CHAPTER 6

VSM and VEM Modules

This chapter describes how to identify and resolve problems that relate to modules and includes the following sections:

Information About Modules

Cisco Nexus 1000V manages a data center defined by a VirtualCenter. Each server in the data center is represented as a module and can be managed as if it were a module in a physical Cisco switch.

The Cisco Nexus 1000V implementation has 2 parts:

- Virtual supervisor module (VSM) – This is the control software of the Cisco Nexus 1000V distributed virtual switch. It runs on a virtual machine (VM) and is based on Cisco NX-OS software.
- Virtual Ethernet module (VEM) – This is the part of Cisco Nexus 1000V that actually switches data traffic. It runs on a VMware ESX 4.0 host. Several VEMs are controlled by one VSM. All the VEMs that form a switch domain should be in the same virtual Data Center as defined by VMware VirtualCenter.

Troubleshooting a Module Not Coming Up on the VSM

This section describes the process you can use when a module does not come up on the VSM. This section includes the following topics:

- Collecting Logs, page 6-13

Guidelines for Troubleshooting Modules

Follow these guidelines when troubleshooting a module controlled by the VSM.

- You must have a VSM VM and a VEM up and running.
- Make sure you are running compatible versions of vCenter Server and VSM.

  For more information, see the *Cisco Nexus 1000V Compatibility Information, Release 4.0(4)SV1(3)*.
- To verify network connectivity between the VSM and vCenter Server, ping the IP address of the vCenter Server. If you are using a domain name service (DNS) name, use the DNS name in the ping. If a ping to the vCenter Server fails, check to see if you can ping the gateway. Otherwise, check the mgmt0 interface configuration settings.
- Make sure the firewall settings are OFF on the vCenter Server. If you want the firewall settings, then check to see if these ports are open.
  - Port 80
  - Port 443
- If you see the following error, verify that the VSM extension was created from vCenter Server.
  - ERROR: [VMware vCenter Server 4.0.0 build-150489]
    Extension key was not registered before its use

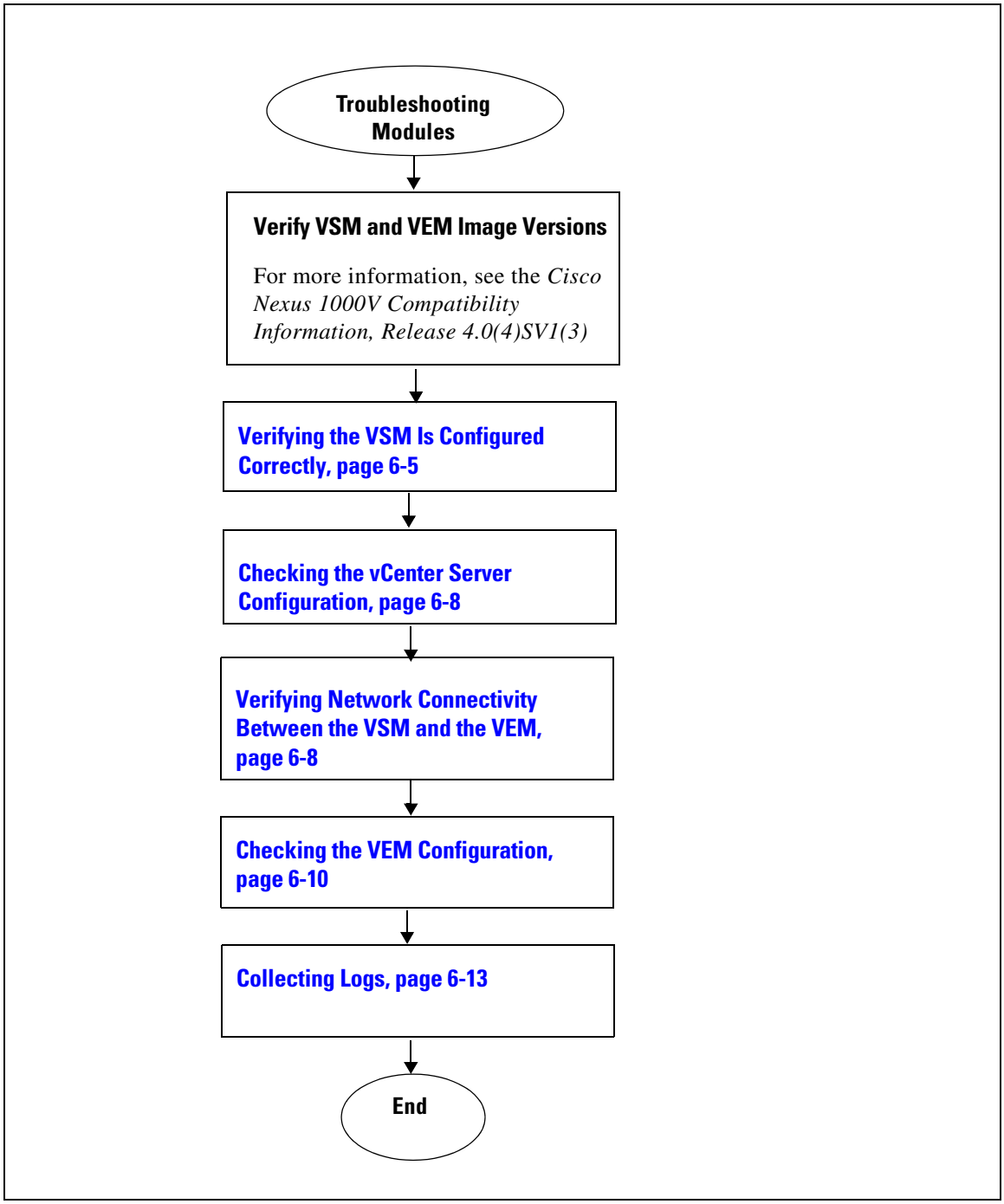
  To verity that the extension or plugin was created, see the "Finding the Extension Key Tied to a Specific DVS" procedure on page 3-8.

