
- Supported NetApp SMI-S Provider software package installed on the Windows host

In addition, you should have reviewed the *NetApp SMI-S Provider Release Notes*.

NetApp SMI-S Provider 5.2.2 Release Notes

Steps

1. Log in as Administrator.
2. Depending on your current version of SMI-S Provider, perform the associated steps:

Version	Action
5.2.1P1	Perform the in-place upgrade: **a.** Navigate to the directory that contains the NetApp SMI-S Provider software package (`smisprovider-`*`version_number`*`.msi`), and then double-click the package name. **b.** Complete the steps in the setup wizard. NetApp SMI-S Provider is started automatically toward the end of the installation process.
5.2.1 or earlier	**a.** Create the new NetApp SMI-S Provider 5.2.2 installation directory `C:\Program Files (x86)\NetApp\smis\pegasus`. **b.** Copy the following configuration and database files from the previous installation location (`C:\Program Files (x86)\ONTAP\smis\pegasus`) to the new installation directory. • `cfilers.dat` • `identity.dat` • `hwidcache.dat` • `cimserver.passwd` **c.** Uninstall the existing version of NetApp SMI-S Provider. **d.** Navigate to the directory that contains the NetApp SMI-S Provider software package (`smisprovider-`*`version_number`*`.msi`), and then double-click the package name. **e.** Complete the steps in the setup wizard. NetApp SMI-S Provider is started automatically toward the end of the installation process. **Note:** Be aware of the potential for indication subscription loss. For details on re-subscribing to indications, see “Manual Intervention” within Prerequisites for Upgrading.

Related tasks

Uninstalling NetApp SMI-S Provider from a Windows host on page 20

Related references

Types of CIM users and associated operations on page 28

Upgrading NetApp SMI-S Provider on a Linux host

You can upgrade your existing version of SMI-S Provider.

Before you begin

You must already have the following credentials and software:

- Login credentials for the root account
- Supported NetApp SMI-S Provider software package installed on the Linux host

In addition, you should have reviewed the *NetApp SMI-S Provider Release Notes*.

NetApp SMI-S Provider 5.2.2 Release Notes

Steps

1. Log in as root.
2. Back up the following configuration and database files from the current installation location (`/user/ontap/smis/pegasus`):
   - `cfilers.dat`
   - `identity.dat`
   - `hwidcache.dat`
   - `cimserver.passwd`
3. Uninstall the existing version of NetApp SMI-S Provider.
4. Navigate to the directory that contains the NetApp SMI-S Provider software package (`smisprovider-`*`version_number`*`.tar`), and do one of the following:
   - Extract the `.tar` file into a temporary directory, and then delete all temporary files, including the install script (`install_smisprovider`):

     `tar -xvf smisprovider-`*`version_number`*`.tar`
   - Extract the `.tar` file into a temporary directory without deleting the temporary files:

     `tar -xvf smisprovider-`*`version_number`*`.tar -k`
5. Install the software package:
   - To install the software package and automatically delete all temporary files, including the install script:

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

     `./install_smisprovider -k`
   - To reinstall the software package and overwrite the previously installed version of NetApp SMI-S Provider:

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

     `./install_smisprovider -f -s`

6. Copy the backed-up configuration and database files to the new installation location (`/usr/netapp/smis/pegasus`).
7. Restart the CIM server:

   `smis cimserver restart`

   Note: : Be aware of the potential for indication subscription loss. For details on re-subscribing to get indications using the client, see “Manual Intervention” within Prerequisites for upgrading.

Result

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

Related tasks

Uninstalling NetApp SMI-S Provider from a Linux host on page 20

Related references

Types of CIM users and associated operations on page 28

Uninstalling NetApp SMI-S Provider

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

Uninstalling NetApp SMI-S Provider from a Windows host

Depending on the existing version of SMI-S Provider, you might need to uninstall SMI-S Provider before you can upgrade to the latest version.

About this task

If the existing version of SMI-S Provider is 5.2.1P1 or later, you can perform an in-place upgrade, without uninstalling the existing version.

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

If you do not want a clean re-install, SMI-S Provider will retain the configuration, user, and other database files after the uninstall.

Steps

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

Uninstalling NetApp SMI-S Provider from a Linux host

Uninstalling SMI-S Provider 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_smisprovider` script options:

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

About this task

If you plan to reinstall SMI-S Provider after the uninstall and want to retain your storage system database, then back up the `cfilers.dat` file before you uninstall SMI-S Provider. Then, after the reinstallation, copy this file to the `/usr/netapp/smis/pegasus` directory.

Steps

1. Log in as root.
2. Navigate to the `pegasus/bin` directory (`/usr/netapp/smis/pegasus/bin`), and uninstall SMI-S Provider from the Linux host:

   `./uninstall_smisprovider`

Preconfiguration validation

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

Perform the following tasks before using SMI-S Provider:

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

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

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

Related tasks

Verifying the CIM server status on page 21
Adding a CIM server user on page 22
Verifying that the storage system is working correctly on page 22
Generating a self-signed certificate for the CIM server on page 23
Enabling or disabling authentication for NetApp SMI-S Provider on page 40

Verifying the CIM server status

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

Before you begin

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

Steps

1. Log in as root (Linux) or Administrator (Windows).
2. Access NetApp SMI-S Provider by navigating to the directory where the executables reside by performing one of the following actions:

Platform	Description
Linux	From a command prompt with elevated administrative privileges, navigate to `/usr/netapp/smis/pegasus/bin`.
Windows	From a command prompt with elevated administrative privileges, navigate to `C:\Program Files (x86)\NetApp\smis\pegasus\bin`. Alternatively, from the **Start** > **Programs** menu, right-click **NetApp SMI-S Provider** and select `Run as Administrator`.

3. View the CIM server status:

   `smis cimserver status`

If the CIM server has been started, the following message displays:
`NetApp SMI-S Provider is running.`

Adding a CIM server user

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

Before you begin

- You must already have logged in as root (Linux) or Administrator (Windows).
- You must already have accessed SMI-S Provider.

Steps

1. Depending on your environment, complete one of the following actions:
   - For Windows environments, create a local user account, and add the user to the Administrators group.
   - For Linux environments, you can use the local root account.

   For more information, see your system documentation.
2. Add a CIM server user:

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

   #### Example

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

   `cimuser -a -u chris`
3. When prompted, enter and reenter the password.

Verifying that the storage system is working correctly

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

Before you begin

- You must already have logged in as root (Linux) or Administrator (Windows).
- You must already have accessed SMI-S Provider.

Steps

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

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

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

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

2. Verify the output for the following commands:

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

Related references

smis add on page 49
smis addsecure on page 51
smis disks on page 60
smis list on page 62
smis luns on page 63
smis pools on page 64
smis volumes on page 67

Generating a self-signed certificate for the CIM server

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

Before you begin

- You must already have logged in as root (Linux) or Administrator (Windows).
- You must already have accessed SMI-S Provider.

Steps

1. Generate a private key:

   `openssl genrsa -out cimom.key 2048`

2. Generate a certificate request:

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

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

4. Generate the self-signed certificate:

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

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

5. Copy the `cimom.key` and `cimom.cert` files to the `pegasus` directory (Windows: `C:\Program Files (x86)\NetApp\smis\pegasus`; Linux: `/usr/netapp/smis/pegasus`).

Result

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

Managing the CIM server

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

Before you begin

- You must already have login credentials as root (Linux) or Administrator (Windows).
- You must already have logged in to the host system as root (Linux) or Administrator (Windows).

Steps

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

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

Related references

smis cimserver on page 53

Managing storage systems

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

Before you begin

- You must already have login credentials as root (Linux) or Administrator (Windows).
- You must already have logged in to the host system as root (Linux) or Administrator (Windows).

About this task

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

Steps

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

Action	Command	Additional information
Add a storage system with an HTTP connection between the provider and the storage system	**`smis add`** ***`storage_sys storage_sys_user`***	The command waits for up to 15 minutes for the provider to update the cache and respond.
Add a storage system with an HTTPS connection between the provider and the storage system	**`smis addsecure`** ***`storage_sys storage_sys_user`***	The command waits for up to 15 minutes for the provider to update the cache and respond.
List NFS and CIFS exports for a storage system	**`smis exports`**	n.a.
List the storage systems for the CIMOM repository	**`smis list`**	You can run this command to verify the storage systems in the CIMOM repository before adding or deleting storage systems.
List exported LUNs for a storage system	**`smis luns`**	n.a.

Action	Command	Additional information
Delete a storage system from the CIMOM repository	**`smis delete`** ***`storage_sys`***	If you no longer need to manage a storage system, you can delete it from the CIMOM repository. Because SMI-S Provider gathers information from all storage systems in the CIMOM repository, you should delete an unused storage system from the repository to maintain optimal performance.
List the current CIM server configuration information	**`smis config show`**	n.a.
List the Fibre Channel and iSCSI port information for storage system	**`smis initiators`**	n.a.
List the storage pools for storage system	**`smis pools`**	n.a.
List the traditional and flexible volumes for storage system	**`smis volumes`**	n.a.

