

SolutionPack for Cisco MDS Nexus

Release number 3.5

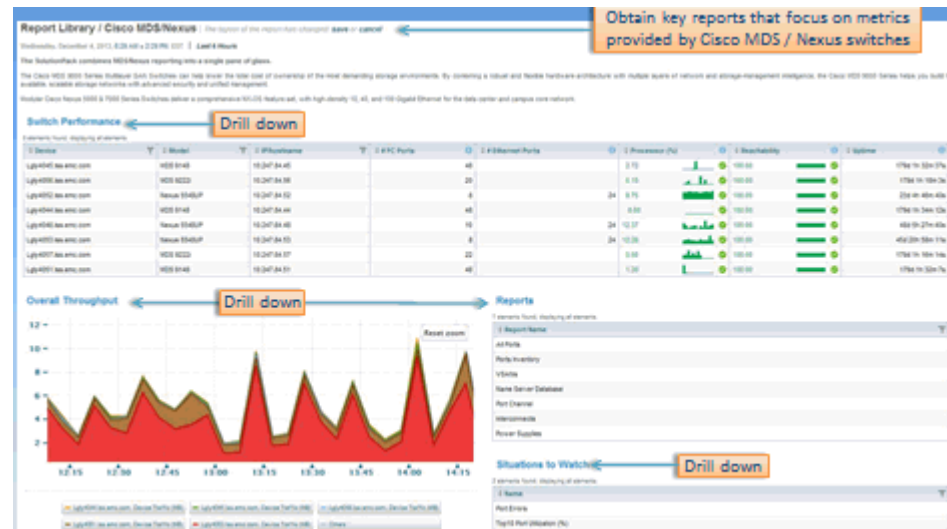
Summary Sheet

June, 2014

- ◆ [Overview](#)..... 2
- ◆ [Technical specifications](#)..... 2
- ◆ [Performing pre-configuration tasks](#)..... 3
- ◆ [Configuring switches for SNMPv1 and SNMPv2](#)..... 4
- ◆ [Configuring switches for SNMPv3](#)..... 4
- ◆ [Configuring Cisco switches for alert consolidation](#)..... 5
- ◆ [Installing the solutionpack](#)..... 6
- ◆ [Enabling passive host discovery for Cisco MDS/Nexus through Generic-SNMP](#)..... 7

Overview

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



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

Technical specifications

SolutionPack version

3.5

Compatible ViPR SRM version

3.5

Supported systems

- ◆ MDS 9120, 9124, 9134, 9140, 9148, 9216, 9222i, 9506, 9509, 9513
- ◆ ONS 15201, 15202
- ◆ Nexus 5548, 1000V
- ◆ Alert collection using SNMP traps for those above and for MDS 9000

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, Ethernet ports and Port-Channel.
- ◆ VSAN - VSAN utilization and relationship.
- ◆ ISL - Interconnect report.

- ◆ Name Server - Name Server topology information.
- ◆ Environmental elements - Power Supply, temperature sensors.
- ◆ Alert collection using SNMP traps for all above and MDS 9000.
- ◆ All Alerts Console.

Supported models

Table 1 Supported models for Cisco fabric

Supported model ^{a bc}	Collector	Prerequisites	Port
• Cisco MDS (9120, 9124, 9134, 9140, 9148, 9216, 9222i, 9506, 9509, 9513) • Cisco ONS (15201, 15202) • Cisco Nexus (5548, 1000V)	Generic-SNMP	The following Cisco MIBs are needed: • cisco-entity-frr-control-mib • cisco-entity-sensor-mib • cisco-fc-fe-mib • cisco-fcs-mib • cisco-vsan-mib	SNMP (default port is 161)

- Discovery is limited to FC ports only.
- ViPR SRM does not support Cisco device aliases or Cisco enhanced device aliases.
- 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 the same SNMP credentials for use with ViPR SRM. For example, if the SNMPv1/v2 community setting private is used, all Cisco switches in the fabric should have the SNMPv1/v2 private community name set with a role of network-admin. For an SNMPv3 user, the same SNMPv3 credentials with the role of network-admin should be set on every switch in the fabric.

