NetApp SANtricity® SMI-S Provider 11.73

Installation and Configuration Guide

May 2022 | 215-15153_D0
doccomments@netapp.com

NetApp®

Table of Contents

About This Guide

This installation guide describes how to install, configure, deploy, and uninstall the NetApp SANtricity® SMI-S Provider.

Overview of the NetApp SANtricity SMI-S Provider

The Storage Networking Industry Association (SNIA) began the Storage Management Initiative (SMI) to develop a standard for managing multi-vendor storage networks. The SMI specification (SMI-S) is based on the Common Information Model (CIM) and the Web-Based Enterprise Management (WBEM) standards defined by the Distributed Management Task Force. SMI-S has been adopted by all of the major storage vendors. Visit www.snia.org for more information about SMI-S.

SMI-enabled management applications are known as clients. To allow clients to manage a storage device, a SMI-S Provider is required. SMI-S Providers can be implemented in two ways:

- An SMI-S Provider can be implemented as a proxy interface to translate the application programming interface (API) of a device to an SMI-S-compliant interface. This implementation is the quickest path to SMI-S compliance, but it requires that the proxy provider and a Common Information Model Object Manager (CIMOM) are installed on a server. A CIMOM receives, validates, and authenticates CIM requests from the client application. The CIMOM directs the requests to the appropriate device provider.
- An SMI-S Provider can be a native feature of the storage device API. This implementation is sometimes referred to as an *embedded agent*.

NetApp's implementation of SMI-S takes the proxy interface approach. The NetApp SMI-S Provider must run on a server on the storage network. The open source CIMOM OpenPegasus is installed during the installation.

What's New

This section lists what is new with SMI-S Provider 11.73.

- Updated to OpenSSL 1.1.1n

Abbreviations, Acronyms, Terms, and Definitions

The following table shows the abbreviations, acronyms, and definitions of terms used in this document.

Abbreviations, Acronyms, Terms	Definitions
CIM	Common Information Model
CIMOM	Common Information Model Object Manager
SA	Service Agent
SLP	Service Location Protocol
SMI-S	Storage Management Initiative Specification

Supported Profiles and Subprofiles

This section describes profiles and subprofiles supported in SMI-S Provider 11.73.

- Block Storage Views
- Thin Provisioning
- Replication Services
- Physical Package
- Profile Registration
- Device Credentials
- Multiple Computer System
- Block Services
- Disk Drive Lite
- Copy Services
- Job Control
- Extent Composition
- Disk Sparing
- Initiator Port (Fibre Channel, SAS, and SATA)
- Target Port (Fibre Channel and SAS)
- iSCSI Target Port
- Access Points
- Indications
- Masking And Mapping
- Location
- Software Inventory
- Software Update
- Block Server Performance

  NOTE: Block Server Performance Statistics are not available for controller firmware versions prior to 7.10.

- Erasure
- Battery
- Storage Asymmetry
- Message Log
- Storage Enclosure

For detailed information about specific implementations of the SMI-S Provider for these profiles, refer to *SMI-S Provider Functional Specification*, which you can obtain from your storage vendor.

Supported Operating Systems for SMI-S Provider 11.73

Review the specifications for your operating system (OS) to make sure that your system meets the minimum requirements. The versions listed in the table were current at the time of release, but it is possible that more recent versions of the OS have been added since then.

For the most up to date information on supported operating systems for the SANtricity SMI-S Provider, please refer to the NetApp Interoperability Matrix Tool (IMT).

NOTE: Not all versions of controller firmware are supported for I/O attach to all OS versions listed here.

Operating System	Version
Windows Clients	Windows 10
Windows Server	2012 R2 2016 2019

Operating System	Version
Windows Server 2012 Hyper-V	2012 R2*
VMware ESXi*	N/A
*Hypervisors are supported for SMI-S Provider running on a supported guest OS.	

Component	Version
SMI-S Provider	11.73.0G00.0001
SMI-S	1.6.1
OpenPegasus CIMOM	2.14.1 on the Windows operating system
OpenSSL	1.1.1n The latest version of OpenSSL is integrated at the time of publication. Regular OpenSSL patches are issued for critical security updates that affect integration with OpenPegasus. **NOTE:** Subsequent to release of the provider, OpenSSL patch packages may be made available to address security vulnerabilities.
OpenSLP	2.0.0

Supported Firmware Versions

For a complete and up-to-date listing of all compatible client operating systems and firmware for the SMI-S Provider, refer to the NetApp Interoperability Matrix Tool.

System Requirements

To install and run SMI-S Provider, make sure your system meets the following requirements:

- **Memory** – At least 1 GB. 2 GB is recommended.
- **Connectivity**
  - Ethernet with 100BASE-T minimum (Gigabit Ethernet is recommended), TCP/IP.
- **Port** – TCP port 5988 or TCP port 5989, or any other available port if these ports are not available.
- **Storage array password (Optional)**
  - The Device Credentials profile requires the storage array password (SharedSecret) for modifying operations.
  - SMI-S Provider persistently tracks an instance of SharedSecret for each storage array.
  - A password is not mandatory if you have no password set on the storage array.
- **Scalability**
  - There is no hard limit on how many storage systems can be supported by a single provider instance.

- For large configurations that exceed more than 5000 volumes, a distributed architecture is recommended to ensure product performance remains at a high level.

- **Legacy Management (SYMbol)**
  - Legacy management interface (SYMbol) must be enabled. If you disabled the interface, see the *SANtricity System Manager* online help or the *Command Line Reference* for information on re-enabling it.

Installing and Uninstalling SMI-S Provider

This section describes how to install, upgrade, and uninstall SMI-S Provider for the supported operating systems, including OpenPegasus CIM sever.

NOTE: Due to its inclusion in the distribution and the client applications ability to follow the workflow, CIMCLI is used within the workflow examples throughout this document.

Windows operating system install and uninstall process

Installing SMI-S Provider (Windows operating system)

SMI-S Provider is packaged as an installation executable file for Windows operating system servers.

NOTE: In order to maintain compatibility with the Federal Information Processing Standard (FIPS), the SMI-S Provider installer for the Windows operating system uses FIPS-level encryption for digital signatures.

ATTENTION! The following workflow is incompatible for users upgrading from SMI-S Provider version 10.26 or earlier.

Keep these guidelines in mind when adding a CIMOM user while enabling the CIMOM authentication:

- If you enter a user name that is not a valid user on the local system, an error message is displayed.
- The password should be less than or equal to eight characters. Passwords with more than eight characters are truncated.
- CIMOM authentication is enabled only after at least one user is added successfully.

1. Move the SMI-S Provider installation archive file or executable file into the file system on the server where you want to install SMI-S Provider.
2. For the Windows operating system, double-click the installation executable icon, and follow the directions provided on the screen.

