McData 4Gb SAN Switch for HP p-Class Blade Systems SMI-S Provider for HP Systems Insight Manager

About this document

HP Systems Insight Manager (HP SIM) uses CIM/WBEM servers and providers that conform to the Storage Management Initiative Specification (SMI-S). Before HP SIM can manage and report on a storage host, the appropriate SMI-S provider must be installed and configured.

About the SMI-S provider

- The SMI-S provider (also referred to as *SMI-Agent*, *CIMAgent*, *cim_server*, or *CIM*) includes a Pegasus-based CIMOM and corresponding providers.

- The SMI-S provider is embedded in the switch firmware.

- The SMI-S provider is delivered with switch firmware version 5.2.0.29 and later.

Models supported

This SMI-S provider enables HP SIM support for the following switch:

- McDATA 4Gb SAN Switch for HP p-Class BladeSystems

Requirements

The following requirements must be met in order for HP SIM to support the McDATA 4Gb SAN Switch for HP p-Class BladeSystems:

- HP SIM 5.0 or later must be installed on the central management server (CMS).

- HP recommends firmware version 5.2.2.15 or later.

Setting up the SMI-S provider

This section contains instructions for installing and setting up the SMI-S provider. Connection and discovery information required by HP SIM is described in the next section.

You can set up the SMI-S provider with a graphical user interface (GUI) or in a Telnet session.

Setting up the SMI-S provider

1. Verify that the switch has an Ethernet connection to the LAN, and that you can ping it.

2. Open a web browser and enter the switch address (for example, http://15.16.17.18). The Initial Start Dialog – Switch Manager window appears.

Figure 1 Switch Manager Initial Start Dialog

3. Select **Open existing fabric** and click **Proceed**. The Add a
New Fabric window appears.

Figure 2 Add a New Fabric window

4. Enter the switch IP address, login name, and password, and
then click **Add Fabric**.

5. If you are prompted to establish a non-secure connection and
want to continue, click **Yes**.

6. You should now be able to navigate in the Switch Manager
window. In the Switch tree view on the left, click the key icon to
expand the fabric and reveal the switch. Click the switch name
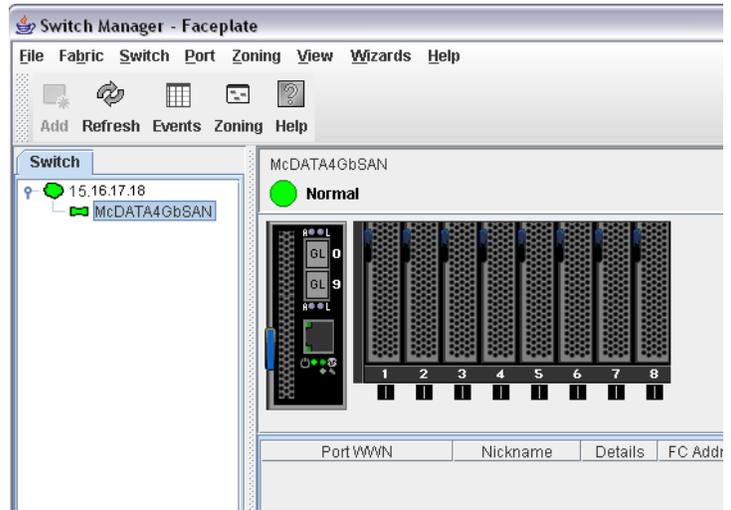to select it.

Figure 3 Switch Manager window

7. Select **Switch > Services**

8. Verify that the SMI-S provider (listed as **CIM**) is enabled.
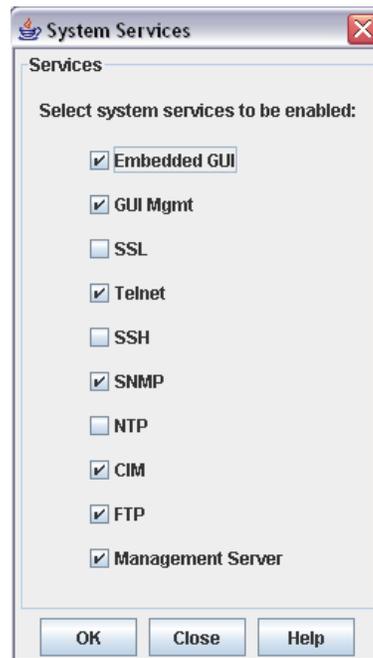
Figure 4 System Services window

2

9. By default, the SMI-S provider communicates over a non-secure http connection on port 5988. If you want the SMI-S provider to use an encrypted connection (https over port 5989), ensure that **SSL** is also enabled.

> **NOTE**:
> If SSL is enabled, the SMI-S provider will not respond to non-secure requests (http on port 5988).