Related references

smis add on page 49
smis addsecure on page 51
smis exports on page 60
smis list on page 62
smis luns on page 63
smis delete on page 59
smis config show on page 55
smis initiators on page 61
smis pools on page 64
smis volumes on page 67
Issue entering passwords containing special characters on page 87

Managing CIM server users

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

Before you begin

- You must already have login credentials as root (Linux) or Administrator (Windows).
- You must already have logged in to the host system as root (Linux) or Administrator (Windows).

Steps

1. Access NetApp SMI-S Provider.
2. Depending on your environment, complete one of the following actions:
   - For Windows environments, create a local user account, and add the user to the Administrators group.
   - For Linux environments, you can use the local root account.

   For more information, see your system documentation.
3. Complete one of the following actions:

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

Related references

cimuser on page 47
Types of CIM users and associated operations on page 28
Issue entering passwords containing special characters on page 87

Types of CIM users and associated operations

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

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

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

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

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

Managing CIMOM configuration settings

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

Before you begin

- You must already have login credentials as root (Linux) or Administrator (Windows).
- You must already have logged in to the host system as root (Linux) or Administrator (Windows).

About this task

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

Steps

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

Action	Command	Additional information
Enable the HTTP connection	**`cimconfig -s enableHttpConnection=true -p`**	n.a.
Disable the HTTP connection	**`cimconfig -s enableHttpConnection=false -p`**	n.a.
Enable the HTTPS connection	**`cimconfig -s enableHttpsConnection=true -p`**	n.a.
Disable the HTTPS connection	**`cimconfig -s enableHttpsConnection=false -p`**	n.a.
Modify the HTTP port number	**`cimconfig -s httpPort=`*`new_port_number`*** **`-p`**	By default, the HTTP port number is 5988. If you wanted to change it to 5555, for example, you would input this command: **`cimconfig -s httpPort=5555 -p`**
Modify the HTTPS port number	**`cimconfig -s httpsPort=`*`new_port_number`*** **`-p`**	By default, the HTTP port number is 5989. If you wanted to change it to 5556, for example, you would input this command: **`cimconfig -s httpsPort=5556 -p`**

3. Restart the CIM server:

```
smis cimserver restart
```

Related references

cimconfig on page 45

Managing logging and tracing

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

Configuring log settings

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

Before you begin

- You must already have login credentials as root (Linux) or Administrator (Windows).
- You must already have logged in to the host system as root (Linux) or Administrator (Windows).

Steps

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

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

3. Restart the CIM server:

   `smis cimserver restart`

Related references

Logging levels on page 33

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.

Managing tracing

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

Specifying trace settings

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

Before you begin

- You must already have login credentials as root (Linux) or Administrator (Windows).
- You must already have logged in to the host system as root (Linux) or Administrator (Windows).

Steps

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

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

3. Restart the CIM server:

   `smis cimserver restart`

Related tasks

Specifying trace file size on page 35
Specifying the number of trace files saved on page 35

Related references

Trace setting values on page 34

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 33
Specifying trace file size on page 35
Specifying the number of trace files saved on page 35

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.

Before you begin

- You must already have login credentials as root (Linux) or Administrator (Windows).
- You must already have logged in to the host system as root (Linux) or Administrator (Windows).

Steps

1. Access NetApp SMI-S Provider.
2. 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.)

Example

Specify the trace file size on Linux:

```
export PEGASUS_TRACE_FILE_SIZE=20971520
```

3. Restart the CIM server:

```
smis cimserver restart
```

Related tasks

Specifying trace settings on page 33
Specifying the number of trace files saved on page 35

Related references

Trace setting values on page 34

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.

Before you begin

- You must already have login credentials as root (Linux) or Administrator (Windows).
- You must already have logged in to the host system as root (Linux) or Administrator (Windows).

About this task

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

Steps

1. Access NetApp SMI-S Provider.
2. 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.)

Example

Specify the number of trace files saved on Linux:

```
export PEGASUS_TRACE_FILE_NUM=10
```

3. Restart the CIM server:

```
smis cimserver restart
```

Related tasks

Specifying trace settings on page 33
Specifying trace file size on page 35

Related references

Trace setting values on page 34

Enabling or disabling audit logging for SMI-S commands

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

Before you begin

- You must already have login credentials as root (Linux) or Administrator (Windows).
- You must already have logged in to the host system as root (Linux) or Administrator (Windows).

About this task

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

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

The common practice is to leave audit logging enabled.

The audit log file (`cimserver_auditlog`) is stored in the pegasus log directory (For Windows: `C:\Program Files (x86)\Netapp\smis\pegasus\logs`; for Linux: `/usr/netapp/smis/pegasus/logs`).

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

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

Steps

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

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

Managing SMI-S Provider advanced settings

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

Specifying the SMI-S Provider automatic cache refresh interval

By default, SMI-S Provider automatically retrieves information from storage systems every 5 minutes (300 seconds). You can set the automatic cache refresh interval (`CACHE_REFRESH_SEC` environment variable) to a value from 300 through 86400 seconds (24 hours).

Before you begin

- You must already have login credentials as root (Linux) or Administrator (Windows).
- You must already have logged in to the host system as root (Linux) or Administrator (Windows).

About this task

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

Steps

1. Access NetApp SMI-S Provider.
2. 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.)

3. Restart the CIM server:

```
smis cimserver restart
```

Related tasks

smis refresh on page 65

Specifying the concrete job lifetime value

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

Before you begin

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

- You must already have logged in to the host system as root (Linux) or Administrator (Windows).

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

Before you begin

- You must already have login credentials as root (Linux) or Administrator (Windows).
- You must already have logged in to the host system as root (Linux) or Administrator (Windows).

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 82

Specifying the maximum number of threads per message service queue

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

Before you begin

- You must already have login credentials as root (Linux) or Administrator (Windows).
- You must already have logged in to the host system as root (Linux) or Administrator (Windows).

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 fewer than 20, using the command **`cimcli -n root/ontap niall`** causes the provider 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 provider.

Steps

1. Access NetApp SMI-S Provider.
2. 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.)

3. Restart the CIM server:

   `smis cimserver restart`

Enabling or disabling authentication for NetApp SMI-S Provider

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

Before you begin

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

Steps

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

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

   CIMOM does not use Windows authentication.

3. Restart NetApp SMI-S Provider:

   ```
   smis cimserver restart
   ```

Enabling indications in SMI-S Provider

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

Before you begin

- You must already have login credentials as root (Linux) or Administrator (Windows).
- You must already have logged in to the host system as root (Linux) or Administrator (Windows).

About this task

When `PEGASUS_DISABLE_INDICATIONS` is set to `false`, then Alert (`ONTAP_AlertIndication`), FileSystem Quota (`ONTAP_FSQuotaIndication`), and Lifecycle indications are enabled on NetApp SMI-S Provider.

Steps

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

   ```
   smis cimserver restart
   ```

Related references

SMI-S Provider configuration settings when using ServiceNow on page 41

SMI-S Provider configuration settings when using ServiceNow

If you use ServiceNow, you might want to modify certain SMI-S Provider configuration settings when monitoring NetApp storage.

When using ServiceNow, consider modifying the following environment variables in the SMI-S Provider configuration to take advantage of performance enhancements:

Environment variable	Action
`CACHE_REFRESH_SEC`	For configurations supporting up to 100 Storage Virtual Machines (SVMs), you should increase the `CACHE_REFRESH_SEC` environment variable to a value higher than the default value based on the scale of your storage systems that are managed by SMI-S Provider. If your configuration is smaller, you do not need to increase the `CACHE_REFRESH_SEC` environment variable.

Environment variable	Action
`PEGASUS_DISABLE_INDICATIONS`	For better performance, Alert and Lifecycle indications for SMI-S Provider should be disabled. By default, these indications are disabled.

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.

slp.conf file management

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

Location

- Linux: `/usr/netapp/smis/pegasus/cfg`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\cfg`

Privilege level

A user with a valid user name and password

Description

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

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

Parameters

`interfaces`

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

`multicast`

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

`BroadcastOnly`

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

`securityEnabled`

Enables security for received URLs and attribute lists.

Example

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

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

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

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

CIMOM commands

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

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

Syntax

```
cimconfig options
```

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\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

Change the maximum log file size to 15000 KB:

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

CIM user commands

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

cimuser

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

Syntax

```
cimuser options
```

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\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

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

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

SMI-S Provider commands

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

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

smis `-help`

Displays a command summary.

smis `-help` examples

Displays usage examples.

smis `-help` *`subcommand`*

Displays help for the specified subcommand.

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

smis add

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

Syntax

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

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

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\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

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

`storage_sys_user`

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

`storage_sys_pwd`

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

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

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Storage system-agent and agent-client protocol

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

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

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

Example

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

```
smis add 10.32.1.4 user2
```

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

Example

Add a storage system using IPv6 over HTTP:

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

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

Example

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

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

Note: When operating in a 7-Mode environment, replace *`vsadmin`* with *`root`*.

