



SOLUTIONPACK FOR CISCO MDS NEXUS

TABLE OF CONTENTS

- Summary Sheet

 - Overview

 - Technical specifications

 - Performing pre-configuration tasks

 - Known issue with user-defined roles

 - Configuring switches for SNMPv1 and SNMPv2

 - Configuring switches for SNMPv3

 - Configuring Cisco switches for alert consolidation

 - Installing the SolutionPack

 - Enabling passive host discovery for Cisco MDS/Nexus through Generic-SNMP

 - Reconfiguring the Generic-SNMP SolutionPack block instance

 - How to add or modify zone naming patterns

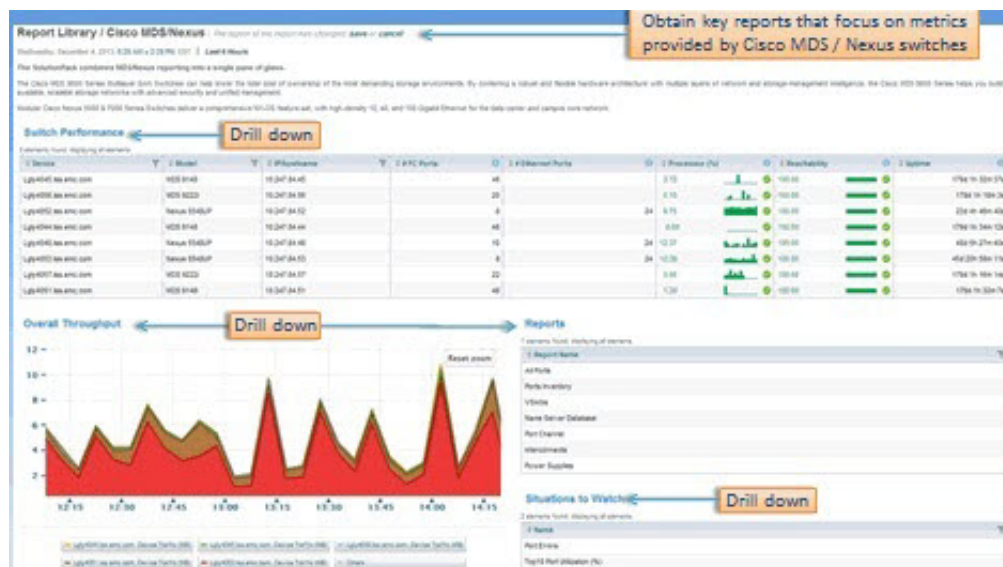
 - Activating modified zone name patterns

OVERVIEW

This article explains how to install and configure SolutionPack for Cisco MDS/Nexus. The SolutionPack for Cisco MDS/Nexus accesses performance data that was automatically collected and interpreted (using resource grouping and mathematical calculations) across multiple MDS/Nexus fabrics.

This article applies to EMC ViPR SRM version 3.5.1.

Alerts are consolidated from Cisco MDS/Nexus Switches and shown on the **All Alerts Console**.



SolutionPack for Cisco MDS/Nexus

TECHNICAL SPECIFICATIONS

SolutionPack version

3.5.1

Compatible ViPR SRM version

EMC ViPR SRM version: 3.5.1

Data collection methods

- Accesses performance data information that was automatically collected and interpreted (using resource grouping and mathematical calculations) from across multiple fabrics. Uses SNMP to collect fabric information.

Main reports

Port Utilization

Report over Fibre channel ports and Port-Channel.

VSAN

VSAN utilization and relationship.

Overall Throughput

The sum of throughput of all the interfaces of each switch

Switch Performance

Report on the utilization, reachability, and uptime of the switch

Name Server

Name Server topology information.

Environmental elements

Power Supply, temperature sensors.