10. Click **OK**, and then close the Switch Manager application. The SMI-S provider is now enabled and should be running.

11. Verify that the SMI-S provider is running:

    a. Telnet into the switch. You will need the current administrator user name and password. The default values are `admin` and `password`.

    b. Enter `ps` at the command prompt to list the currently running processes. If the SMI-S provider is running `cim_server` is listed.

12. Use an SMI-S or SLP test tool to verify that the SMI-S provider is responding.

13. Repeat this procedure for each switch in the fabric.

SMI-S Provider: Telnet setup

1. Verify that the switch has an Ethernet connection to the LAN, and that you can ping it.

2. Telnet into the switch. You will need the current administrator user name and password. The default values are `admin` and `password`.

3. Verify that the SMI-S provider is enabled:

    a. At the command prompt, enter `show setup services`. If the SMI-S provider is enabled, `CIMEnabled` appears in the list with a value of `true`.

    b. Enter `ps` at the command prompt to list the currently running processes. If the SMI-S provider is running `cim_server` is listed.

    If the SMI-S provider is not running (CIMEnabled = false or cim_server is not in the process list), enable the service (step 4). If the SMI-S provider is running, skip to step 5.

4. If the SMI-S provider is not enabled/running:

    a. Enter the following commands at the command prompt:

    McDATA4GbSAN: admin> **admin begin**
    McDATA4GbSAN (admin) : admin > **set setup services**

    b. Press Enter after each attribute line to accept the current value, until you reach the CIMEnabled attribute.

TelnetEnabled	(True / False)	[True]

SSHEnabled	(True / False)	[False]
GUIMgmtEnabled	(True / False)	[True]
SSLEnabled	(True / False)	[False]
EmbeddedGUIEnabled	(True / False)	[True]
SNMPEnabled	(True / False)	[True]
NTPEnabled	(True / False)	[False]
CIMEnabled	(True / False)	[False] True
FTPEnabled	(True / False)	[True]
MgmtServerEnabled	(True / False)	[True]

    c. Enter `True` on the `CIMEnabled` line, and press **Enter** to keep the current values for the other entries.

> **NOTE**:
> To terminate this process before reaching the end of the list, type **q** or **Q** and press **Enter**.

    d. When the `Do you want to save and activate this services setup?  (y/n):   [n]` prompt appears, type y and press **Enter**.

    The following message appears:

```
Services setup saved and activated.

McDATA4GbSAN:  admin>

Log Msg: [22] [Tue Mar 03 00:11:38.727 UTC 1970]
[C] [8400.004C] [Switch] [Services setup is
changing – may lose connection – admin being
released automatically]

McDATA4GbSAN : admin>
```

    - Further configuration might be required after you enable a service
    - If you disable a service, the connection to the switch may be lost

    e. Repeat step 3 to verify that the SMI-S provider is enabled.

5. If the switch supports SSL, and you want to use an encrypted connection rather than a non-secure connection (the default), enable SSL as described below.

    a. Verify that the date and time settings on the switch and the workstation from which the SSL connection will be started match. A new certificate may need to be created to ensure a secure connection to the switch.

    b. Enter the following commands at the command prompt:

    McDATA4GbSAN: admin> **admin begin**
    McDATA4GbSAN (admin) : admin> **set setup services**

    c. Press **Enter** after each attribute line to accept the current value, until you reach the SSLEnabled attribute.

TelnetEnabled	(True / False)	[True]
SSHEnabled	(True / False)	[False]
GUIMgmtEnabled	(True / False)	[True]
SSLEnabled	(True / False)	[False] True
EmbeddedGUIEnabled	(True / False)	[True]
SNMPEnabled	(True / False)	[True]

NTPEnabled	(True / False)	[False]
CIMEnabled	(True / False)	[False]
FTPEnabled	(True / False)	[True]
MgmtServerEnabled	(True / False)	[True]

d. Enter `True` on the SSLEnabled line, and press **Enter** to keep the current values for the other entries.

> **NOTE**:
> To terminate this process before reaching the end of the list, type **q** or **Q** and press **Enter**.

e. When the `Do you want to save and activate this services setup?  (y/n):  [n]` prompt appears, type `y` and press **Enter**.

The following message appears:

```
Services setup saved and activated.

McDATA4GbSAN:  admin>

Log Msg: [23] [Tue Mar 03 00:11:38.727 UTC 1970]
[C] [8400.004C] [Switch] [Services setup is
changing — may lose connection — admin being
released automatically]

McDATA4GbSAN : admin>
```

- Further configuration might be required after you enable a service
- If you disable a service, the connection to the switch may be lost

f. Enter the `show setup services` command to verify that `SSLEnabled` is now set to True.