  For more information about extension keys or plugins, see the "Managing Extension Keys" section on page 3-6.
- If you see the following error, see the "Checking the vCenter Server Configuration" procedure on page 6-8.
  - ERROR: Datacenter not found
- For a list of terms used with Cisco Nexus 1000V, see the *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3)*.

Flow Chart for Troubleshooting Modules

Use the following flowchart to troubleshoot modules.

Flowchart: Troubleshooting Modules



Verifying the VSM Is Connected to the vCenter Server

You can use the following procedure to verify that the VSM is connected to the vCenter Server.

Step 1 Verify the connection between the VSM and vCenter Server.

show svs connections

The output should indicate that the operational status is **Connected**.

```
Example:
n1000v# show svs connections
connection vc:
    ip address: 172.23.231.223
    protocol: vmware-vim https
    certificate: user-installed
    datacenter name: hamilton-dc
    DVS uuid: 92 7a 14 50 05 11 15 9c-1a b0 f2 d4 8a d7 6e 6c
    config status: Disabled
    operational status: Disconnected
```

Step 2 Do one of the following:

- If the status is **Connected**, then return to the Flowchart: Troubleshooting Modules, page 6-3.
- If not, then continue with the next step.

Step 3 Connect to the vCenter Server.

config t

svs connection *datacenter_name*

connect

```
Example:
n1000v# conf t
n1000v(config)# svs connection HamiltonDC
n1000v(config-svs-conn)# connect

Example:
n1000v# conf t
n1000v(config)# svs connection HamiltonDC
n1000v(config-svs-conn)# connect
ERROR: [VMWARE-VIM] Extension key was not registered before its use.
```

Step 4 Do one of the following:

- If you see an error message about the Extension key, continue with the next step.
- If not, go to Step 6.

Step 5 Do the following and then go to Step 6.

- Unregister the extension key using the "Unregistering the Extension Key in the vCenter Server" procedure on page 3-12.
- Install a new extension key using the following procedure in the *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3)*.
  - *Creating a Cisco Nexus 1000V Plug-In on the vCenter Server*

Step 6 Verify the connection between the VSM and vCenter Server.

show svs connections

The output should indicate that the operational status is **Connected**.

Example:

```
n1000v# show svs connections
connection vc:
    ip address: 172.23.231.223
    protocol: vmware-vim https
    certificate: user-installed
    datacenter name: hamilton-dc
    DVS uuid: 92 7a 14 50 05 11 15 9c-1a b0 f2 d4 8a d7 6e 6c
    config status: Disabled
    operational status: Disconnected
```

Step 7 Do one of the following:

- If the status is **Connected**, then you have completed this procedure.
- If not, then return to the Flowchart: Troubleshooting Modules, page 6-3.