Related references

Issue entering passwords containing special characters on page 87

smis addsecure

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

Note: Because the OpenSSL version in Data ONTAP is not compatible with the OpenSSL version in NetApp SMI-S Provider, the `smis addsecure` command does not function in Data ONTAP systems operating in 7-Mode.

Syntax

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

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

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\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

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

storage_sys_user

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

storage_sys_pwd

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

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

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Storage system-agent and agent-client protocol

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

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

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

Example

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

```
smis addsecure 10.32.1.4 user2 password2
```

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

Example

Add a storage system using IPv6 over HTTPS:

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

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

Example

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

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

Related references

Issue entering passwords containing special characters on page 87

smis cimom

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

Syntax

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

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Example

The `smis cimom` command and its output:

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

smis cimserver

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

Syntax

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

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\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

Note: The commands in the following examples are within a Linux environment. Messages during the process might vary when run within a Windows environment.

Start the CIM server:

```
smis cimserver start
Logs Directory = /usr/netapp/smis/pegasus/./logs CIM Server x.xx.x
Listening on HTTP port 5988.
Listening on HTTPS port 5989.
Listening on local connection socket.
Started.
Loading storage system(s). This may take a few minutes...
NetApp SMI-S Provider started.
```

Stop the CIM server:

```
smis cimserver stop
NetApp SMI-S Provider stopped
```

Restart the CIM server:

```
smis cimserver restart
CIM Server stopped

Logs Directory = /usr/netapp/smis/pegasus/./logs CIM Server x.xx.x
Listening on HTTP port 5988.
Listening on HTTPS port 5989.
Listening on local connection socket.
Started.
Loading storage system(s). This may take a few minutes...
NetApp SMI-S Provider started.
```

Get the status of the CIM server:

```
smis cimserver status
NetApp SMI-S Provider is running under id xxxxx.
```

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

Privilege level

A user with a valid user name and password

Parameters

name_space

Name space supported by the CIMOM

niall

Enumerate all instance names

ei

Enumerate instances for a class

ni

Enumerate instance names for a class

gi

Get instances for a class

gc

Get class for a class name

class_name

Name of the class for which you want information

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Example

The `smis class` command and its abbreviated output:

```
smis class root/ontap gi CIM_StorageVolume
1:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID
="P3LfGJdC-
mN5",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP
:0135027815"
2:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID
="P3LfGJcmzpHt",SystemCreationClassName="ONTAP_StorageSystem",System
Name="ONTAP:0135027815"
3:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID
="P3LfGJc30t26",SystemCreationClassName="ONTAP_StorageSystem",System
Name="ONTAP:0135027815"
4:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID
="P3LfGJcSgbiT",SystemCreationClassName="ONTAP_StorageSystem",System
Name="ONTAP:0135027815"
5:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID
="P3LfGJcSgrA9",SystemCreationClassName="ONTAP_StorageSystem",System
Name="ONTAP:0135027815"
```

smis config show

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

Syntax

```
smis config show
```

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

Root or sudo (Linux) or Administrator (Windows)

Example

The `smis config show` and its output:

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

tracelevel:
Current value: 4

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

traceFilePath:
Current value: traces/cimserver.trc

enableAuditLog:
Current value: true

logLevel:
Current value: WARNING

sslKeyFilePath:
Current value: cimom.key

sslCertificateFilePath:
Current value: cimom.cert

passwordFilePath:
Current value: cimserver.passwd

enableHttpConnection:
Current value: true

enableHttpsConnection:
Current value: true

httpPort:
Current value: 5988

httpsPort:
Current value: 5989

enableAuthentication:
Current value: true
```

smis crp

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

Syntax

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

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Example

The `smis crp` command and its output:

```
smis crp

PG_RegisteredProfile.InstanceID="SNIA:Profile Registration:1.4.0"
PG_RegisteredProfile.InstanceID="SNIA:SMI-S:1.4.0"
PG_RegisteredProfile.InstanceID="SNIA:SMI-S:1.5.0"
PG_RegisteredProfile.InstanceID="SNIA:SMI-S:1.6.0"
PG_RegisteredProfile.InstanceID="SNIA:Server:1.4.0"
PG_RegisteredProfile.InstanceID="SNIA:Server:1.5.0"
PG_RegisteredProfile.InstanceID="SNIA:Server:1.6.0"
PG_RegisteredProfile.InstanceID="DMTF:Profile Registration:1.4.0"
PG_RegisteredProfile.InstanceID="DMTF:Indications:1.4.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Indication:1.4.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Indication:1.5.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Indication:1.6.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Software:1.4.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Software:1.5.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Software:1.6.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Object Manager Adapter:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:iSCSI Target Ports:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:iSCSI Target Ports:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Software:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Disk Drive Lite:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Disk Drive Lite:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Disk Drive Lite:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Multiple Computer System:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Access Points:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Target Port:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Initiator Ports:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Initiator Ports:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Initiator Ports:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Masking and Mapping:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Masking and Mapping:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Extent Composition:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Extent Composition:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Extent Composition:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Server Performance:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Server Performance:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Physical Package:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Physical Package:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Services:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Services:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Services:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Health:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FileSystem:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Storage:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Export:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Export Manipulation:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Export Manipulation:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File System Manipulation:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Filesystem Manipulation:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Server Manipulation:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FileSystem Quotas:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Job Control:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Job Control:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Location:1.4.0"
```

```
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:NAS Network Port:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Replication Services:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Replication Services:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Capacity Utilization:1.4.0"
```

smis crsp

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

Syntax

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

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Example

The `smis crsp` command and its abbreviated output:

```
smis crsp

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

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

smis delete

The `smis delete` command deletes a storage system.

Syntax

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

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\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

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Example

Delete a storage system labeled mgt-1:

```
smis delete mgt-1
```

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

smis disks

The `smis disks` command displays disk information for storage systems.

Syntax

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

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Example

The `smis disks` command and its abbreviated output:

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

Privilege level

A user with a valid user name and password

Parameters

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Example

The `smis exports` command and its output:

```
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_Storag
eSystem",CSName="ONTAP:68f6b3c0-923a-11e2-
a856-123478563412",FSCreationClassName="ONTAP_LocalFS",FSName="nilesh_vserver
_rootvol",Id="nilesh_vserver_rootvol:0",Name=""
ONTAP_Qtree.CreationClassName="ONTAP_Qtree",CSCreationClassName="ONTAP_Storag
eSystem",CSName="ONTAP:68f6b3c0-923a-11e2-
a856-123478563412",FSCreationClassName="ONTAP_LocalFS",FSName="NAS_vol",Id="N
AS_vol:0",Name=""
ONTAP_Qtree.CreationClassName="ONTAP_Qtree",CSCreationClassName="ONTAP_Storag
eSystem",CSName="ONTAP:68f6b3c0-923a-11e2-
a856-123478563412",FSCreationClassName="ONTAP_LocalFS",FSName="NAS_vol",Id="N
AS_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: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Example

The `smis initiators` command and its abbreviated output:

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

smis licensed

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

Syntax

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

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Example

The `smis licensed` command and its abbreviated output:

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

smis list

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

Syntax

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

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Example

The `smis list` command and its output:

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

smis luns

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

Syntax

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

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Example

The `smis luns` command and its abbreviated output:

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

```
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID
="684f5fb9-0fdd-4b97-8678-188774bdcdd0",SystemCreationClassName="ONT
AP_StorageSystem",SystemName="ONTAP:68f6b3c0-923a-11e2-
a856-123478563412"
```

smis namespaces

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

Syntax

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

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Example

The `smis namespaces` command and its abbreviated output:

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

smis pools

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

Syntax

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

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Example

The `smis pools` command and its abbreviated output:

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

smis refresh

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

Syntax

```
smis refresh storage_system_ip [-t {http | https}]
```

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

storage_system_ip

Refreshes a specific storage system.

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Example

The `smis refresh` command and its output:

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

Related references

Specifying the SMI-S Provider automatic cache refresh interval on page 38

smis slpd

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

Syntax

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

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

Root or sudo (Linux) or Administrator (Windows)

Example

Start the SLP daemon:

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

Stop the SLP daemon:

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

smis version

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

Syntax

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

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Example

The `smis version` command and its output:

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

smis volumes

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

Syntax

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

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

[-t {http | https}]

Protocol to be used: HTTPS (default) or HTTP

Example

The `smis volumes` command and its abbreviated output:

```
smis volumes
ONTAP_LogicalDisk.CreationClassName="ONTAP_LogicalDisk",DeviceID="d46de7f0-39
25-
11df-8516-00a0980558ea",SystemCreationClassName="ONTAP_StorageSystem",SystemN
ame
="ONTAP:0084259609"
ONTAP_LogicalDisk.CreationClassName="ONTAP_LogicalDisk",DeviceID="397cd140-3a
45-
11df-8516-00a0980558ea",SystemCreationClassName="ONTAP_StorageSystem",SystemN
ame
="ONTAP:0084259609"
ONTAP_LogicalDisk.CreationClassName="ONTAP_LogicalDisk",DeviceID="69c472c0-4b
27-
11df-8517-00a0980558ea",SystemCreationClassName="ONTAP_StorageSystem",SystemN
ame
="ONTAP:0084259609"
ONTAP_LogicalDisk.CreationClassName="ONTAP_LogicalDisk",DeviceID="6c7ea0b0-39
27-
11df-8516-00a0980558ea",SystemCreationClassName="ONTAP_StorageSystem",SystemN
ame
="ONTAP:0084259609"
```

SLP commands

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

slptool

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

Syntax

```
slptool [options] subcommand
```

Location

- Linux: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\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: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

service

Specifies the service type.

Example

The `slptool findattrs` command and its abbreviated output:

```
slptool findattrs service:wbem
(template-url-syntax=http://10.229.90.227:5988),(service-id=PG:
10-229-90-227),(service-hi-name=Pegasus),(service-hi-
description=Pegasus CIM Server Version 2.12.0),(template-type=wbem),
(template-version=1.0),(template-description=This template
describes the attributes used for advertising Pegasus CIM Servers.),
(InteropSchemaNamespace=interop),(FunctionalProfilesSupported=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: `/usr/netapp/smis/pegasus/bin`
- Windows: `C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Privilege level

A user with a valid user name and password

Parameters

service

Specifies the service type.