   NOTE: During the installation for Windows operating systems, the command line user interface ArrayMgmtUtil (Array Management Utility) installs at `<install dir>\netapp\pegasus\bin`. This utility allows you to add and remove storage arrays to the Provider while the system is online, and it allows you to expand the repositories of snapshot volumes that you created using Replication Service profile. For information about using this command line interface, see Array Management Utility.

   a. Enter an IP address for each storage array that you want to use. The installation opens a text file in Notepad.
   b. Close Notepad. After you have added the storage arrays and closed Notepad, the installation program continues normally. Follow the instructions and prompts on the screen.
   c. Choose the CIMOM authentication type. The default is *Disable Authentication*, which allows unrestricted access to the CIMOM server. To restrict access to the CIMOM server to authorized users only, select *Enable Authentication*, and then follow the instructions and prompts to enter the username and password of the authorized users of the CIMOM server.

NOTE: The username is not case sensitive, so usernames `admin` and `ADmin` are treated the same. When installing the SMI-S Provider for the first time, you can add all users who need access to the CIMOM server. If you add a username and then realize it should not have been added, be sure to remove that username. If you need to add or remove CIMOM users after this initial installation, you can use the `cimuser` command. In addition, when upgrading the SMI-S Provider, you need to add back in all the authorized users and remove users who are no longer authorized for access.

d. Select the option to add firewall exceptions for SMI-S traffic (CIM-XML ports 5988-5990 and SLP port 427).
e. Delete the installation executable file.

3. Delete the original archive file and installation file.

   If you want to change the configuration of OpenPegasus CIM Server, see Configuring the OpenPegasus CIM Server.

Silent Installation for SMI-S Provider on Windows operating system

The SMI-S Provider silent mode installation package for Windows operating system supports the command line option, which saves time when you need to install the Provider software on a large number of servers. During silent mode installation, no user interface is displayed on the screen. The installer completes the installation without user interaction. However, during silent mode installation, you can use the command line option `ADDUSERS` to add multiple Pegasus users and, thereby, enable CIMOM authentication.

When using the command line interface, consider the following:

- If the user name specified with the -u option is not a valid user on the local system, that username is not added in the Pegasus.
- Because this is a silent mode installation, no error is displayed if adding a user fails.
- `-u` and `-p` options work in pair, otherwise, the users might not be added properly. For example, `-u` must be followed by `-p`.
- Authentication can be enabled only if at least one user is successfully added with Pegasus.
- Username is not case sensitive. Username `admin` and `ADmin` are treated the same.
- The maximum length of the password is eight characters. If more than eight characters are specified, the password is truncated to eight characters.
- During Provider upgrade, be sure to add back in all the authorized users and remove users who are no longer authorized for access.

The SMI-S Provider installation is packaged as an executable file for Windows operating system servers. You can execute the installer in silent mode by performing the following procedure:

1. Move the SMI-S Provider installation package into the file system on the server where you want to install SMI-S Provider.
2. Open the Windows command prompt, and run the following command:

   ```
   <installer>.exe /s /v"/qn”
   ```

   a. During the silent mode installation, you can use the command line to restrict access to the CIMOM server to authorized users only by adding the username and password of the authorized users of the CIMOM server. You can also add firewall exceptions for SMI-S traffic by specifying the FIREWALL option. To perform these tasks using the command line, enter the installer name, and then enter the following options:

   ```
   <installer>.exe /s /v"/qn" [/V"ADDUSERS=\"-u <username1>
   ```

```
-p <password1> -u <username2> -p <password2>...\""] [/ V"FIREWALL=yes"]
[/v"/L*v\"LogFile.log\""]
```

The installation logs are captured in the LogFile.log, if specified during installation. In the command line, username and password are separated by option `-u` and `-p`, respectively. In that example, /s /v“/qn" indicates a silent mode installation. Note the use of the small v. Also, note the capital V that is used for setting the command line argument.

NOTE: You cannot remove a username during silent mode installation. To remove a user name, use the `cimuser` command after installation is completed. See Configuring the OpenPegasus CIM Server.

3. If desired, delete the original installation file.

To change the configuration of OpenPegasus CIM, see Configuring the OpenPegasus CIM Server.

OpenSLP configuration for Windows operating system

OpenSLP is installed during the SMI-S Provider installation process for the Windows operating system. Upon completion of the SMI-S provider installation process, you can configure OpenSLP for Windows.

1. From the Service menu, select **Service Location Protocol**.

   The slpd service starts.
2. Enter the following command at the prompt:

```
cimconfig -s slp=true -p
```

   The SLP service turns within Pegasus.
3. To restart the cimserver, select **Pegasus CIM Object Manager** from the Service menu.

   The cimserver restarts.

NOTE: When uninstalling the SMI-S Provider from the Windows operating system, all OpenSLP-related services stop and are removed automatically.

Uninstalling SMI-S Provider (Windows operating system)

Perform the following to uninstall the SMI-S Provider within the Windows operating system:

1. From the Windows desktop, click **Start,** and select **Control Panel**.

   The Control Panel window is displayed.
2. Select **Programs**.

   The Uninstall or Change a Program window is displayed.
3. Within the Uninstall or Change a Program window, select **NetApp SANtricity SMI-S Provider**, and click **Uninstall**.

   The uninstaller for the SMI-S Provider is displayed.
4. Run the uninstaller for the SMI-S Provider.

   The SMI-S Provider is uninstalled from the Windows operating system.

NOTE: The uninstall process might leave files that were created by the SMI-S provider after the installation was complete. These files might include trace files, repository files, and other administrative files. Manually delete these files to remove the SMI-S provider completely.

Configuring the OpenPegasus CIM Server

Use these commands to perform OpenPegasus CIM configuration operations only when you need to change the default settings. To see the default settings, run the following commands to list the configuration options:

```
cimconfig -l
cimconfig -g
```

Restart the OpenPegasus CIM server after each operation completes.

- Set an http port

  ```
  # cimconfig -s httpPort=<port> -p
  ```

- Set an https port

  ```
  # cimconfig -s httpsPort=<port> -p
  ```

- Enable or disable the http connection

  ```
  # cimconfig -s enableHttpConnection={true | false} -p
  ```

- Enable or disable the https connection

  ```
  # cimconfig -s enableHttpsConnection={true | false} -p
  ```

- Enable or disable authentication

  ```
  # cimconfig -s enableAuthentication={false | true} -p
  ```

- Add a user

  ```
  # cimuser -a -u <username> -w <password>
  ```

- Remove a user

  ```
  # cimuser -r -u <username>
  ```

- Generate a list of authenticated users

  ```
  # cimuser -l
  ```

- Enable or disable service location protocol (SLP)

  ```
  # cimconfig -s slp={true | false} -p
  ```

If SLP is enabled, refer to the following table for additional settings information. Commands use the following format `cimconfig -s <propertyName>={true|false} -p`, in which **<propertyName>** is a bold column heading in the following table.

For more detailed questions, refer to the documentation available in the source release archive at www.openpegasus.org.