Supported models for Cisco fabric

Supported model	Collector	Prerequisites	Port/Protocol
- Cisco MDS (9xxx) - Cisco ONS (1520x) - Cisco Nexus (5548, 1000V)	Generic-SNMP	Supported MIBs: - CISCO-FLASH-MIB - CISCO-NS-MIB - CISCO-DM-MIB - CISCO-ENTITY-SENSOR-MIB - ENTITY-MIB - CISCO-FC-FE-MIB - IF-MIB - CISCO-ENTITY-FRU-CONTROL-MIB - CISCO-VSAN-MIB - CISCO-DM-MIB - CISCO-ZS-MIB - CISCO-SYSTEM-EXT-MIB - SNMPv2-MIB - CISCO-FCS-MIB - CISCO-FEATURE-CONTROL-MIB Some switch models might not have all of the listed MIBs and in that case those capabilities will not be discovered.	SNMP (default port is 161)

Note

The following points apply to all of the supported models:

1. Discovery is limited to FC ports only.
 2. ViPR SRM does not support Cisco device aliases or Cisco enhanced device aliases.
 3. ViPR SRM does not support discovery of VDC (virtual device context) and Fabric extenders.
-

PERFORMING PRE-CONFIGURATION TASKS

Before you discover a Cisco switch in ViPR SRM you need to perform the following checks.

All switches in the Cisco fabric must have SNMP credentials for use with ViPR SRM. For example, if SNMPv1/v2c is used, all Cisco switches in the fabric should have the SNMPv1/v2c community name set with a role of network-admin or network-operator. For example, if SNMPv3 is used, all Cisco switches in the fabric should have the SNMPv3 user set with the role of network-admin or network-operator.

PROCEDURE

1. Ensure all hardware and software is listed as supported in the *EMC ViPR SRM Support Matrix*.
2. Verify the TCP/IP connectivity to the switches to be discovered. Test by issuing a ping command to these switches.
3. Determine if SNMP traps are enabled. Log in to the switch and run the command `show snmp trap`.
4. Run the command `snmp-server enable traps` to enable SNMP traps.
SWDevCisco8-9216i# config terminal
Enter configuration commands, one per line. End with CNTL/Z.

SWDevCisco8-9216i (config)# snmp-server enable traps
5. Display the traps that are enabled. Execute the `show snmp trap` command. The values in the **Enabled** column should be **Yes**.

KNOWN ISSUE WITH USER-DEFINED ROLES

If an SNMPv3 user or SNMPv1/v2c community string used for switch discovery is assigned to a role that has VSAN policy set to **deny**, there is a possibility of switch reboot and supervisor fail-over.

This is due to an issue in Cisco NX-OS 5.2(6) through 6.2(x).

The workaround is to execute the following commands in sequence:

```
linbge197#config t
linbge197#role name <name of the role>
```

```
linbge197#no vsan policy deny
linbge197#copy run start
linbge197#exit
```

CONFIGURING SWITCHES FOR SNMPV1 AND SNMPV2

You have to configure Cisco switches for SNMPv1 or SNMPv2c to enable switch discovery, and alert consolidation for the switches. The SNMPv1 or SNMPv2c information you provide when performing discovery is necessary for ViPR SRM to contact the switch to obtain information.

BEFORE YOU BEGIN

If SNMPv1/v2c is used, all Cisco switches in the fabric should have the SNMPv1/v2c community name set with a role of network-admin/network-operator.

ViPR SRM collects data from the switch using the SNMP community name. It uses the SNMP port for communication. The default port set is port 161.

Note

The Cisco documentation provides information on configuring Cisco switches for SNMPv1 and SNMPv2c management.

PROCEDURE

1. Log into the switch as an administrator.
2. To configure the snmp-server community string with read-only privileges, run the following commands:
Cisco8-9216i# config terminal

```
Cisco8-9216i(config)# snmp-server community srmuser ro
```

You have to type configuration commands, one per line and end with **CNTRL/Z**.

3. To verify if the SNMPv1 community string exists, run the command show snmp community.
A sample output of the command:

Community	Group/Access
srmuser	network-operator

CONFIGURING SWITCHES FOR SNMPV3

You have to configure Cisco switches for SNMPv3 to enable discovery and alert consolidation for the switches. The SNMPv3 information you provide when performing discovery is necessary for ViPR SRM to contact the switch to obtain information.

ViPR SRM collects data from the switch using SNMPv3 secure credentials. ViPR SRM supports SNMPv3 with all the combinations of Auth (MD5, SHA) and Priv (AES, DES, NONE).

Note

Create the SNMPv3 users with authentication and privacy passwords on all physical switches in the fabric. The Cisco documentation provides information on creating SNMPv3 users on Cisco switches.

This procedure provides an example of creating an SNMPv3 user called srmuser with a network-operator role, SHA authorization, and AES128 authentication.