Example

The `slptool findsrvs` command and its output:

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

Using System Center 2012 - Virtual Machine Manager

You can use System Center 2012 - Virtual Machine Manager (SCVMM) or System Center 2012 R2 - Virtual Machine Manager to manage SMI-S Provider functions, including establishing an iSCSI session and allocating storage to host pools. SMI-S Provider cannot run on the same machine as SCVMM.

For information about the following tasks and more, see the associated *Best Practices and Implementation Guide* (TR-4271):

- Tracking lifecycle indications in SCVMM 2012
- Discovering SMI-S Provider in SCVMM 2012
- Allocating storage to host pools using SCVMM 2012
- Establishing an iSCSI session using SCVMM 2012
- Modify the size of a share using SCVMM 2012

Related information

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

Microsoft TechNet: Configuring an SMI-S Provider for iSCSI Target Server

NetApp Technical Report 4271: Best Practices and Implementation Guide for NetApp SMI-S Agent 5.2

Remote replication overview

Using SAN replication with Azure Site Recovery enables you to leverage existing SAN infrastructure for storage replication and combine it with Azure Site Recovery capabilities to protect your mission-critical applications. Using SAN replication instead of Hyper-V replication provides support for guest clusters and ensures replication consistency across different tiers of an application with synchronized replication.

Microsoft Azure Site Recovery orchestrates protection of VMs running on Hyper-V host servers located in System Center Virtual Machine Manager (SCVMM) clouds.

Using Azure Site Recovery, you can fail over and replicate VMs from an on-premise site to Azure, or from one on-premise site to another using SnapMirror (SAN replication).

SAN replication provides support for guest clusters and ensures replication consistency across different tiers of an application with synchronized replication. SAN replication also enables you to replicate guest-clustered VMs with iSCSI or Fibre Channel storage or guest-clustered VMs using shared virtual hard disks (VHDX).

Regarding remote replication, you should be aware of the following limitations:

- SMI-S Provider supports fully discovered model for the remote application feature.
  This means that Primary site SMI-S Provider manages recovery site storage in addition to the primary site storage. The Recovery site SMI-S Provider manages primary site storage in addition to recovery site storage. However, the Primary site VMM Server manages the primary site storage using Primary site SMI-S Provider, and Recovery site VMM Server manages recovery site storage using Recovery site SMI-S Provider.

- For an Initial Replication job within the Enable Replication workflow, the Azure Site Recovery timeout is 2 hours. If initializing a baseline transfer on a source volume takes more than 2 hours, it is recommended that you create and initialize SnapMirror out-of-band using CLI or other NetApp tools. After SnapMirror is initialized, you must refresh SMI-S Provider and rescan it in Microsoft System Center Virtual Machine Manager to manage this SnapMirror relationship with Azure Site Recovery.
- SMI-S Provider currently supports the management of Data Protection (DP) SnapMirror relationships.

Remote replication requirements

Before you use remote replication from Microsoft Azure Site Recovery (ASR), you must meet the requirements of ASR, clustered Data ONTAP, and VM networks operating in SCVMM.

Azure Site Recovery requirements

- You must have an Azure account.
- The Azure Site Recovery feature must be enabled.
- A Hyper-V host server cluster must be deployed in the source and destination sites, running at least Windows Server 2012 with the latest updates and managed by SCVMM 2012 R2 SAN disaster recovery preview build.
- At least one cloud should be configured on the primary VMM server (which would be protected) and one cloud configured on the secondary VMM server.

Data ONTAP requirements

- You must be running clustered Data ONTAP 8.2.x or 8.3.x.

Requirements for VM networks in SCVMM

- VM network mapping must be configured so that the virtual machines connect to VM networks after failover.
- The source VM network must be linked to a logical network that is associated with the cloud.
- In Azure Site Recovery, the networks in both the primary and the secondary sites should be paired.

License requirements

- A SnapMirror license is required on both source and destination clusters to use remote replication.
- A FlexClone license is required for remote replication test failover.

Links to operations involved in configuring the SCVMM cloud fabric

After you have the deployment requirements completed, you should configure the System Center Virtual Machine Manager (SCVMM) cloud fabric. This includes assigning fabric elements such as host groups, networks, storage, and library resources to the cloud; allocating cloud capacity; and assigning cloud users.

For information on how to perform the following operations, follow the corresponding link:

- *Creating a Private Cloud in VMM Overview*

- *Walkthrough: Creating Private Clouds with System Center 2012 SP1 Virtual Machine Manager - Build Your Private Cloud in a Month*
- *How to Create a Hardware Profile*
- *Configuring Self-Service in VMM*

Setting up cluster and SVM peering for disaster recovery

To use remote replication from Microsoft Azure Site Recovery, you must set up cluster and SVM peering for disaster recovery, using SnapMirror on a NetApp Cluster Mode array.

Before you begin

You must have SCVMM 2012 R2 UR5 (update rollup 5) installed to use remote replication.

You must have verified that you have enough space on your aggregate to work, using the following:

```
user1_cluster::> storage aggregate show-space
```

Steps

1. Create and configure your routing groups:

   a. Create SVMs:

   Example

   ```
   user1_cluster::> vserver create -vserver user1_vs3 -rootvolume
   user1_vs3_rootvol -aggregate aggr1_node3 -ns-switch file -
   rootvolume-security-style mixed
   [Job 1311575] Job
   succeeded:
   Vserver creation completed

   user1_cluster::> vserver create -vserver user1_vs4 -rootvolume
   user1_vs4_rootvol -aggregate aggr1_node4 -ns-switch file -
   rootvolume-security-style mixed
   [Job 1311577] Job
   succeeded:
   Vserver creation completed
   ```

   b. Create network interfaces:

   Example

   ```
   user1_cluster::> net int create -vserver user1_vs3 -lif
   vs3_iscsi_mgmt -home-port e0a -address 10.60.167.23 -role data -
   data-protocol iscsi -home-node smis-ts-3170-3 -netmask
   255.255.255.0
     (network interface create)

   Info: Your interface was created successfully; the routing group
         d10.60.167.0/24 was created

   user1_cluster::>
   user1_cluster::> net int create -vserver user1_vs3 -lif
   vs3_iscsi_partner -home-port e0a -address 10.60.167.24 -role data -
   data-protocol iscsi -home-node smis-ts-3170-4 -netmask
   255.255.255.0
     (network interface create)

   user1_cluster::>

   user1_cluster::> net int create -vserver user1_vs4 -lif
   ```

```
vs4_iscsi_mgmt -home-port e0a -address 10.60.167.25 -role data -
data-protocol iscsi -home-node smis-ts-3170-4 -netmask
255.255.255.0
  (network interface create)

user1_cluster::> net int create -vserver user1_vs4 -lif
vs4_iscsi_partner -home-port e0a -address 10.60.167.26 -role data -
data-protocol iscsi -home-node smis-ts-3170-3 -netmask
255.255.255.0
  (network interface create)

user1_cluster::>
Info: Your interface was created successfully; the routing group
      d10.60.167.0/24 was created
```

c. Create routing groups:

Example

```
user1_cluster::> net routing-groups route create -vserver
user1_vs3 -routing-group d10.60.167.0/24 -destination 0.0.0.0/0 -
gateway 10.60.167.1
  (network routing-groups route create)

user1_cluster::>
user1_cluster::> net routing-groups route create -vserver
user1_vs4 -routing-group d10.60.167.0/24 -destination 0.0.0.0/0 -
gateway 10.60.167.1
  (network routing-groups route create)
```

d. Enable management traffic on one of the logical interfaces:

Example

```
user1_cluster::> net int modify -vserver user1_vs3 -lif
vs3_iscsi_mgmt -firewall-policy mgmt
  (network interface modify)

user1_cluster::>
user1_cluster::> net int modify -vserver user1_vs4 -lif
vs4_iscsi_mgmt -firewall-policy mgmt
  (network interface modify)

user1_cluster::>
```

These interfaces are added to SMI-S providers.