Commands	Settings	Behavior
`runInternalPegasusSLP`	true	External Pegasus SLP registration runs in cimserver with a default registration timeout of 3 hours, which is the same as the SLP default timeout.
`registerExternalPegasusSLP`	false	
`registerExternalOpenSLP`	false	
`registerMultipleSLP`	false	

Commands	Settings	Behavior
`runInternalPegasusSLP`	false	External Pegasus SLP registration runs in cimserver with a default registration timeout of 3 hours, which is the same as the SLP default timeout.
`registerExternalPegasusSLP`	true	
`registerExternalOpenSLP`	false	
`registerMultipleSLP`	false	

Commands	Settings	Behavior
`runInternalPegasusSLP`	false	External OpenSLP registration runs in cimserver.
`registerExternalPegasusSLP`	false	
`registerExternalOpenSLP`	true	
`registerMultipleSLP`	false	

Commands	Settings	Behavior
`runInternalPegasusSLP`	false	External OpenSLP registration is attempted and falls back to external Pegasus SLP registration if it fails (default setting).
`registerExternalPegasusSLP`	false	
`registerExternalOpenSLP`	true	
`registerMultipleSLP`	true	

Commands	Settings	Behavior
`runInternalPegasusSLP`	false	External Pegasus SLP registration is attempted and falls back to external OpenSLP registration if it fails.
`registerExternalPegasusSLP`	true	
`registerExternalOpenSLP`	false	
`registerMultipleSLP`	true	

Commands	Settings	Behavior
`runInternalPegasusSLP`	false	All other combinations of settings have undefined behavior.
`registerExternalPegasusSLP`	true	
`registerExternalOpenSLP`	false	
`registerMultipleSLP`	true	

Microsoft Storage Management API Support

Windows 8 and Windows Server 2012 introduced the new Microsoft Storage Management API (SMAPI) replacing the existing VDS interface. VDS deprecated by Microsoft and the management applications in Windows 8 and Windows Server 2012 does not use the VDS providers. However, the existing VSS provider continues to be supported in Windows 8 and Windows Server 2012.

This release of NetApp E-Series SMI-S Provider supports management of E-Series storage arrays using management applications based on SMAPI.

The programmable interfaces to SMAPI include WMI interface and PowerShell cmdlets. The File and Storage Service user interface in Windows Server 2012 uses SMAPI.

The online document for storage cmdlets in Windows PowerShell is available at:

http://technet.microsoft.com/en-us/library/hh848705.aspx.

The MSDN documentation for WMI classes with descriptions for properties, methods, and associations is available at:

http://msdn.microsoft.com/en-us/library/hh830613(v=vs.85).aspx.

To obtain the PowerShell cmdlets related to the storage management, use the following PowerShell cmdlet:

```
get-command -Module storage
```

The PowerShell cmdlets used to configure SMI-S Provider with Storage Service have been categorized by Microsoft into the *`SMISConfig`* module. To obtain the cmdlets, use the following command:

```
get-command -Module SMISConfig
```

During Installation of SMI-S Provider

The https connection is enabled by default during installation on port 5989 to enable secure communication. The Microsoft Storage Service uses https for listening to indications from provider and, therefore, dynamic cache update of Storage Service is available only when the provider is registered with https mode.

Make sure that you use CIMOM authentication along with https communication while registering the provider with Microsoft Storage Service for a secure communication. An option is provided during installation to enable CIMOM authentication and to add users during installation. For more details about CIMOM authentication, refer to Installing SMI-S Provider (Windows Operating System).

Options are provided during provider installation in the Windows operating system to create firewall exceptions automatically or CIM-XML transport ports (5988/5989/5990) and SLP discovery port 427. Using these options during installation minimizes the manual steps required for configuring the provider after the installation to support SMAPI.

To add firewall exceptions manually in either Windows operating system, go to Adding Firewall Exclusions for SMI-S Traffic.

After Installation of SMI-S Provider

Before registering the provider with the Microsoft Management Service, be certain that the storage subsystems are added to and managed by the provider. When using https mode of communication with the Microsoft Storage Service, be certain of the following:

1. The sslClientVerificationMode configuration property is set to disabled in the OpenPegasus configuration and that the status of sslClientVerificationMode property is get/set with the cimconfig command.
2. The SSL certificate of the CIMOM server is placed in the directory pointed to by the PEGASUS_HOME environment variable.

During Uninstallation of SMI-S Provider

Be certain that the provider is unregistered from Microsoft Storage Service before the provider is uninstalled. Otherwise, the Microsoft Storage Service cache retains the data collected from the provider before the uninstallation and that stale data can be removed only by manually updating the cache.

The firewall exceptions are removed automatically in the Windows operating system while you uninstall the provider.

Adding Firewall Exclusions for SMI-S Traffic

Windows

```
netsh advfirewall firewall add rule name="SLP-udp" dir=in protocol=UDP
localport=427 action=allow

netsh advfirewall firewall add rule name="SLP-tcp" dir=in protocol=TCP
localport=427 action=allow

netsh advfirewall firewall add rule name="CIM-XML in" dir=in
protocol=TCP localport=5988-5989 action=allow

netsh advfirewall firewall add rule name="SLP-udp" dir=out protocol=UDP
localport=427 action=allow

netsh advfirewall firewall add rule name="SLP-tcp" dir=out protocol=TCP
localport=427 action=allow

netsh advfirewall firewall add rule name="CIM-XML out" dir=out
protocol=TCP localport=5988-5990 action=allow
```

Windows-related FAQs and Known Limitations

Configuring port 5990 for indications in Windows 2012 server

The Microsoft Storage Service uses an https listener using port 5990 in compliance with DMTF requirements. To configure port 5990 to listen to CIM indications, do the following on the Windows Server 2012 system:

1. Open TCP port 5990 through the firewall by using the following command:

   ```
   netsh advfirewall firewall add rule name="CIM-XML Indication" dir=in
   protocol=TCP localport=5990 action=allow
   ```

2. Allow Network Service to bind to HTTPS port 5990 as follows (Delete old ACL for http://*:5990, if any):

   ```
   netsh http add urlacl url=https://*:5990/ user="NT AUTHORITY\NETWORK SERVICE
   ```

SMI-S Provider registration in Microsoft Storage Service allows you to register the same provider, but with different IP addresses. For example, if you register a provider twice using `localhost` and an IP address, both are registered and shows as duplicate information for all the CIM instances. For example, entering the two `commands Register-SmisProvider -ConnectionUri 'https:// AA.BB.CC.DD:5989'and Register-SmisProvider -ConnectionUri 'https://localhost:5989` registers the same provider instance twice with Storage Service.

Be sure to perform a manual cache update of Microsoft Storage service whenever Microsoft Storage Service or provider is restarted.

You should perform a manual cache update in Microsoft Storage Service whenever you change a configuration in the storage subsystem using any application other than Microsoft Storage Service. You can limit the cache update to one storage subsystem by using the following cmdlet:

```
PS C:\Users\Administrator> Update-StorageProviderCache - DiscoveryLevel Full -
RootObject ([ref]%SA1) -StorageSubSystem $SA1
```

In this command, `$SA1` is:

```
PS C:\Users\Administrator> $SA1 = Get-StorageSubSystem - FriendlyName
<Storage_Subsystem_Name>
```

This cmdlet performs the cache update faster when multiple storage subsystems are being managed by Microsoft Storage Service.