PROCEDURE

1. Log into the switch as an administrator.
Cisco8-9216i# config terminal
Enter configuration commands, one per line. End with **CNTL/Z**.

Cisco8-9216i (config)#snmp-server user srmuser network-operator auth sha <SHA-password> priv aes-128 <AES-password>

2. Run the snmp-server user commands as follows:
config terminal

snmp-server user srmuser network-operator auth sha <SHA-password> priv aes-128 <AES-password>

You have to type configuration commands, one per line and end with **CNTL/Z**.

3. To verify the new user creation run the command show snmp user.

Sample output of show snmp user command

		SNMP USERS	
User	Auth	Priv(enforce)	Groups

admin	md5	no	network-admin
srmuser	sha	aes-128(no)	network-operator
NOTIFICATION TARGET USERS (configured for sending V3 Inform)			
User	Auth	Priv	
SWDevCisco8-9216i#			

CONFIGURING CISCO SWITCHES FOR ALERT CONSOLIDATION

Use the snmp-server command to forward SNMP v1 alert traps from Cisco FC switches to ViPR SRM.

PROCEDURE

1. Log into the Cisco FC switch as the administrator.
2. Type `# config`, and press **Enter**.
3. Type `snmp-server host <trap recipient IP> traps <SNMP trap version> <Community String> udp-port <trap listening port >`, and press **Enter**.

In the command syntax:

**Syntax
element** **Input**

<trap recipient IP>	In a single vApp installation is the ViPR SRM IP, and in a distributed environment, is the suite's Backend server's IP.
<SNMP trap version>	version 1
<Community String>	public
<trap	2041 , which is the ViPR SRM trap listening port.

listening port

>

Example: `snmp-server host 10.247.24.190 traps version 1 public udp-port 2041`

4. If you have multiple Cisco FC switches in your storage environment, repeat this procedure on each switch.

INSTALLING THE SOLUTIONPACK

BEFORE YOU BEGIN

- ViPR SRM core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.
- [Managing Alert Consolidation](#) explains how to configure alerts consolidation.

PROCEDURE

1. Log in.
2. Click **Administration**.
3. Click **Centralized Management**.
4. Click **SolutionPacks**.
5. Select **SolutionPack Center**.
6. Select the SolutionPack for Cisco MDS/Nexus in the **Browse and Install SolutionPacks** screen.
7. Click **Install**.
8. In the **Alert Consolidation** field of the **Select the components to install** window, select the Primary Backend host.
9. In the **Pre-configured alerts** field, select the Primary Backend host.
10. In the **Reports** field, select the Frontend host.
11. In the **SNMP Masks** field, select the Frontend host.
12. Click **Next**.
13. Click **Next**.
14. In the **Alerting on data collection** field of the **Pre-configured alerts** window, you can select a different destination for alerts: select **Add a new Alerting on data collection**, and select a Primary Backend host as the **Alerting Web Service Instance**.

15. Click **Next**.
16. In the **Administration Web-Service Instance** field of the **Reports** window, select the Frontend host.
17. Click **Next**.
18. Click **Install**.
The SolutionPack installation begins.
19. Click **Ok** once installation is complete.
20. Add an SNMP collector and discover switches as described in [Discovering SAN Switch Devices](#).

ENABLING PASSIVE HOST DISCOVERY FOR CISCO MDS/NEXUS THROUGH GENERIC-SNMP

If you cannot access the active host, you cannot use active host discovery. In this case, you have to enable passive host discovery if you want to see end to end topology from hosts to array and identify chargeback on SAN enabled hosts.

To enable passive host discovery through the SolutionPack for Cisco MDS/Nexus, you need to reconfigure the Generic-SNMP independent SolutionPack block instance after selecting the **Enable Passive Host Discovery** checkbox.

The default zone naming patterns supported in SolutionPack for Cisco MDS/Nexus are:

- **z_%h%**
- **z_%h%_***
- **z_%h%_*_***
- **%h%_***

z_%h% specifies where the host name occurs in a zone name. The wildcard character (*) indicates that any character can occur at that location in a zone name.

Only add to or modify the existing zone naming patterns if default zoning patterns do not support your zoning configurations.

To add to or modify existing zone naming patterns, add or modify the regex patterns in the VHF xml file `/opt/APG/Collecting/Variable-Handling-Filter/Generic-SNMP-block-instance-name/conf/vhf-mds-zone-dns.xml`.