Verifying the VSM Is Configured Correctly

This section includes the following procedures to verify the VSM configuration.

Verifying the Domain Configuration

You can use the following procedure to verify the domain configuration.

BEFORE YOU BEGIN

Before beginning this procedure, you should know or do the following:

- You are logged in to the CLI in EXEC mode.
- The output of the show **svs domain** command should indicate the following:
  - The presence of a control VLAN and a packet VLAN.
  - The domain configuration was successfully pushed to VC.

Step 1 On the VSM, verify the domain configuration.

show svs domain

Example:

```
n1000v# show svs domain
SVS domain config:
  Domain id:    682
  Control vlan: 3002
  Packet vlan:  3003
  L2/L3 Control VLAN mode: L2
  L2/L3 Control VLAN interface: mgmt0
  Status: Config push to VC successful
```

Verifying the System Port Profile Configuration

You can use this procedure to verify that there is at least one port profile configured as follows:

- The port profile type is Ethernet.
- The port profile has a system VLAN.
- The port profile is configured in trunk mode.
- The list of allowed VLANs is either a superset of or the same as the list of system VLANs.

For more information about system port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)*.

BEFORE YOU BEGIN

Before beginning this procedure, you should know or do the following:

- You are logged in to the CLI in EXEC mode.
- You know the name of your system port profile.

DETAILEDS STEPS

Step 1 On the VSM, verify the system port profile configuration.

show port-profile name *system-port-profile-name*

Example:

```
n1000v# show port-profile name system-uplink
port-profile system-uplink
  description: "System profile for critical ports"
  type: ethernet
  status: enabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: 260
  port-group: system-uplink
  max ports: -
  inherit:
  config attributes:
    switchport mode trunk
    switchport trunk allowed vlan 260
    no shutdown
  evaluated config attributes:
    switchport mode trunk
    switchport trunk allowed vlan 260
    no shutdown
  assigned interfaces:
n1000v(config-port-prof)#
```

Verifying the Control and Packet VLAN Configuration

You can use the following procedure to verify that the control and packet VLANs are configured on the VSM.

BEFORE YOU BEGIN

Before beginning this procedure, you should know or do the following:

- You are logged in to the CLI in EXEC mode.
- You know the VLAN IDs of the control and packet VLANs

  The control and packet VLANs can be the same VLAN or separate VLANs.

  If you do not know the VLAN IDs, use the **show running-config** command.
- The control and packet VLANs are also system VLANs in the system port profile.

Step 1 On the VSM, verify the control and packet VLANs.

show running-config vlan *vlan-id*

```
Example:
n1000v# show running-config vlan 260-261
version 4.0(4)SV1(3)
vlan 260
  name cp_control
vlan 261
  name cp_packet
n1000v#

Example:
n1000v# show running-config
version 4.0(4)SV1(3)
. . .
vlan 260
  name cp_control
vlan 261
  name cp_packet
. . .
n1000v#
```

Step 2 On the VSM, verify that the control and packet VLANs are also system VLANs in the system port profile.

show port-profile name *system-port-profile-name*

```
Example:
n1000v# show port-profile name system-uplink
port-profile system-uplink
  description: "System profile for critical ports"
  type: ethernet
  status: enabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: 260
  port-group: system-uplink
  max ports: -
  inherit:
  config attributes:
    switchport mode trunk
    switchport trunk allowed vlan 260
```

```
    no shutdown
  evaluated config attributes:
    switchport mode trunk
    switchport trunk allowed vlan 260
    no shutdown
  assigned interfaces:
n1000v(config-port-prof)#
```

Step 3 Do one of the following:

- If the control and packet VLANs are present and are system VLANs in the system port profile, you have completed this procedure.
- If not, configure them using the following procedure in the *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3).*

  Configuring the System Port Profile for VSM-VEM Communication

Checking the vCenter Server Configuration

You can use the following procedure from vSphere client to verify the configuration on the vCenter Server.

Step 1 Confirm that the host is added to the data center and the **n1000V** DVS in that data center.

Step 2 Confirm that at least one pnic of the host is added to the DVS, and that pnic is assigned to the **system-uplink** profile.

Step 3 Confirm that the three VSM vnics are assigned to the port groups containing the control VLAN, packet VLAN, and management network.