If a PowerShell cmdlet to change the storage array configuration fails with Unspecified Error, this could be due to a CIM operation timeout. This could occur even if the storage array configuration was successfully changed. Make certain that you perform a manual cache update in Microsoft Storage Service, and verify that the requested configuration change for the storage array was successful.

For a list of unsupported SMAPI properties and methods, see Unsupported SMAPI Properties and Methods.

Using SMI-S Provider

This chapter describes how to use the following functions of SMI-S Provider:

- Starting and stopping the OpenPegasus CIM server
- Adding a device to manage
- Removing a device
- Setting a device password
- Configuring the SMI-S Provider

NOTE: Due to its inclusion in the distribution and the client applications ability to follow the workflow, CIMCLI is used within the workflow examples throughout this document.

Starting and Stopping the OpenPegasus CIM Server

You can start and stop the Pegasus CIM Object Manager server any time you want.

1. For the Windows operating system, open the Service window by performing one of these actions:
   - From the Service window, start or stop the Pegasus CIM Object Manager.
   - If you want to use the command line interface (CLI), type `net start cimserver`. You also can stop the Pegasus CIM Object Manager server by typing `net stop cimserver`.

NOTE: Performing this procedure does not install the Pegasus CIM Object Manager server as a daemon by default. The system administrator can set up the daemon if desired.

Adding a Device to Manage

At installation, you are prompted to enter IP addresses into a file. After this initial installation, the SMI-enabled client must use the SMI-S Provider Proxy Server System Management profile to add or remove devices.

NOTE: Arrays can be added to the `ArrayHost.txt` file during installation only. You must use the `ArrayMgmtUtil` to add arrays post-installation of the SMI-S Provider. For information on how to add arrays through the `ArrayMgmtUtil`, refer to Adding a Storage Array.

Removing a Device

At installation, you are prompted to enter IP addresses into a file. If you entered the IP addresses during installation, and later you want to remove the device, you must follow a two-step process.

NOTE: Completing these steps ensures that the device is not discovered and managed again by the provider when the CIMOM is restarted.

1. The SMI-enabled client must use the SMI-S Provider Proxy Server System Management profile to remove the device.
2. Depending on your operating system, go to one of the following files, and remove the device's IP address.

   - **For a Windows operating system,** the filename is `<Provider install dir>\pegasus\provider\array\ArrayHosts.txt`.
   - **For a UNIX-based operating system,** the filename is `<Provider install dir>/pegasus/providers/array/ArrayHosts.txt`.

Setting a Device Password

You can set a device password so that only authorized users can make configuration changes. Keep the following two conditions in mind about device passwords:

- **When you add a device to manage –** Use **modifyInstance** to set the Secret property of the **DefaultSharedSecret instance** to the device's password. Add the device using the **AddSystem** extrinsic method.
- **When the device is already added without setting the device password in DefaultSharedSecret, and the device has password set –** Set the Secret property to the device's password in the **SharedSecret** instance associated with the added device to prevent authentication failure errors during configuration change operations. In case of authentication failure, the error return value of all methods is `4`.

NOTE: For additional information about issues with device passwords, refer to Troubleshooting and locate the issue "The storage array password is missing."

The Secret property in the **DefaultSharedSecret** instance retains the last set value. To add another device with a different password (or no password) subsequently, modify the Secret property of **DefaultSharedSecret** instance with the new value before adding the device. Otherwise, any configuration change operation on the device would fail with return value `4`. To resolve this error, use **modifyInstance** to set the Secret property of the **SharedSecret instance** to the device's password.

If all devices have the same password, set the Secret property of **DefaultSharedSecret instance** to the device password only one time and all subsequent **AddSystem** operations set the device password correctly.

Configuring the SMI-S Provider

This section describes the configuration options that are available.

1. To make changes to any configuration option, go to the directory where SMI-S Provider is stored.

   - For a Windows operating system, the directory is `<install dir>\netapp\pegasus\provider\array`.

2. Edit the providerTraceLog.properties file in a text file editor such as Notepad or vi.
3. Save the file, and exit the text editor.

4. Stop and start the OpenPegasus CIM server by using the specific location and name. See Starting and Stopping the OpenPegasus CIM Server.

Debug Tracing

CAUTION Any change to the tracing level requires that you stop and start SMI-S Provider for the changes to take effect. Turn on tracing only under the direction of technical support.

1. Remove the pound sign (#) from the lines containing FILE and EVENTS. You can edit the file name and directory as you want.
2. You can either change or disable the default trace level (DEBUG).

   - To change the default trace level (DEBUG), set the value of LEVEL to one of the allowed values.
   - To disable the default trace level (DEBUG), add the pound sign (#) before LEVEL.

EVENTS

This option is not used in the implementation and does not have any impact on the provider.

TIMECOUNTERSUPPORTED

This option allows you to configure the timer counter properties reporting in Block Server Performance subprofile. When set to FALSE, the timer counter properties, **IOTimeCounter, ReadIOTimeCounter, and WriteIOTimeCounter** are not reported in the Block Server Performance reporting. When set to TRUE, the time counter properties are reported in the Block Server Performance reporting.

PERSISTDEFAULTSS

This option allows you to configure the persistence of **DefaultSharedSecret** instance across provider restarts. The **DefaultSharedSecret** instance holds the default password used when adding a device. When a device has a non-default password set, the client modifies the Secret in **DefaultSharedSecret** to the device's password, and then adds the device for management.

When set to TRUE, the **DefaultSharedSecret** instance is persisted during provider shutdown. On subsequent restart, the persisted **DefaultSharedSecret** is loaded back. This option is helpful when a client needs to add and manage devices that have the same password/credential across provider restarts.

When set to FALSE, the **DefaultSharedSecret** instance is not persisted across provider restarts.

JOB_POLLING_FREQUENCY

This option allows you to configure the **CIM_ConcreteJob** instance update/refresh frequency in minutes. The default value is 5 minutes, and the valid value range for this option is 1 to 10 minutes.

ENABLE_SSD_CACHE

This option allows you to configure whether SSD-based cache is enabled for the newly created volumes and snapshots. You can create SSD cache using either SANtricity Storage Manager or the SMI-S method CreateFlashCache defined in NetApp FlashCacheconfigurationService class. This setting is invalid if the SSD cache does not already exist. If the default value is set to FALSE, SSD-based caching is not available for the newly created volumes or snapshots. If the default value is set to TRUE, SSD-based caching is available for the newly created volumes or snapshots.

SNAPSHOT_IMAGE_GROUP_REPOS_FULL_POLICY

This option allows you to configure how you want snapshot image processing to continue if the repository volumes for the snapshot image group (NetApp_PiTGroup) are full. The valid values are PURGE and FAILWRITES. The default value is PURGE. When set to PURGE, the oldest snapshot image (PiT) in the snapshot image group is purged to free space when the repository is full. When set to FAILWRITES, write operations to base volumes of the snapshot image group are failed.