PROCEDURE

1. [Reconfiguring the Generic-SNMP SolutionPack block instance](#)
2. [How to add or modify zone naming patterns](#)

RECONFIGURING THE GENERIC-SNMP SOLUTIONPACK BLOCK INSTANCE

PROCEDURE

- 1. Click **Administration**.
- 2. Click **Centralized Management**.
- 3. Click **SolutionPacks**.
- 4. Under **Independent SolutionPack Blocks**, click the reconfigure icon to reconfigure the **Generic-SNMP**SolutionPack Block instance.
- 5. Select the **Enable Passive Host Discovery** checkbox.
- 6. Click **Reconfigure**.

HOW TO ADD OR MODIFY ZONE NAMING PATTERNS

Edit regex patterns in VHF XML files.

The regex patterns in the xml file is based on Java's regular expression format.

The following section of XML code needs to be added or modified for supporting new zone name patterns:

```
<regex-property name="zname" keep="true">
<!-- <regex>(.*?)</regex>-->
<!-- supporting hostname format (z_%h) -->
<regex>^(z_) ([A-Z0-9a-z]+)$</regex> <!-- zone member name pattern -->
<part name="hostname" value="2" />
<part name="device" value="2"/>
<part name="devtype" value="PassiveHost"/>
<part name="parttype" value="Disk"/>
</regex-property>
```

Sample modifications of zone naming patterns

Regex is <code>^(z_)([A-Z0-9a-z]+)\$</code> and hostname position is 2	Matches all the zone names that start with 'z_' and extracts the hostname from that matches the rest of the string that follows 'z_' Example: For zone name z_lingz099, the hostname extracted is lingz099.
Regex is <code>^([z_][A-Z0-9a-z]+)_([A-Za-z0-9]+)</code> and hostname position	Matches all the zone names that doesn't start with 'z_' and extracts the hostname from zone name that is before the first

is 1	underscore. Example: For lgloe111_1106, the hostname extracted is lgloe111.
------	--

For more information on writing Java's regular expression refer to <http://docs.oracle.com/javase/tutorial/essential/regex/>

ACTIVATING MODIFIED ZONE NAME PATTERNS

After modifying a zone name pattern, activate the modifications.

Procedure

1. Click **Administration**.
2. Click **Centralized Management**.
3. Click **Logical Overview**.
4. Click **Collecting**.
5. Click **Collector-Manager:: Generic-SNMP<instance name>**.
6. In the Service Status section, click **Stop** and then click **Start**.

EMC REDEFINES:

CLOUD COMPUTING »

BIG DATA »

TRUSTED INFRASTRUCTURE »

FLASH STORAGE »

SOCIAL@EMC »

EMC Pulse News Blog

Recent Blog Posts

All EMC Blogs

EMC Community Network

Facebook

Twitter

YouTube

LinkedIn

[Flickr](#)

LEARNING »

[Training and Certification](#)

[RSA Security Training](#)

[EMC Academic Alliance](#)

[EMC Proven Professional](#)

[Partner Readiness](#)

[Events](#)

[Resource Library](#)

[EMC Glossary](#)

POPULAR

[About EMC](#)

[Investor Relations](#)

[Careers @ EMC](#)

[EMC Pulse News Blog](#)

[Newsroom](#)

[Sustainability](#)

[EMC TV](#)

[EMC MOBILE](#)

[EMC Store](#)

[Product Security](#)



[SHARE](#)

[CONTACT](#)

[FEEDBACK](#)

[SITE MAP](#)

[PRIVACY POLICY](#)

[LEGAL NOTICES](#)

EMC builds information infrastructures and virtual infrastructures to help people and businesses around the world unleash the power of their digital information. EMC offerings in backup and recovery, enterprise content management, unified storage, big data, enterprise storage, data federation, archiving, security, and deduplication help customers move to and build IT trust in their next generation of information management and enable them to offer IT-as-a-Service as part of their journey to cloud computing.

We are an Equal Employment Opportunity employer that values the strength diversity brings to the workplace. All qualified applicants,

regardless of race, color, religion, gender, sexual orientation, marital status, gender identity or expression, national origin, genetics, age, disability status, protected veteran status, or any other characteristic protected by applicable law, are strongly encouraged to apply.

© 2014 EMC Corporation. All rights reserved.