2. Create and unlock a user on each SVM:

Example

a. Create a user on each SVM:

Example

```
user1_cluster::> security login password -vserver user1_vs3 -
username vsadmin

Enter a new password:
Enter it again:

user1_cluster::>
user1_cluster::> security login password -vserver user1_vs4 -
```

```
username vsadmin

Enter a new password:
Enter it again:
```

b. Unlock the users:

Example

```
user1_cluster::> security login unlock -vserver user1_vs3 -
username vsadmin

user1_cluster::>
user1_cluster::> security login unlock -vserver user1_vs4 -
username vsadmin
```

3. Create iSCSI service:

Example

```
user1_cluster::> iscsi create -vserver user1_vs3

user1_cluster::>
user1_cluster::> iscsi create -vserver user1_vs4

user1_cluster::>
```

4. Populate the SVMs and volumes and establish a peer relationship between the SVMs.

a. Create a couple of volumes on each SVM:

Example

```
user1_cluster::> vol create -volume datavol1 -vserver user1_vs3 -
aggregate aggr1_node3 -size 1GB -state online -type RW
  (volume create)
[Job 1311655] Job succeeded:
Successful

user1_cluster::>
user1_cluster::> vol create -volume datavol2 -vserver user1_vs3 -
aggregate aggr1_node3 -size 1GB -state online -type RW
  (volume create)
[Job 1311664] Job succeeded:
Successful

user1_cluster::> vol create -volume datavol1 -vserver user1_vs4 -
aggregate aggr1_node4 -size 1GB -state online -type DP
  (volume create)
[Job 1311669] Job succeeded:
Successful

user1_cluster::> vol create -volume datavol2 -vserver user1_vs4 -
aggregate aggr1_node4 -size 1GB -state online -type DP
  (volume create)
[Job 1311670] Job succeeded:
Successful

user1_cluster::>
```

On the target SVM, the volume type must be Type DP (Data Protected).

The language of source and destination volumes must be the same. This cannot be modified after the volume is created.

b. Create a LUN on each volume for the source SVM:

Example

```
user1_cluster::> lun create -vserver user1_vs3 -path /vol/datavol1/
lun1 -size 200MB -ostype windows -space-reserve enabled

Created a LUN of size 204m (213857280)

user1_cluster::>
user1_cluster::> lun create -vserver user1_vs3 -path /vol/datavol1/
lun2 -size 200MB -ostype windows -space-reserve enabled

Created a LUN of size 204m (213857280)

user1_cluster::>
user1_cluster::> lun create -vserver user1_vs3 -path /vol/datavol2/
lun1 -size 200MB -ostype windows -space-reserve enabled

Created a LUN of size 204m (213857280)

user1_cluster::> lun create -vserver user1_vs3 -path /vol/datavol2/
lun2 -size 200MB -ostype windows -space-reserve enabled

Created a LUN of size 204m (213857280)

user1_cluster::>
```

c. Create a peer relationship between the two SVMs in the same cluster:

Example

```
user1_cluster::> vserver peer create -vserver user1_vs3 -peer-
vserver user1_vs4 -applications SnapMirror -peer-cluster
user1_cluster

Info: 'vserver peer create' command is successful.

user1_cluster::>
```

5. Set up the SnapMirror relationship:

a. Create a SnapMirror relationship:

Example

```
user1_cluster::> SnapMirror create -source-path user1_vs3:datavol1
-destination-path user1_vs4:datavol1
Operation succeeded: SnapMirror create for the relationship with
destination "user1_vs4:datavol1".
```

b. Initialize the SnapMirror relationship:

Example

```
user1_cluster::> SnapMirror initialize -source-path
user1_vs3:datavol1 -destination-path user1_vs4:datavol1
Operation is queued: SnapMirror initialize of destination
"user1_vs4:datavol1".
```

c. Verify the SnapMirror relationship:

Example

```
user1_cluster::> SnapMirror show

    Progress
Source            Destination  Mirror  Relationship
Total             Last
Path        Type  Path         State   Status        Progress
Healthy Updated
----------- ---- ------------ ------- -------------- ---------
------- --------
user1_vs3:datavol1
            DP   user1_vs4:datavol1
                              SnapMirrored
                                      Idle           -
true    -
```

6. Create a peer relationship between two clusters:

a. Create a LIF on the node hosting the SVM of each cluster for inter-cluster communication.

Example

On cluster1:

```
smis-ts-3170-1_2::> net int create -vserver smis-ts-3170-1 -lif
interclus_lif -role intercluster -home-node smis-ts-3170-1 -home-
port e0b -address 10.60.167.9 -netmask 255.255.255.0 -status-admin
up -failover-policy nextavail -firewall-policy mgmt
  (network interface create)

Info: Your interface was created successfully; the routing group
i10.60.167.0/24 was created
```

On cluster2:

```
user1_cluster::> net int create -vserver smis-ts-3170-4 -lif
interclus_lif -role intercluster -home-node smis-ts-3170-4 -home-
port e0a -address 10.60.167.13 -netmask 255.255.255.0 -status-
admin up -failover-policy nextavail -firewall-policy intercluster
  (network interface create)

Info: Your interface was created successfully; the routing group
i10.60.167.0/24 was created
```

b. Create a cluster peer relationship on either cluster:

Example

```
smis-ts-3170-1_2::> cluster peer create -peer-addrs 10.60.167.13 -
username admin
```

If you fail to enter the correct password, then you must try this operation from the other cluster.

c. Because the intercluster LIF was created there, log in to the node management interface of the other node:

Example

```
user1_cluster::> cluster peer create -peer-addrs 10.60.167.9 -
username admin

Remote Password:

user1_cluster::> cluster peer show
Peer Cluster Name          Cluster Serial Number Availability
-------------------------- --------------------- ---------------
smis-ts-3170-1_2           1-80-000011           Available

user1_cluster::>
```

d. Create SVM peering between SVMs on the two clusters.

   Perform this operation on the node from which you established cluster peer relationship:

   Example

```
user1_cluster::> vserver peer create -vserver user1_vs4 -peer-
vserver SMIS_VS5 -applications SnapMirror -peer-cluster smis-
ts-3170-1_2

Info: [Job 1378689] 'vserver peer create' job queued
```

e. Accept the SVM peer request on other cluster:

   Example

```
smis-ts-3170-1_2::> vserver peer show
            Peer        Peer
Vserver     Vserver     State
----------- ----------- ------------
SMIS_VS5    SMIS_VS6    peered
SMIS_VS5    user1_vs4  pending
SMIS_VS6    SMIS_VS5    peered
3 entries were displayed.

smis-ts-3170-1_2::> vserver peer accept -vserver SMIS_VS5 -peer-
vserver user1_vs4

Info: [Job 1701431] 'vserver peer accept' job queued
```

f. Set up a SnapMirror relationship between the two volumes on the two clusters:

   Example

```
user1_cluster::> SnapMirror create -source-volume datavol2 -source-
vserver SMIS_VS5 -destination-volume datavol2 -destination-vserver
user1_vs4 -type DP -schedule
5min

Operation succeeded: SnapMirror create for the relationship with
destination
"user1_vs4:datavol2".




user1_cluster::> SnapMirror initialize -source-volume datavol2 -
```

```
source-vserver SMIS_VS5 -destination-volume datavol2 -destination-
vserver user1_vs4 -type DP
Operation is queued: SnapMirror initialize of destination
"user1_vs4:datavol2".
```

On the destination volume, the volume type must be Type DP (Data Protected).

The language of source and destination volumes must be the same. This cannot be modified after the volume is created.

7. Add the SVMs by using NetApp SMI-S Provider:

Example

```
user1_cluster::>smis add user1_vs3 username "password"
user1_cluster::>smis add user1_vs4 username "password"
```

8. If you want to remove peering between SVMs, you must release the SnapMirror relationships from the source:

Example

```
smis-ts-3170-1_2::> SnapMirror release -destination-path
user1_vs4:datavol2 -source-path SMIS_VS5:datavol2
[Job 1725034] Job succeeded: SnapMirror Release
Succeeded



smis-ts-3170-1_2::>

smis-ts-3170-1_2::> SnapMirror release -destination-path
user1_vs4:datavol2 -source-path SMIS_VS5:datavol2

Error: command failed: Source information for relationship with
destination "user1_vs4:datavol2" not found. (entry doesn't exist)

smis-ts-3170-1_2::>
smis-ts-3170-1_2::> vserver peer delete -vserver SMIS_VS5 -peer-
vserver user1_vs4

Info: [Job 1725050] 'vserver peer delete' job queued

smis-ts-3170-1_2::>

user1_cluster::*> vserver peer delete -vserver user1_vs4 -peer-
vserver SMIS_VS5

Info: [Job 1387367] 'vserver peer delete' job queued

user1_cluster::*>
user1_cluster::*>
user1_cluster::*> vserver peer show
            Peer        Peer
Vserver     Vserver     State
----------- ----------- ------------
user1_vs3  user1_vs4  peered
user1_vs4  SMIS_VS5    deleted
user1_vs4  user1_vs3  peered
3 entries were displayed.

user1_cluster::*>
user1_cluster::*> vserver peer show -vserver user1_vs4 -peer-vserver
SMIS_VS5

  Local Vserver Name: user1_vs4
```

```
    Peer Vserver Name: SMIS_VS5
        Peering State: deleted

user1_cluster::*>
```

9. Configure to create clones of ReplicationGroup for TestFailover:

Example

```
user1_cluster::> vserver modify -vserver user1_vs4 -aggr-list
aggr1_node4
```

This is a one-time, out-of-band operation and should be performed from the cluster or node management LIF.