Verifying Network Connectivity Between the VSM and the VEM

You can use the following procedure to verify Layer 2 network connectivity between the VSM and VEM.

you are logged in to the ESX host.

one vem per esx host

BEFORE YOU BEGIN

Before beginning this procedure, you should know or do the following:

- You are logged in to the VSM CLI in EXEC mode.
- You are logged in to the VEM.
- You are logged in to the CLI of the upstream switch.

Step 1 On the VSM, find its MAC address.

show svs neighbors

The VSM MAC address displays as the AIPC Interface MAC.

The user VEM Agent MAC address of the host displays as the Src MAC.

Example:
```
n1000v# show svs neighbors

Active Domain ID: 1030

AIPC Interface MAC: 0050-568e-58b7
Inband Interface MAC: 0050-568e-2a39

Src MAC           Type   Domain-id    Node-id     Last learnt (Sec. ago)
------------------------------------------------------------------------

0002-3d44-0602     VEM      1030         0302     261058.59
```

Step 2 Do one of the following:

- If the output of the **show svs neighbors** command in Step 1 does not display the VEM MAC address, then there is a problem with connectivity between the server hosting the VSM and the upstream switch. Recheck the VSM configuration and vCenter Server configuration.
- Otherwise, continue with the next step.

Step 3 On the VEM, run the vem-health script using the VSM MAC address you found in Step 1.

Note If the vem-health script is not in the PATH, you can find it under /usr/lib/ext/cisco/nexus/vem*/sbin/.

vem-health check *vsm_mac_address*

The vem-health script output shows the cause of the connectivity problem and recommends next steps in troubleshooting.

Example:
```
~ # vem-health check  00:50:56:a3:36:90
VSM Control MAC address: 00:50:56:a3:36:90
Control VLAN: 90
DPA MAC: 00:02:3d:40:5a:03

VSM heartbeats are not reaching the VEM.
Your uplink configuration is correct.
Recommended action:
Check if the VEM's upstream switch has learned the VSM's Control MAC.
```

Step 4 Do one of the following:

- If the VEM health check in Step 3 indicates a problem with connectivity to the upstream switch. continue with the next step.
- Otherwise, go to Step 7.

Step 5 On the upstream switch, display the MAC address table to verify the network configuration.

Example:
```
switch# show mac address-table interface Gi3/1 vlan 3002
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age              ports
------+---------------+--------+-----+----------+--------------------------
Active Supervisor:
```

```
* 3002  0050.56be.7ca7   dynamic  Yes          0   Gi3/1

switch# show mac address-table interface Gi3/2 vlan 3002
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
Active Supervisor:
* 3002  00:02:3d:40:0b:0c   dynamic  Yes          0   Gi3/2
```

Step 6 Do one of the following:

- If the output from Step 5 does not display the MAC address of the VSM, then there is a problem with connectivity between the server hosting the VSM and the upstream switch. Recheck the VSM configuration and vCenter Server configuration.
- Otherwise, continue with the next step.

Step 7 On the VEM, enter the following commands to verify that the VSM MAC appears in the control and packet VLANs.

config t

module vem *module_number* **execute vemcmd show l2** *control_vlan_id*

module vem *module_number* **execute vemcmd show l2** *packet_vlan_id*

The VSM eth0 and eth1 MAC addresses should display in the host control and packet VLANs.

```
Example:
n100v# config t
n1000v(config)# module vem 3 execute vemcmd show l2 3002
Bridge domain 3002 brtmax 100, brtcnt 3, timeout 120
    Dynamic MAC 00:50:56:be:7c:a7  LTL    16 pvlan     0 timeout   110
    Dynamic MAC 00:02:3d:40:0b:0c  LTL    10 pvlan     0 timeout   110

n1000v(config)# module vem 3 execute vemcmd show l2 3003
Bridge domain 3002 brtmax 100, brtcnt 3, timeout 120
    Dynamic MAC 00:50:56:be:7c:a7  LTL    16 pvlan     0 timeout   110
    Dynamic MAC 00:02:3d:20:0b:0c  LTL    10 pvlan     0 timeout   110
```

Step 8 Do one of the following:

- If the MAC address of the VSM does not appear in the output of Step 7, then check the VEM configuration as explained in "Checking the VEM Configuration" section on page 6-10.
- Otherwise, you have completed this procedure.

Checking the VEM Configuration

You can use the following procedure to verify that the ESX host received the VEM configuration and setup.