SNAPSHOT_IMAGE_GROUP_REPOS_SIZE

This option allows you to configure the snapshot image group (NetApp_PiTGroup) repository size as percentage of base volume. The minimum default value is 40 percent. The maximum value is controlled by the storage array default attribute settings. Any value for this option that exceeds the default maximum value is reset to the maximum value supported by the storage array.

SNAPSHOT_REPOS_SIZE

This option allows you to configure the snapshot volume (NetApp_PiTView) repository size as percentage of base volume. The minimum default value is 40 percent. The maximum value is controlled by the default attribute settings of the storage array. Any value for this option that exceeds the default maximum value is reset to the maximum value supported by the storage array.

AUTO_DELETE_HOST

This option allows you to configure whether or not a host/cluster that is auto created by Provider during LUN masking and mapping operations is automatically deleted during HidePaths and DeleteStorageHardwareID extrinsic method invocations. The auto-created host/cluster is recognized based on the host name format used by SMI-S Provider. The valid values are TRUE and FALSE. The default value is set to TRUE. When set to TRUE, the auto-created host is deleted when the last initiator ID is removed from the host, and the auto-created cluster is deleted when the last host in the cluster is deleted. When set to FALSE, the auto created host/cluster is retained without deletion during HidePaths and DeleteStorageHardwareID.

SUPPORT_BUNDLE_LOCATION

You can configure the directory path to save the device support bundle collected using the **CaptureSupportBundle** extrinsic method in **NetApp_StorageSystem** class.

Array Management Utility

This chapter describes how to use the following functions of the Array Management Utility:

- Adding a storage array
- Removing a storage array
- Adding and removing In-Band management hosts
- Get repository sizes of snapshot volumes and snapshot image groups
- Expand repositories of snapshot volumes and snapshot image groups
- Configuring the Array Properties

Using the Array Management Utility (ArrayMgmtUtil)

The `ArrayMgmtUtil` is included in the provider package. This utility allows you to add and remove storage arrays to the SMI-S Provider while the system is online. The adding and removing of In-Band

management hosts is supported through the `ArrayMgmtUtil`. The utility also allows you to expand the repositories of snapshot volumes that you created using Replication Service profile.

As you install SMI-S Provider, the command line user interface for `ArrayMgmtUtil` installs at one of the following locations:

- **Windows –** `<install dir>\netapp\pegasus\bin`

Adding a Storage Array

Use the following command to add a storage array to the provider for out-of-band management by entering the network address for that storage array. Adding a storage array through out-of-band management differs from the in-band management process, which adds all storage arrays with an in-band connection to a host. For more information on how to add storage arrays through in-band management, refer to Adding an In-Band Management Host.

NOTE: Any CIM client can be used to add storage arrays to the proxy system with methods in the Proxy Server profile.

If the storage array has a password, which is needed to authorize configuration change operations, enter the password in the optional `-ArrayPass` parameter. When you enter the storage array password, the utility adds the storage array and sets the storage array password.

```
ArrayMgmtUtil -AddArray [-l <CIMOM Host IP:CIMOM Port>] -n <CIM Array
Namespace> [-s [--cert <SSL Certificate Path> --key <SSL Key Path>]] [-u <CIMOM
User> -p <User password>] -ArrayIP <Array IP Address> [-ArrayPass <Array
Password>]
```

Examples:
To add a storage array without a password:

```
ArrayMgmtUtil -AddArray -l 10.85.34.23:5988 -n root/netapp/santricity -ArrayIP
10.85.34.135
```

To add a storage array with a password:

```
ArrayMgmtUtil -AddArray -l 10.85.34.23:5988 -n root/netapp/santricity -ArrayIP
10.85.34.135 -ArrayPass password
```

To add a storage array securely without a password:

```
ArrayMgmtUtil -AddArray -l 10.85.34.23:5989 -s --cert "c:\my cert\client.pem" -
-key "c:\my cert\clientkey" -n root/lsiarray13 -ArrayIP 10.85.34.135
```

To add a storage array when the CIMOM user authentication is enabled:

```
ArrayMgmtUtil -AddArray -l 10.85.34.23:5988 -n root/netapp/santricity -u Admin
-p password -ArrayIP 10.85.34.135
```

NOTE: You can also add a storage array during installation on a Windows operating system when prompted to enter the IP address in the `ArrayHosts.txt` file. Adding storage arrays through the `ArrayHosts.txt` file is

deprecated and on-going use will eventually be discontinued. If a storage array is added without setting a password, refer to Setting a Device Password to set the password after adding the storage array.

Removing a Storage Array

Use this command to stop managing and to remove a storage array from the provider by entering the network address or the WWN (World Wide Identifier Name) for that storage array.

```
ArrayMgmtUtil -RemoveArray [-l <CIMOM Host IP:CIMOM Port>] -n <CIM Array
Namespace> [-s [--cert <SSL Certificate Path> --key <SSL Key Path>]] [-u <CIMOM
User> -p <User password>] {-ArrayIP <Array IP Address> | -ArrayWWN <Array WWN>}
```

Examples:
To remove a storage array using its IP address:

```
ArrayMgmtUtil -RemoveArray -l 10.85.34.23:5988 -n root/netapp/santricity -ArrayIP
10.85.34.135
```

To remove a storage array using its WWN:

```
ArrayMgmtUtil -RemoveArray -l 10.85.34.23:5988 -n root/netapp/santricity -ArrayWWN
60080E50002904680000000050233008
```

NOTE: If you have entered the IP address of the removed storage array into a file during installation, go to Step 2 under Removing a Device to ensure that the storage array is not rediscovered when you restart CIMOM or provider.

Adding an In-Band Management Host

When an in-band connection is added to the provider, it adds the connections for *all* storage arrays with an in-band connection to the identified host. To add an in-band host, you specify the host through the `-HostIP` parameter through the following command:

```
ArrayMgmtUtil.exe -AddHost -1 1XX.0.0.1:5988 -n root/netapp/santricity -HostIP
1X.1XX.XX.XXX
```

NOTE: Password-protected hosts are not accepted through the Add Host command.