10. Configure a 15-minute schedule to support default the recovery point objective (RPO) of disaster recovery:

Example

```
user1_cluster::> schedule cron create -name 15min -minute 00,15,30,45
  (job schedule cron create)

user1_cluster::> schedule show
  (job schedule show)
Name         Type      Description
-----------  ---------
-------------------------------------------------------
….
15min     cron      @:00,:15,:30,:45
```

If RPO details are not provided for CreateGroupReplica, the SnapMirror relationship defaults to the *15min* schedule.

You can configure the RPO value using the environment variable `SMIS_SNAPMIRROR_RPO`. The variable value is defined in seconds, and must meet the following conditions:

- Must be ≥60 seconds
- Must be in increments of 60

Related references

SnapMirror broken, a failover happened on page 84

Related information

NetApp Documentation: Clustered Data ONTAP 8.2 Express Guides

Troubleshooting SMI-S Provider

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

Possible errors while loading shared libraries

Message

The error messages received might vary, even for the same executable.

`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/netapp/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/netapp/smis/pegasus/bin/cimcli: symbol lookup error: /usr/netapp/smis/pegasus/bin/cimcli: undefined symbol: _ZN7Pegasus16StringConversion21decimalStringToUint64EPKcRy` when executing `cimcli`.

These examples are not all-inclusive.

Description

This message (and similar messages) 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/netapp/smis/pegasus/lib
```

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

Access is denied error

Message

`Access is denied.`

Description

This message occurs in two possible situations:

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

Corrective action

Complete the action that corresponds to the situation:

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

Connection refused

Message

`Connection refused`

Cause

The CIM server has not been started.

Corrective action

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

```
smis cimserver status
```

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

```
smis cimserver start
```

Filer return: No ontap element in response

Message

`Filer return: No ontap element in response`.

Description

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

Corrective action

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

Related tasks

Specifying the ONTAPI timeout value on page 39

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.

ProviderLoadFailure

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

Message

```
/usr/netapp/smis/pegasus/bin/smis list cimcli CIMException: Cmd= ni
Object=ONTAP_FilerData Code= 1
```

```
CIM_ERR_FAILED: ProviderLoadFailure:
```

```
(/usr/netapp/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. Set `LD_LIBRARY_PATH`:

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

2. Enter the following commands:

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

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

   `ldd /usr/netapp/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, check the NetApp Support Site and download the correct binaries.

Warning 26130

Message

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

Description

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

Corrective action

1. On each host machine, add the IP address of each storage system to the iSCSI Initiator application.

2. If required, on each storage system, for each host machine, create one unique igroup linked with the proper iSCSI node name from the corresponding host machine.

3. For each host machine connected to Data ONTAP, open the MPIO application and add the following 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. Set the storage pool again.

SnapMirror broken, a failover happened

Message

```
SnapMirror broken, a failover happened
```

Description

This message occurs during remote replication setup, when the user creates a job for CreateGroupReplica and the job returns the broken status from the array. This might occur for either of two reasons:

1. Another request performed a failover using the same SnapMirror relationship as the user initialized.
2. The destination pool or ReplicationGroup was read-write.
   The destination pool or ReplicationGroup must be read-only to succeed. If it is read-write, the initialization fails, leaving the SnapMirror relationship in a broken state.

Corrective action

For the first scenario, run the CreateGroupReplica job again.

For the second scenario, reconfigure the destination pool or ReplicationGroup as read-only.

Related tasks

Setting up cluster and SVM peering for disaster recovery on page 73

EntityRef: expecting ';' error

Message

```
cimcli CIMException: Cmd= ci Object= ONTAP_FilerData Code= 1
CIM_ERR_FAILED: Filer return: EntityRef: expecting ';' - With
storage system
```

Description

This message occurs on Linux systems when you modify the `/etc/issue` and `/etc/issue.net` files.

Corrective action

Revert the modified `/etc/issue` and `/etc/issue.net` files to the original default settings.

HostAgentAccessDenied (ID: 26263)

Message

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

Description

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

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

Corrective action

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

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

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

Related references

Types of CIM users and associated operations on page 28

Cannot connect to localhost:5988

Message

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

Description

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

Corrective action

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

`cimconfig -g enableHttpConnection`

`cimconfig -g enableHttpsConnection`

`cimconfig -g httpPort`

`cimconfig -g httpsPort`

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

`cimconfig -s enableHttpConnection -p`

`smis cimserver restart`

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

```
cimconfig -s httpPort=5988 -p
```

```
smis cimserver restart
```

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

Cannot connect to localhost:5989

Message

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

Description

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

Corrective action

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

```
cimconfig -g enableHttpsConnection
```

```
cimconfig -g httpsPort
```

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

```
cimconfig -s enableHttpsConnection -p
```

```
smis cimserver restart
```

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

```
cimconfig -s httpsPort=5989 -p
```

```
smis cimserver restart
```

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

SMI-S Provider crashes in Linux

Issue

SMI-S Provider crashes in Linux.

Cause

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

Corrective action

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

- Core file from the `/usr/netapp/smis/pegasus/bin` directory or the /root directory
- Log files from the `/usr/netapp/smis/pegasus/logs` directory
- Trace files from the `/usr/netapp/smis/pegasus/traces` directory

- The files `version.txt` and `cimserver_current.conf` from the `/usr/netapp/smis/pegasus` directory

Multiprocess mode disabled in Linux

Description

NetApp SMI-S Provider does not currently support multiprocess mode in Linux.

SMI-S Provider crashes in Windows

Issue

SMI-S Provider crashes in Windows.

Cause

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

Corrective action

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

- Dump file from the `C:\Program Files (x86)\NetApp\smis\pegasus\pegasus\logs` directory
  When running Windows Server 2012, the provider might not generate a dump file. If the provider does not generate a dump file, it can be found under the Windows Error Reporting tool.
- Log files from the `C:\Program Files (x86)\NetApp\smis\pegasus\pegasus\logs` directory
- Trace files from the `C:\Program Files (x86)\NetApp\smis\pegasus\pegasus\traces` directory
  Messages similar to the following also appear in the trace file:
  ```
  23-May-2013 20:46:36.874 INFO cimserver: createMiniDump: SMI-S Agent has crashed, attempting to generate a dump file
  23-May-2013 20:46:37.14 INFO cimserver: createMiniDump: Process dumped to C:\Program Files (x86)\netapp\smis\pegasus\logs\SMI-S Agent-8be55da-2011_05_23-20_46_36.dmp
  ```
- The files `version.txt` and `cimserver_current.conf` from the `C:\Program Files (x86)\NetApp\smis\pegasus\pegasus` directory

Issue entering passwords containing special characters

Issue

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

Cause

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

, & ' < > ; | = ^ "

Corrective action

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

Issuing passwords with special characters

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

Related tasks

Managing storage systems on page 26
Managing CIM server users on page 28

Related references

smis add on page 49
smis addsecure on page 51

Manually enabling ALUA in 7-Mode environments

Because NetApp SMI-S Provider 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 LUNs. You should use Data ONTAP MPIO DSM 3.5 for clustered LUNs.

ALUA is automatically enabled for clustered Data ONTAP.

Cloning technology used in SMI-S Provider

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

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

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

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

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 NetApp SMI-S Provider.

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

Requirement for using fileshares on Windows

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

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

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

Creating a volume to be used for CIFS shares and SCVMM

When creating a volume to be used for CIFS shares and System Center Virtual Machine Manager (SCVMM), the volume has to be of NTFS type. To create the volume with NTFS, enter the following:

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

Nondefault firewalls must have ports manually added as exceptions

Issue

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

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

Cause

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

Corrective action

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

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

Issue

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

Cause

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

Corrective action

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

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

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

Adding a storage system that uses port 8000 for HTTP traffic

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

No response from the server

Issue

The server does not respond when queried.

Cause

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

Corrective action

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

```
smis list
```

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

```
smis add storage_sys storage_sys_user storage_sys_pwd
```

Runtime library issues

Issue

You encounter runtime library issues.

Corrective action

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

Related information

Microsoft

NetApp SMI-S Provider takes a long time to start

Description

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

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

Total managed space for a storage pool (volume) discrepancy

Issue

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

Cause

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

Corrective action

This is an expected behavior; no corrective action.

During 7-Mode aggregate creation, SMI-S Provider incorrectly reports initial aggregate size

Issue

During 7-Mode aggregate creation, SMI-S Provider might report back an initial aggregate size of 16 exabytes.

Corrective action

None. After the aggregate has finished being created, the aggregate size will be reflected correctly.