Procedure

1. Ensure all hardware, including the switch model, 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`.

Configuring switches for SNMPv1 and SNMPv2

You have to configure Cisco switches for SNMPv1 or SNMPv2 to enable discovery, data collection, and alert consolidation for the switches. The SNMPv1 or SNMPv2 information you provide when performing discovery is necessary for ViPR SRM to contact the switch to obtain information.

Before you begin

Ensure that the Cisco switches have an SNMPv1 community name that has read only privileges set on every switch in the fabric. The SNMP community selected must have a network-operator role.

ViPR SRM collects data from the switch using the same 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 SNMPv2 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 eccuser ro
```

You have to type configuration commands, one per line and end with **CTRL/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
eccuser	network-operator

Configuring switches for SNMPv3

You have to configure Cisco switches for SNMPv3 to enable discovery, data collection, 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 uses the SNMP port for communication. ViPR SRM supports SNMPv3 with all the combinations of Auth (MD5, SHA) and Priv (AES, DES, NONE).

Note

Create the same SNMPv3 users with the same 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 ECCuser 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 ECCuser 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 ECCuser 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`.

A sample output of the command:

SNMP USERS			
User	Auth	Priv(enforce)	Groups
admin	md5	no	network-admin
ECCuser	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 this procedure to configure forwarding of alert traps (SNMP v1) from Cisco FC switches to the suite.

Procedure

1. Log into the Cisco FC switch as the administrator.
2. To enter the global configuration mode, at the terminal prompt, type `# config`, and press **Enter**.

Cisco documentation provides more information on the global configuration mode.

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
<i><trap recipient IP></i>	In a single vApp installation is the VIPR SRM IP, and in a distributed environment, is the suite's Backend host IP.
<i><SNMP trap version></i>	version 1

Syntax element	Input
<i>Community String</i>	public
<i>trap listening port</i>	2041 , which is the ViPR SRM trap listening port.

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

- 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.

Procedure

- Log in and select **Administration**.
- Select **Centralized Management** in the Administration tree.
- Select **SolutionPacks** in the tree.
- Select **SolutionPack Center**.
- Select the SolutionPack for Cisco MDS/Nexus in the **Browse and Install SolutionPacks** screen.
- Click **Install**.
- In the **Alert Consolidation** field of the **Select the components to install** window, select the Primary Backend host.
- In the **Pre-configured alerts** field, select the Primary Backend host.
- In the **Reports** field, select the Frontend host.
- In the **SNMP Masks** field, select the Frontend host.
- Click **Next**.
- Click **Next**.
- 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**.
- Click **Next**.
- In the **Administration Web-Service Instance** field of the **Reports** window, select the Frontend host.
- Click **Install**.
The SolutionPack installation begins.
- Click **Ok** once installation is complete.
Performance data will displayed in about an hour.

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

You have to enable passive host discovery when you want to see end to end topology from hosts to array and identify chargeback on SAN enabled hosts, without active host discovery.

You need to reconfigure Generic-SNMP independent solution pack to enable passive host discovery through the SolutionPack for Cisco MDS/Nexus.

The zone naming patterns supported in ViPR SRM are:

`z_%h%`

`z_%h%_*`

`z_%h%_*_*`

`%h%_*`

If you want to add or modify the existing zone naming patterns:

Procedure

1. Add or modify the regex patterns in the VFH xml file `/opt/APG/Collecting/Variable-Handling-Filter/Generic-SNMP-block-instance-name/conf/vhf-mds-zone-dns.xml`
2. After modifying these xml files, restart the collection-manager service of Generic SNMP instance in case of the SolutionPack for Cisco MDS/Nexus

How to add or modify zone naming patterns

Edit regex patterns in VFX 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="\${1}" />  <!-- hostname position in
the pattern -->
  <part name="createdBy" value="System" />
  <part name="devtype" value="PassiveHost" />
</regex-property>
```

The following examples explain how to read and interpret these patterns in simple terms:

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 is 1	Matches all the zone names that doesn't start with 'z_' and extracts the hostname from zone name that is before the first 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/>

Copyright © 2014 EMC Corporation. All rights reserved. Published in USA.

Published June, 2014

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC², EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

For the most up-to-date regulatory document for your product line, go to EMC Online Support (<https://support.emc.com>).