Removing an In-Band Management Host

When an in-band connection is removed from the provider, it removes the connections for *all* storage arrays with an in-band connection to the identified host. To remove an in-band host, you must specify the host through the `-HostIP` parameter through the following command:

```
ArrayMgmtUtil.exe -RemoveHost -1 1XX.0.0.1:5988 -n root/netapp/santricity -
HostIP 1X.1XX.XX.XXX
```

Get Repository Size of Snapshot Volume

Use this command to get the current size of the repository of a snapshot volume, which you created using Replication Services Profile.

```
ArrayMgmtUtil -GetSnapshotReposSize [-l <CIMOM Host IP:CIMOM Port>] -n <CIM
Array Namespace> [-s [--cert <SSL Certificate Path> --key <SSL Key Path>]] [-u
<CIMOM User> -p <User password>] -SnapshotID <Snapshot WWN>
```

To get the repository size of a snapshot volume from a CIMOM in the localhost:

```
ArrayMgmtUtil -GetSnapshotReposSize -n root/netapp/santricity - SnapshotID
6008FA50002904680000000005023300D
```

Expand Repository of Snapshot Volume

Use this command to expand the size of the repository of a snapshot volume, which you created using Replication Services Profile. The value for `-NewSize` is the desired total size of the repository after expansion.

```
ArrayMgmtUtil -SetSnapshotReposSize [-l <CIMOM Host IP:CIMOM Port>] -n <CIM
Array Namespace> [-s [--cert <SSL Certificate Path> --key <SSL Key Path>]] [-u
<CIMOM User> -p <User password>] -SnapshotID <Snapshot WWN> -NewSize
<SizeInBytes>
```

To expand the repository size of a snapshot volume from a CIMOM in the localhost:

```
ArrayMgmtUtil -GetSnapshotReposSize -n root/netapp/santricity - SnapshotID
6008FA50002904680000000005023300D -NewSize 10737418240
```

Get Repository Size of Snapshot Image Group

Use this command to get the current size of the repository of a snapshot image group, which you created using Replication Services Profile.

```
ArrayMgmtUtil -GetSnapshotGroupReposSize [-l <CIMOM Host IP:CIMOM Port>] -n
<CIM Array Namespace> [-s [--cert <SSL Certificate Path> --key <SSL Key Path>]]
[-u <CIMOM User> -p <User password>] -SnapshotID <Snapshot WWN>
```

To get the repository size of a snapshot image group:

```
ArrayMgmtUtil -GetSnapshotGroupReposSize -l 11.40.67.23:5988 -n
root/netapp/santricity -SnapshotID 6008FA50002904680000000005023300D
```

Expand Repository of Snapshot Image Group

Use this command to expand the size of the repository of a snapshot image group, which you created using Replication Services Profile. The value for `-NewSize` is the desired total size of the repository after expansion.

```
ArrayMgmtUtil -SetSnapshotGroupReposSize [-l <CIMOM Host IP:CIMOM Port>] -n
<CIM Array Namespace> [-s [--cert <SSL Certificate Path> --key <SSL Key Path>]]
[-u <CIMOM User> -p <User password>] -SnapshotID <Snapshot WWN> -NewSize
<SizeInBytes>
```

To expand the repository size of a snapshot image group:

```
ArrayMgmtUtil -SetSnapshotReposSize -l 11.40.67.23:5988 -n
root/netapp/santricity -SnapshotID 6008FA50002904680000000005023300D - NewSize
10737418240
```

Interactive Mode

When a utility is invoked without any parameters, it runs in interactive mode. The following options are available in interactive mode:

```
1. Add Array
2. Add Host
3. Remove Array
4. Remove Host
5. Get Snapshot Volume Repository Size
6. Set Snapshot Volume Repository Size
7. Get Snapshot Group Repository Size
8. Set Snapshot Group Repository Size
9. Exit
```

Asynchronous Remote Volume Mirroring

Asynchronous Mirroring provides a controller-level, firmware-based mechanism for data replication between a local site and a remote site. Replication is managed on a per-volume basis, allowing a storage administrator to associate a distinct remote mirrored volume with every primary volume on a given storage array. For Asynchronous Mirroring, the local storage array and the remote storage array can run different versions of firmware. The minimum firmware version supported is SANtricity firmware version 7.84.

Asynchronous mirror groups allow you to manage the synchronization process as a set to create a crash-consistent data-set on the remote storage array. Point-in-time images are used on the primary volume and the secondary volume to batch the resynchronization process. A data repository volume is required for each mirrored volume.

Note: When creating a mirrored pair with FIPS drives, ensure that the mirrored pair has the same level of security capabilities. For example, FDE drives provide security, but do not contain the same security level as FIPS drives.

The SMI-S Provider provides volume-to-volume support and allows for the creation of new volumes on both primary and remote arrays prior to establishing the asynchronous link. The SMI-S provider establishes the asynchronous link by adding the primary volume to the mirror group on the primary array and complete link on the remote array in a single step.

The following classes and associations are used for ARVM support through the SMI-S Provider:

Classes and Associations:

- **NetApp_AsyncMirrorGroup** – A class that must be created for every AsyncMirrorGroup on each array. An association of NetApp_AsyncMirrorGroup is returned for each pair of NetAppAsyncMirrorGroup created between arrays.
- **NetApp_AsyncMirrorPair** – An association class for relationships between two volumes that exist on separate storage systems.
- **NetApp_RemoteReplicationCollection** – A class that models a remote storage system.
- **NetApp_AMGStorageSetting** – A class that describes settings for each asynchronous mirror group.

- **NetApp_AsyncMirrorGroupMembers** – An association between the two volumes on each array that are AsyncMirrorGroupMembers of the AsyncMirrorGroup.
- **NetApp_AsyncMemberGroupMemberOfGroup** – An association linking a volume that is a member of an AMG to its parent AMG. There is one association per array generated for each volume that is an Async Mirror Group Member of an AsyncMirrorGroup.
- **NetApp_GroupSynchronized** – An association between a local and remote storage volume. Created when a mirror pair is created.

Handling of Remote Systems

The NETAPP_RemoteReplicationCollection class models a remote storage system. This class requires the remote storage array to be managed by the same CIMOM as the local storage array.

Property Name	Description
InstanceID	AMGMemberLocal.WWN + "_" + AMGMemberRemote.WWN

There are two returned for every pair of storage systems that have a common Asynchronous Mirror Group member between them. The storage arrays have to be known by the CIMOM to exist. That is, if a storage system has a mirror to another storage system, but that other storage system is not in the CIMOM, nothing is returned for that pair. There is a pair returned for each storage system pair, because each storage system has the perspective where it is the local array, and the other one is the remote.

Handling AMG Settings (Synch periodicity, etc.)

When managing or creating in a NETAPP_AsyncMirrorGroup, you can manage whether to resume synchronization, suspend synchronization, or swap primary/secondary roles. You can do this by passing in an "Operation" parameter. This parameter is an integer and here is how it maps to actual roles:

- 16 – Resume Synchronization
- 20 – Reverse Roles
- 22 – Suspend Synchronization

Job Requirements

A job is created for when you want to synchronize mirror groups across arrays, as it can take a long time to complete.

When you call ModifyListSynchronization on the ReplicationService with the "Operation" argument being set to "ResyncReplica", a call to the array for the specified AsyncMirrorGroupSynchronized instance is made to resynchronize the mirrors. When this method returns, the output parameter "Job" is filled in with a reference to the created job. You can then monitor the status of the job by grabbing the instance of the job from the provider and status.

Creating Asynchronous Mirror Groups

NOTE: Due to its inclusion in the distribution and the client applications ability to follow the workflow, CIMCLI is used within the workflow examples throughout this document.