6. Use an SMI-S or SLP test tool to verify that the SMI-S provider is responding.

7. Repeat these steps for each switch in the fabric.

SMI-S provider connection and discovery information

This section describes the connection and discovery information required by HP SIM.

Physical configuration

An Ethernet connection to the switch is required to contact the CIMAgent.

SMI-S provider connection information

Management application connection information

- All profiles, including the Server profile, are implemented in the root/switch namespace.

- If SSL is enabled on the switch, the CIMAgent will not accept non-secure http connections over port 5988.
- Additional use accounts can be added via Telnet or the SANSurfer Manager.

Use the following parameters to connect to the SMI-S provider:

IP Address	IP address of the switch
Namespace	root/switch
User	Same as Telnet login
Password	Same as Telnet login
Port	5988 (SSL Disabled) 5989 (SSL Enabled)

Enabling Service Locator Protocol (SLP)

SLP Server Agent support is integrated into the CIMAgent. If the switch is on and the CIM service is enabled, the CIMAgent will advertise its presence and respond to requests for service.

Advertised profiles

Service, Fabric, and Switch. Sub-profiles are not advertised via SLP.

Limitations

- No support for TCP messages.

- No support for the SPI attribute in the SrvRqst message. The CIMAgent will drop any request containing SPI information.

- No support for the Predicate attribute in the SrvRqst message. This attribute is ignored.

- The SrvTypeRqst is not supported. The CIMAgent will drop this request.

State changes

In the event of an IP address change, or if SSL is enabled or disabled, the service advertisement will change. The CIMAgent will let all existing SLP Directory Agent (DA) registrations expire, and reregister the new information with all known DAs.

If the CIMAgent is disabled, or the switch is shut down, no SrvDeReg will be sent, and the registration is expected to time out. The default registration timeout is 130 seconds. The DA may require a larger timeout, which would be used for that DA.

SSL support

SSL capability is supported on this switch, and can be enabled or disabled.

If SSL is enabled, a client must use the SSL protocol to connect, and if it is disabled, clear TCP/IP must be used.

Fabric discovery

The CIMAgent provides information about all the switches and ports in the fabric by querying the management server and name server on other switches in the fabric. If the management server is disabled or incompletely implemented on the remote switches, a truncated fabric is reported.

Limitations

- HP SIM might experience a slight delay in discovering the switches while the SMI-S provider gathers information from the switches for the first time.

Frequently asked questions

Is SSL supported?

See SSL support.

How do I reconfigure the port used by the SMI-S provider?

The SMI-S provider is embedded in the switch, and there is only one SMI-S provider running on the switch. Therefore, there should never be a port conflict, so there is no need to reconfigure the default port usage (http/5988 or https/5989).

Does the SMI-S provider support SLP?

See Enabling SLP.

What indications are supported?

- The CIMAgent supports the lifecycle indications required by the SMI-S specification.

- Alert indications are not supported

- No indications are generated as a result of a system reset, or CIM service reset.

- Initial discovery of devices in the fabric does not result in generation of life cycle indications.

Indication registration limitations:

- 32 cimlisteners can be created

- 50 total cimsubscribers

- 6 subscriptions per Listener

How is vendor and product information reported?

If the switch is rebranded, the property values for the rebranded product are supplied by the SMI-S provider. The product related properties and values supported by the SMI-S provider are listed below.

- QLGC_PhysicalChassis: CIM_PhysicalPackage: All switches report a single physical chassis that models the framework on which the switch components are mounted.

  - Manufacturer: The name of the switch manufacturer.

  - Model: Contains the switch model name. If the switch is rebranded, the name assigned by the vendor is used.

  - PartNumber: Contains a string that matches the part number printed on the switch chassis.

  - SerialNumber: Contains a string that matches the serial number printed on the switch chassis.

- QLGC_Prodict: CIM_PRODUCT: Product models the combination of hardware and software that make up the switch. The embedded CIMAgent reports a single product instance representing the switch hosting the SMI-S provider.

  - IdentifyingNumer: Contains the switch serial number as printed on the chassis.

  - Name: Contains the commonly known name of the product. For rebranded switches, this is the vendor-assigned product name.

  - Vendor: The name of the switch vendor.

  - Version: Contains the value 0.

  - ElementName: Contains the commonly known name of the product. For rebranded switches, this is the vendor-assigned product name. This property matches the SNMP System Description.

Is the SMI-S provider proxied or embedded in the device?

It is embedded in the firmware version 5.2.0.29 and later.

What CIMOM implementation is used by the SMI-S provider?

Open Pegasus

Links

- HP SIM overview:
  http://h18013.www1.hp.com/products/servers/management/hpsim/index.html

- HP SIM SMI-S provider information:
  http://h18013.www1.hp.com/products/servers/management/hpsim/smi-s-providers.html