Network path not found

Message

`Network path not found`

Description

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

Typically, the domain DNS server should automatically update the host record within 24 to 48 hours when a new host is configured in the domain. However, this update does not always automatically happen.

Corrective action

- If you are a domain administrator, manually update the DNS host record.
- If you are not a domain administrator, update the host file (`C:\Windows\System32\drivers\etc\hosts`).
  The host file does not have a file extension (`.txt`).

Insufficient system resources exist to complete the requested service

Message

```
Insufficient system resources exist to complete the requested
service
```

Description

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

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

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

Corrective action

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

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

SMB share size dropping to 0 in SCVMM

Issue

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

Cause

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

Corrective action

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

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

Issue

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

Cause

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

Corrective action

1. Uninstall SMI-S Provider and install it again.

2. Run the rescan operation in SCVMM for the SMI-S Provider.

Relationship with destination <volume> already exists

Message

```
VMM could not invoke method CreateGroupReplica on ,,,,:
CIM_ERR_FAILED: Filer return: Relationship with destination
<volumename> already exists. - With storage system <SVM>
```

Description

This message occurs when old, deleted SnapMirror relationships on the primary replication group or FlexVol volume are not released properly and the Azure Site Recovery EnableProtection operation fails in SCVMM.

Corrective action

1. Execute the `snapmirror release` command on the primary cluster or SVM interface to release old, deleted SnapMirror relationships from the primary replication group or FlexVol volume.
2. Rescan the primary SMI-S Provider in the primary SCVMM server and recovery SMI-S Provider in the recovery SCVMM server.
3. Execute the EnableProtection operation in Azure Site Recovery.

Any SnapMirror relationship that is deleted should also be released to unlock and delete the Snapshot copy on the primary volume in that SnapMirror relationship.

Copyright information

Copyright © 1994–2016 NetApp, Inc. All rights reserved. Printed in the U.S.

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

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

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

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

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

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

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at *http://www.netapp.com/us/legal/netapptmlist.aspx*.

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email to *doccomments@netapp.com*. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

A

access
SMI-S Provider *21*
troubleshooting *81*, *91*
access denied error
resolving *81*
adding
CIM server users *28*
storage system using nondefault HTTP port, error caused by *89*
storage system using nondefault HTTPS port, error caused by *89*
adding users
CIM server *22*
addition
of storage systems to CIMOM repository *26*
aggregates
size reported incorrectly by SMI-S Agent during creation of 7-Mode *91*
Alert indications
enabling *41*
allowing
SSL-encrypted traffic *30*
unencrypted traffic *30*
ALUA
manually enabling in 7-Mode environments *88*
audit logging for SMI-S commands
enabling or disabling *36*
authentication for SMI-S Provider
enabling, disabling *40*
Azure Site Recovery
requirements *72*

B

before using SMI-S Provider
validation process *21*

C

cache refresh
manual *65*
one-time *65*
cache refresh interval, SMI-S
specifying *38*
Cannot connect to localhost:5988
resolving error *85*
Cannot connect to localhost:5989 error
resolving *86*
changing
default HTTP port number *30*
HTTPS port number *30*
CIFS shares
See fileshares
CIM server
restarting *25*
reviewing status *25*
starting *25*
starting slow *90*
stopping *25*
user passwords, modifying *28*
users, listing *28*
CIM server status
verifying *21*
CIM server users
adding *22*, *28*
removing *28*
CIM user
Built-in Domain Administrator user *28*
Built-in Local Administrator user *28*
Domain administrator of the Administrators group *28*
Domain user of the Local Administrators group *28*
Domain user of the Users group *28*
Local user of the Local Administrators group *28*
Local user of the Users group *28*
operations that can be performed *28*
CIM-XML encoding over HTTPS exchange protocol
described *7*
cimconfig
command options *45*
cimconfig command
options *45*
CIMOM
listing registered namespaces for *64*
CIMOM configuration settings
managing using the `cimconfig` command and options *45*
CIMOM repository
adding storage systems *22*, *26*
deleting storage systems *26*
listing storage systems *26*
cimuser
command options *47*
cimuser command
options *47*
clients
unable to receive indications from SMI-S Provider *89*
cloning technology *88*
cluster and SVM peering
setting up for disaster recovery *73*
CMS server log
changing level of system messages written to *32*
changing location of messages written to *32*
commands
cimconfig *45*
cimuser *47*
slptool *68*
slptool findattrs *68*
slptool findsrvs *69*
smis *49*
smis add *49*
smis addsecure *51*
smis cimom *52*
smis cimserver *53*

smis class *54*
smis config show *55*
smis crp *56*
smis crsp *58*
smis delete *59*
smis disks *60*
smis exports *60*
smis initiators *61*
smis licensed *62*
smis list *62*
smis luns *63*
smis namespaces *64*
smis pools *64*
smis refresh *65*
smis slpd *66*
smis version *66*
smis volumes *67*
commands, SMI-S
enabling or disabling audit logging *36*
comments
how to send feedback about documentation *96*
components
CIMOM *7*
provider objects *7*
repository *7*
SMI-S Provider *7*
concrete job lifetime value
specifying *38*
configuration files
slp.conf *43*
configuration settings, CIMOM
managing using the `cimconfig` command and options *45*
connection errors
cannot connect to localhost:5988 *85*
connection refused *82*
connection failure
troubleshooting *86*
connections, HTTPS
disabling *30*
crashes, SMI-S Provider
guidelines for handling in Linux *86*
guidelines for handling in Windows *87*

D

deleting storage systems
CIMOM repository *26*
deployment
preparing SMI-S Provider *9*
disabling
authentication for SMI-S Provider *40*
HTTP connections *30*
HTTPS connections *30*
disabling audit logging
for SMI-S commands *36*
disaster recovery
setting up cluster and SVM peering *73*
documentation
how to receive automatic notification of changes to *96*
how to send feedback about *96*
downgrade
not supported *13*

E

editing
slp.conf *43*
enabling
authentication for SMI-S Provider *40*
HTTP connections *30*
HTTPS connections *30*
enabling audit logging
for SMI-S commands *36*
enabling indications
Alert, FileSystem Quota, and Lifecycle *41*
enabling, manually
ALUA in 7-Mode environments *88*
EntityRef: expecting ';' error
troubleshooting *84*
error messages
Azure Site Recovery EnableProtection operation fails in SCVMM *93*
cannot open shared object file *81*
Cimserver not running *81*
Error while loading shared libraries *81*
No such file or directory *81*
Relationship with destination <volume> already exists *93*
SnapMirror broken *84*
symbol lookup error *81*
undefined symbol *81*
using to troubleshoot SMI-S Provider *81*
errors
access denied *81*
cannot connect to localhost:5988 *85*
cannot connect to localhost:5989 *86*
connection refused *82*
EntityRef: expecting ';' *84*
Insufficient system resources exist to complete the requested service *91*
Network path not found *91*
no ontap element in response *82*

F

features, new
in this release of SMI-S Provider *6*
feedback
how to send comments about documentation *96*
Filer return; No ontap element in response error
resolving *82*
fileshares
creating on NTFS-only volumes *89*
using on Windows *89*
FileSystem Quota indications
enabling *41*
firewalls
adding ports *89*
requirements for nondefault *89*
FlexClone technology
when used *88*

G

generating self-signed certificate for CIM server
Linux *23*
Windows *23*

H

hardware requirements
verifying before installing SMI-S Agent *11*
HostAgentAccessDenied error
troubleshooting *85*
hosts, Linux
upgrading SMI-S Provider software on *18*
hosts, Windows
upgrading SMI-S Provider software on *16*
HTTP
using nondefault port, error caused by *89*
HTTP connections
disabling *30*
enabling *30*
HTTP port number, default
changing *30*
HTTPS
using nondefault port, error caused by *89*
HTTPS connection
adding a storage system with *51*
HTTPS connections
disabling *30*
enabling *30*
HTTPS port number
changing *30*
default *30*

I

ID: 26263
troubleshooting *85*
important objects
confirming visibility of *88*
indications
enabling Alert, FileSystem Quota, and Lifecycle *41*
troubleshooting *89*
information
how to send feedback about improving documentation *96*
installation requirements
platform *12*
supported operating system versions *10*
verifying hardware minimums *11*
installing NetApp SMI-S Provider
on a Linux host *14*
installing NetApp SMI-S Provider software
default location *13*
on a Windows host *13*
insufficient resources
troubleshooting *39*
Insufficient system resources exist to complete the requested service error
resolving *91*
interval, SMI-S cache refresh
specifying *38*
issues, runtime library
troubleshooting *90*
issues, troubleshooting
slow starting CIM server *90*
SMI-S crashes in Linux *86*
SMI-S crashes in Windows *87*

J

job lifetime value, concrete
specifying *38*

L

library issues, runtime
troubleshooting *90*
licenses
required *11*
Lifecycle indications
enabling *41*
lifetime value, concrete job
specifying *38*
Linux hosts
upgrading SMI-S Provider software on *18*
listing
CIM server users *28*
exported LUNS *26*
NFS and CIFS exports *26*
storage systems *26*
log, CMS server
configuring message level and location settings *32*
logging
levels *33*
logging, audit
enabling or disabling *36*
LUN clone split
Snapshot operations not allowed during *82*
LUN clones
when used *88*