Asynchronous Mirror Groups (AMG) are created through the CreateGroup command on a Replication Service for a specific array. Perform the following to obtain and pass the required parameters needed to create an AMG through the CreateGroup command:

1. Enter the following command to obtain the Replication Service for the array you want to create an asynchronous mirror group on:

   ```
   cimcli ei -n root/netapp/santricity NETAPP_ReplicationService
   ```

   Paths for the Replication Service on the array is displayed.
   NOTE: The provider will assume the “local” array to be associated with the instance of the replication service.
2. Locate and copy the path for the desired Replication Service path.
   NOTE: When copying the path, exclude the “// path=” content.

   Example of copied path:
   ```
   NETAPP_ReplicationService.CreationClassName=\”NETAPP_ReplicationService\
   ”,Name=\”ReplicationService\”SystemCreationClassName=\”NETAPP_StorageSystem\
   ”,SystemName=\60080E5000298A1C000000005613DD29\”
   ```

3. Enter the following command to obtain the Service Access Point path for the array you want to connect with:

   ```
   cimcli ei -n root/netapp/santricity NETAPP_RemoteServiceAccessPoint
   ```

4. Locate and copy the path for the desired Service Access Point path.
   NOTE: When copying the path, exclude the “// path=” content.

   Example of copied path:
   ```
   NETAPP_RemoteServiceAccessPoint.CreationClassName=\”NETAPP_RemoteServiceAcce
   ssPoint\”,Name=\”RemoteAccessPoint_1\”,SystemCreationClassName=\”NETAPP_Stor
   ageSystem\”,SystemName=\”60080E5000341B0500000000560F401F
   ```

5. Enter the copied Replication Service and Service Access Point paths in the following CreateGroup command to create an asynchronous mirror group:

   ```
   cimcli im -n root/netapp/santricity {ReplicationService} CreateGroup
   GroupName={grp name} ServiceAccessPoint={SAP Path}
   ```

   Example of CreateGroup command:
   ```
   cimcli im -n root/netapp/santricity
   NETAPP_ReplicationService.CreationClassName=\"NETAPP_ReplicationService\",Na
   me=\"ReplicationService\",SystemCreationClassName=\"NETAPP_StorageSystem\",S
   ystemName=\"60080E5000298A1C000000005613DD29\" CreateGroup
   GroupName="JDOE_AMG_3"
   ServiceAccessPoint=NETAPP_RemoteServiceAccessPoint.CreationClassName=\"NETAP
   P_RemoteServiceAccessPoint\",Name=\"RemoteAccessPoint_1\",SystemCreationClas
   sName=\"NETAPP_StorageSystem\",SystemName=\"60080E5000341B0500000000560F401F
   \"
   ```

Creating a Mirror

To create a mirror, you need to call the `CreateListReplica` command on a `ReplicationService` and pass in the following seven parameters:

- **SyncType** – Must be set to 6 (MIRROR)

- **Mode** – Must be set to 3 (ASYNCHRONOUS)
- **SourceElements** – An array of volumes. The array must contain exactly 1 volume that exists on the primary array.
- **SourceAccessPoint** – The path to the ReplicationService for the primary array.
- **TargetElements** – An array of volumes, the array must contain exactly 1 volume that exits on the secondary array.
- **TargetAccessPoint** – The path to the ReplicationService for the secondary array.
- **TargetSettingGoal** – The path to the NETAPP_AMGStorageSetting that corresponds to the AMG.

6. Through a Pegasus CLI client, enter the following command to obtain the Replication Service for the array on which you want to create a mirror:

   ```
   cimcli ei –n root/netapp/santricity NETAPP_ReplicationService
   ```

   Paths for the Replication Service on the array is displayed.

7. Locate and copy the path for the desired Replication Service path.
   NOTE: When copying the path, exclude the "// path=" content.

   Example of copied path:
   ```
   NETAPP_ReplicationService.CreationClassName=\"NETAPP_ReplicationService\
   ",Name=\"ReplicationService\"SystemCreationClassName=\"NETAPP_StorageSystem\
   ",SystemName=\60080E5000298A1C000000005613DD29\"
   ```

8. Enter the following command to obtain the Service Access Point and TargetAccessPoint path for the arrays the AMG connects with:

   ```
   cimcli ei –n root/netapp/santricity NETAPP_RemoteServiceAccessPoint
   ```

9. Locate and copy the path for the desired Service Access Point path.
   NOTE: When copying the path, exclude the "// path=" content.

   Example of copied path:
   ```
   NETAPP_RemoteServiceAccessPoint.CreationClassName=\"NETAPP_RemoteServiceAcce
   ssPoint\",Name=\"RemoteAccessPoint_1\",SystemCreationClassName=\"NETAPP_Stor
   ageSystem\",SystemName=\"60080E5000341B0500000000560F401F
   ```

10. To pass the SourceElement and Target Element into the createMirror call as arrays of volumes, enter the following command to obtain the source and target volumes:

    ```
    cimcli ni –n root/netapp/santricity NETAPP_StorageVolume
    ```

    Paths for the volumes are displayed.

11. Locate and copy the path for the desired source and target volumes.
    NOTE: When copying the path, exclude the "// path=" content.

    Example of copied path:
    ```
    NETAPP_StorageVolume.CreationClassName="NETAPP_StorageVolume",DeviceID="6008
    0E5000341F610000D12E56C49D8F",SystemCreationClassName="NETAPP_StorageSystem"
    ,SystemName="60080E5000341F610000000056A74E0D"
    ```

12. To correlate your volume and volume label, enter the following command to run gi and select the WWN.

    ```
    cimcli gi -n root/netapp/santricity NETAPP_StorageVolume
    ```

    All volume attributes for the selected volume is displayed in the gi.
13. Enter the following command to obtain the Asynchronous Mirror Group to add to the mirror:

    ```
    cimcli ei -n root/netapp/santricity NETAPP_AMGStorageSetting -niq
    ```

    Paths for the Asynchronous Mirror Group is displayed.
14. Locate and copy the path for the Asynchronous Mirror Group.
    NOTE: When copying the path, exclude the "// path=" content.

    Example of copied path:
    ```
    NETAPP_AsyncMirrorGroup.CreationClassName=\"NETAPP_AsyncMirrorGroup\",Device
    ID=\"3700000060080E5000341F610000D12456C3CE05\",InstanceID=\"60080E5000341F6
    10000000056A74E0D_60080E5000341F610000D12456C3CE05\",SystemCreationClassName
    =\"NETAPP_StorageSystem\",SystemName=\"60080E5000341F610000000056A74E0D\"
    ```

15. Enter the following command to create an Asynchronous Mirror Group:

    ```
    cimcli im -n root/netapp/santricity {ReplicationService} CreateListReplica
    SyncType=6 Mode=3 SourceElements=[{source volume path}]
    SourceAccessPoint={SAP Path} TargetElements=[{target volume path}]
    TargetAccessPoint={SAP Path} TargetSettingGoal={amg storage setting path}
    ```

    NOTE: Because the SourceElements and TargetElements are arrays, you must enclose each path with square brackets (i.e., [and]).