M

managed space
total value discrepancy *91*
manually enabling
ALUA in 7-Mode environments *88*
message service queue
specifying the maximum number of threads per *39*
modifying
CIM server user passwords *28*
multiprocess mode
disabled in Linux *87*

N

NetApp SMI-S Provider
prerequisites for upgrading software *16*
NetApp SMI-S Provider software
upgrading on a Linux host *18*
upgrading on a Windows host *16*
Network path not found error
resolving *91*

new features
in this release of SMI-S Provider *6*
no response from server *90*
nondefault firewalls
adding ports as exceptions manually *89*
nondefault HTTP port
causes error when used to add a storage system *89*
nondefault HTTPS port
causes error when used to add a storage system *89*
NTFS volumes
creating fileshares on *89*

O

objects, important
confirming visibility of *88*
ONTAPI timeout value
changing *39*
operating systems
versions supported by SMI-S Provider *10*
options
cimconfig command *45*
overview
SMI-S Provider *6*

P

passwords
issue when containing special characters *87*
passwords, CIM server user
modifying *28*
peering, cluster and SVM
setting up for disaster recovery *73*
performance
impact of number of threads per message service queue *39*
performance impact
of specifying trace settings *33*
performance information
for different Data ONTAP environments *6*
port number, HTTP default
changing *30*
preconfiguration validation
workflow *21*
product overview
SMI-S Provider *6*
protocols
CIM-XML encoding over HTTPS *7*
described *7*
SLP *7*
Provider, SMI-S
product overview *6*
ProviderLoadFailure
troubleshooting *83*

R

refresh interval, SMI-S cache
specifying *38*
remote replication
advantages of using *71*
cluster and SVM peering *73*
disaster recovery setup *73*
links to tasks for configuring the cloud fabric *72*
requirements *72*
SAN replication
advantages of using *71*
SnapMirror *73*
removing
CIM server users *28*
required hardware
verifying before installing SMI-S Agent *11*
requirements
Azure Site Recovery *72*
Data ONTAP for remote replication *72*
remote replication *72*
VM networks for remote replication *72*
requirements, installation
verifying hardware minimums *11*
rescan operation failed, in SCVMM
not able to locate or communicate with SMI-S Provider *92*
restarting
CIM server *25*
server, CIM
restarting *25*
SMI-S Provider
and restarting the CIM server *25*
runtime library
troubleshooting issues *90*

S

SCVMM
links to tasks for configuring the cloud fabric *72*
rescan operation failed to locate or communicate with SMI-S Provider *92*
SMB share size dropping to 0 *92*
uses of *71*
self-signed certificate for CIM server
generating (Linux) *23*
generating (Windows) *23*
server status, CIM
reviewing *25*
server users, CIM
removing *28*
server, CIM
starting *25*
stopping *25*
verifying status of *21*
servers
no response *90*
service queue
specifying the maximum number of threads per *39*
ServiceNow, using
cache refresh *41*
PEGASUS_DISABLE_INDICATIONS environment variable *41*
settings, CIMOM configuration
managing using the `cimconfig` command and options *45*
settings, trace
specifying, impact on performance *33*
share size, SMB
dropping to 0 in SCVMM *92*

sizing information
for different Data ONTAP environments *6*
SLP
configuration settings *43*
managing *43*
starting *43*
stopping *43*
SLP discovery protocol
described *7*
slp.conf
configuration files *43*
editing *43*
parameters *43*
slptool *68*
slptool command options *68*
slptool findattrs command
syntax and example *68*
slptool findsrvs
command *69*
parameters *69*
SMB share size drop
troubleshooting *92*
SMI-S cache refresh interval
manual *65*
one-time *65*
specifying *38*
SMI-S commands
enabling or disabling audit logging *36*
SMI-S profiles and subprofiles
version number *8*
SMI-S Provider
accessing *21*
new features in this release *6*
prerequisites for upgrading software *16*
starting *25*
stopping *25*
unable to communicate with client *89*
SMI-S Provider authentication
enabling, disabling *40*
SMI-S Provider crashes
guidelines for handling in Linux *86*
guidelines for handling in Windows *87*
SMI-S Provider software
upgrading on a Linux host *18*
upgrading on a Windows host *16*
smis
commands *49*
smis add
command *49*
examples *49*
parameters *49*
purpose *49*
smis addsecure
command *51*
parameters *51*
purpose *51*
smis cimom
command *52*
parameters *52*
purpose *52*
smis cimserver
command *53*
parameters *53*
purpose *53*
smis class
command *54*
parameters *54*
purpose *54*
smis config show
command *55*
parameters *55*
purpose *55*
smis crp command
parameters *56*
purpose *56*
smis crsp command
parameters *58*
purpose *58*
smis delete
command *59*
parameters *59*
purpose *59*
smis disks
command *60*
parameters *60*
purpose *60*
smis exports
command *60*
parameters *60*
purpose *60*
smis initiators
command *61*
parameters *61*
purpose *61*
smis licensed
command *62*
parameters *62*
purpose *62*
smis list
command *62*
parameters *62*
purpose *62*
smis luns
command *63*
parameters *63*
purpose *63*
smis namespaces
command *64*
parameters *64*
purpose *64*
smis pools
command *64*
parameters *64*
purpose *64*
smis refresh command
parameters *65*
purpose *65*
smis slpd
command *66*
parameters *66*
purpose *66*
smis version command
parameters *66*
purpose *66*
smis volumes
command *67*

parameters *67*
purpose *67*
SnapMirror broken
error message help *84*
Snapshot operations
not allowed during LUN clone split *82*
software
downloading package *12*
software installation, SMI-S Provider
default location *13*
on a Linux host *14*
on a Windows host *13*
software upgrades, SMI-S Provider
prerequisites for *16*
software, SMI-S Provider
upgrading on a Linux host *18*
upgrading on a Windows host *16*
special characters
issue when using in passwords *87*
specifying
concrete job lifetime value *38*
specifying trace file size *35*
SSL-encrypted traffic
how to allow *30*
starting
CIM server *25*
SMI-S Provider *25*
starting CIM server
slowness *90*
status, CIM server
reviewing *25*
stopping
CIM server *25*
SMI-S Provider *25*
storage capacity allocation
warning 26130 *83*
storage pools
incorrect aggregate size reported by SMI-S Agent during 7-Mode aggregate creation *91*
storage systems
adding to CIMOM repository *22*, *26*
deleting from CIMOM repository *26*
error caused when adding using a nondefault HTTP port *89*
error caused when adding using a nondefault HTTPS port *89*
listing of CIMOM repository *26*
managing *26*
verifying proper operation *22*
Storage Virtual Machines
clustered environments *26*
suggestions
how to send feedback about documentation *96*
supported platforms
Data ONTAP *12*
SVM and cluster peering
setting up for disaster recovery *73*
SVMs
See Storage Virtual Machines
System Center 2012
See SCVMM

T

tasks performed using SMI-S Provider
list of *6*
threads per message service queue
impact on performance *39*
specifying the maximum number *39*
timeout value, ONTAPI
changing *39*
trace files
changing the default number of *35*
size *35*
trace settings
specifying, impact on performance *33*
values *34*
traffic, unencrypted
how to allow *30*
troubleshooting
adding ports to nondefault firewalls *89*
Azure Site Recovery EnableProtection operation fails in SVCMM *93*
Cannot connect to localhost:5988 error *85*
Cannot connect to localhost:5989 error
resolving *86*
EntityRef: expecting ';' *84*
HostAgentAccessDenied error *85*
ID: 26263 *85*
Insufficient system resources exist to complete the requested service error *91*
issues loading shared libraries *81*
ProviderLoadFailure *83*
refused connection *82*
runtime library issues *90*
slow starting CIM server *90*
SMB share size drop *92*
SMI-S crashes in Linux environment *86*
SMI-S crashes in Windows *87*
Snapshot operations during LUN clone split *82*
storage pool allocated to host group *83*
total managed space discrepancy *91*
using error messages *81*
warning 26130 *83*
Twitter
how to receive automatic notification of documentation changes *96*

U

unencrypted traffic
how to allow *30*
uninstalling SMI-S Provider
from a Linux host *20*
from a Windows host *20*
required before upgrade *20*
upgrades
prerequisites for SMI-S Provider software *16*
upgrading
SMI-S Provider software on a Linux host *18*
SMI-S Provider software on a Windows host *16*
user access control
to the CIM server *28*
user passwords, CIM server
modifying *28*

users, CIM server
adding *22*
removing *28*
uses
SMI-S Provider *6*

V

verifying
CIM server status *21*
verifying proper storage system operation
steps *22*
visibility of important objects
confirming *88*
Vserver
See Storage Virtual Machine
Vservers
See Storage Virtual Machines

W

warning 26130
troubleshooting *83*
Windows hosts
upgrading SMI-S Provider software on *16*