Deleting Asynchronous Mirror Group

If needed, perform the following to delete Asynchronous Mirror Groups from the CIMOM:

1. On the ReplicationServices class, invoke the `deletegroup` method.
2. Pass in the CIM object name of the NETAPP_AsyncMirrorGroup that you want to remove as the ReplicationGroup parameter.
   If there are AsyncMirrorPair members in the group, those mirror pairs will be deleted (but not their underlying volumes).

Troubleshooting

SMI-S Issues and Resolutions

Issue	Resolution

On a new installation on a system that did not previously have SMI-S Provider installed, this message appears:
`cimserver not started: Bind failed: Failed to bind socket on port 5989: Address already in use (error code 125)`
	This issue occurs when there is a port conflict. Resolve the conflict either by removing the application that is using the port or by selecting a different port. Run the following commands to select a different port.
	Stop the CIM server.
	`cimserver -s`
	Set the new ports.
	`cimconfig -s httpPort=<HTTP PORT> -p`
	`cimconfig -s httpsPort=<HTTPS PORT> -p`
	Start the CIM server.
	`cimserver`

CIMOM default port in use is not reported on Windows operating systems.	On Windows operating systems, if the default ports 5988 and 5989 are already in use during provider installation, no message is displayed to state that the ports are in use. If a conflict occurs, you should edit the cimserver_current.conf and cimserver_planned.conf files, specify the open ports and then start the cimserver.
SLP SA's (Service Location Protocol Service Agents) in environments with an existing SLP SA.	Because SA's require a fixed port of 427, only one SLP SAP for each individual server can be active.

Issue	Resolution

On a system where the Java provider was previously installed, this message appears:
`cimserver not started:-Bind failed: Failed to bind socket on port 5989: Address already in use (error code 125)`
	This issue occurs when there is a port conflict. In most cases, a file was preserved during the removal of the Java provider that contains the port information from the previous installation. Look at the contents of the `portInfo.properties` file to determine the previous value.
	Use the following commands to change to the previously used port.
	Stop the CIM server.
	`cimserver -s`
	Set the new ports.
	`cimconfig -s httpPort=<HTTP PORT> -p`
	`cimconfig -s httpsPort=<HTTPS PORT> -p`
	Start the CIM server.
	`cimserver`

The storage array password is missing.	During installation, you would not run into any issues with the storage array password because the SMI-S Provider does not yet have information about the storage arrays to manage. However, after you add the storage arrays, a Return Code - 4 message appears for any method that runs. A specific error message does not appear other than the return value, but the provider trace log shows that the method failed because of an authentication failure. Update the value for the Property - Secret with the current storage array password in the LSISSI_SharedSecret instance by using Modify instance CIM operation. After you have updated the file, run the following command: `wbemexec -h host ip of provider -p 5988 -u user id -w password Set_Password.xml` For more information about passwords, see Setting a Device Password.
This message appears when you use the CIM CLI application: `roundTripTime is incorrect in ClientOpPerformanceData`	You can ignore this message when using the CIM command line interface.

Issue	Resolution

On a new installation on a system that did not previously have SMI-S Provider installed, this message appears:
`cimserver not started: Bind failed: Failed to bind socket on port 5989: Address already in use (error code 125)`
	This issue occurs when there is a port conflict. Resolve the conflict either by removing the application that is using the port or by selecting a different port. Run the following commands to select a different port.
	Stop the CIM server.
	`cimserver -s`
	Set the new ports.
	`cimconfig -s httpPort=<HTTP PORT> -p`
	`cimconfig -s httpsPort=<HTTPS PORT> -p`
	Start the CIM server.
	`cimserver`

CIMOM default port in use is not reported on Windows operating systems.	On Windows operating systems, if the default ports 5988 and 5989 are already in use during provider installation, no message is displayed to state that the ports are in use. If a conflict occurs, you should edit the cimserver_current.conf and cimserver_planned.conf files and specify the open ports and then start the cimserver.
SLP SAs (Service Location Protocol Service Agents) in environments with an existing SLP SA.	Because SA's require a fixed port of 427, only one SLP Sap for each individual server can be active.

Unsupported SMAPI Properties and Methods

Some of the properties and methods in the Microsoft Storage Management API classes are not supported by E-Series SMI-S Provider. These properties and methods are not supported either because of unavailability of corresponding capabilities or because they are not relevant to SMI-S providers. Some properties or methods might belong to Storage Spaces. The properties and methods that are not supported are listed in the following tables:

Unsupported SMAPI Properties

SMAPI Class	SMAPI Properties
MSFT_StorageProvider	URI_IP
MSFT_StoragePool	ClearOnDeallocate EnclosureAwareDefault IsClustered IsPowerProtected IsReadOnly LogicalSectorSize OtherOperationalStatusDescription PhysicalSectorSize ReadOnlyReason SupportsDeduplication RetireMissingPhysicalDisks
MSFT_StorageSubSystem	DataTieringType Description NumberOfSlots
MSFT_ResiliencySetting	Description
MSFT_VirtualDisk	DetachedReason FootprintOnPool IsDeduplicationEnabled IsEnclosureAware IsManualAttach NumberOfAvailableCopies OtherUsageDescription ResiliencySettingName
MSFT_PhysicalDisk	SupportedUsage Usage EnclosureNumber SlotNumber IsPartial PartNumber
MSFT_OffloadDataTransferSetting	All Properties

Unsupported SMAPI Methods

SMAPI Class	SMAPI Methods	Powershell cmdlets not supported (Corresponding to the SMAPI Methods)
MSFT_StorageSubSystem	SetDescription()	Set-StorageSubsystem
MSFT_StoragePool	RemovePhysicalDisk() SetAttributes() SetDefaults() SetUsage()	Remove-PhysicalDisk Set-StoragePool for the following options only ClearOnDeallocate, EnclosureAwareDefault FriendlyName IsPowerProtected IsReadOnly OtherUsageDescription ProvisioningTypeDefault ResiliencySettingNameDefault RetireMissingPhysicalDisks Usage Remaining options in Set-StoragePool should be supported

SMAPI Class	SMAPI Methods	Powershell cmdlets not supported (Corresponding to the SMAPI Methods)
MSFT_VirtualDisk	Attach() Detach() RemovePhysicalDisk() Repair() SetAttributes() SetUsage()	Connect-VirtualDisk Disconnect-VirtualDisk Repair-VirtualDisk Set-VirtualDisk
MSFT_PhysicalDisk	Maintenance() SetDescription() SetUsage() Reset() SetFriendlyName()	Enable-PhysicalDiskIndication Disable-PhysicalDiskIndication Set-PhysicalDisk Reset-PhysicalDisk
MSFT_MaskingSet	AddTargetPort() RemoveTargetPort()	Add-TargetPortToMaskingSet Remove-TargetPortFromMaskingSet

Trademark information

Copyright information

Machine translation

See important information about localized content at netapp.com.
https://www.netapp.com/company/legal/machine-translation

How to send your comments

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. 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., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277


NetApp