BEFORE YOU BEGIN

Before beginning this procedure, you should know or do the following:

- You are logged in to the VEM.

- The port LTL number is the port index number, for example, 48.

Step 1 On the ESX host, use the following command to confirm that the VEM Agent is running, and that the correct host uplinks are added to the DVS.

vem status

Example:
```
~ # vem status
VEM modules are loaded

Switch Name     Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0        64          3           64                1500    vmnic0
DVS Name        Num Ports   Used Ports  Configured Ports  Uplinks
n1000v          256         9           256               vmnic1 VEM Agent is running
```

Step 2 Use the following commands to restore connectivity that is lost due to an incorrect MTU value on an uplink:

vemcmd show port *port-LTL-number*

vemcmd set mtu *size* **ltl** *port-LTL-number*

The MTU is reset on the ESX causing the connectivity to be restored.

Example:
```
~ # vemcmd show port 48
LTL    IfIndex   Vlan    Bndl  SG_ID Pinned_SGID  Type  Admin State  CBL Mode
Name  . . .
17   1a030100      1 T   304      1          32  PHYS     UP    UP    1  Trunk vmnic1
~# vemcmd set mtu 9000 ltl 17
```

Note Use these **vemcmds** only as a recovery measure and then update the MTU value in the port profile configuration for system uplinks or in the interface configuration for non-system uplinks.

Step 3 Use the following command to verify that the domain ID, control VLANs, and packet VLANs are configured correctly on the host.

vemcmd show card

Example:
```
~ # vemcmd show card
Card UUID type  2: 58f8afd7-e1e3-3c51-85e2-6e6f2819a7b8
Card name: sfish-srvr-1
Switch name: n1000v
Switch alias: DvsPortset-0
Switch uuid: 56 e0 36 50 91 1c 32 7a-e9 9f 31 59 88 0c 7f 76
Card domain: 1024
Card slot: 4
VEM Control (Control VLAN) MAC: 00:02:3d:14:00:03
VEM Packet (Inband) MAC: 00:02:3d:24:00:03
VEM Control Agent (DPA) MAC: 00:02:3d:44:00:03
VEM SPAN MAC: 00:02:3d:34:00:03
Management IP address: 172.23.232.102
Max physical ports: 32
Max virtual ports: 216
Card control VLAN: 3002
Card packet VLAN: 3003
       Processors: 4
  Processor Cores: 4
Processor Sockets: 2
```

```
  Physical Memory: 4290351104
```

Step 4 Use the following command to verify that the ports of the host added to the DVS are listed, and that the ports are correctly configured as access or trunk on the host.

vemcmd show port

Example:

```
~ # vemcmd show port
LTL    IfIndex   Vlan    Bndl  SG_ID Pinned_SGID  Type  Admin State  CBL Mode   Name
8          0   3969       0      2            2  VIRT     UP    UP    4 Access l20
9          0   3969       0      2            2  VIRT     UP    UP    4 Access l21
10         0   3002       0      2            2  VIRT     UP    UP    4 Access l22
11         0   3968       0      2            2  VIRT     UP    UP    4 Access l23
12         0   3003       0      2            2  VIRT     UP    UP    4 Access l24
13         0      1       0      2            2  VIRT     UP    UP    0 Access l25
14         0   3967       0      2            2  VIRT     UP    UP    4 Access l26
16  1a030100      1 T     0      2            2  PHYS     UP    UP    4  Trunk vmnic1
```

The last line of output indicates that vmnic1 should be in Trunk mode, with the CBL value of 4. The CBL value of the native VLAN does not have to be 4. It will be 0 if it is not allowed, or 1 if it is VLAN 1 and not allowed. This is not an issue unless the native VLAN is the Control VLAN VLAN.The Admin state and Port state should be UP.

Step 5 Use the following commands to verify in the broadcast domain that the vmnic port that is supposed to carry the control VLAN and packet VLAN is present.

vemcmd show bd *control_vlan*
vemcmd show bd *packet_vlan*

Example:

```
~ # vemcmd show bd 3002
BD 3002, vdc 1, vlan 3002, 2 ports
Portlist:
     10  l22
     16  vmnic1
~ # vemcmd show bd 3003
BD 3003, vdc 1, vlan 3003, 2 ports
Portlist:
     12  l24
     16  vmnic1
```

Step 6 Use the **vemcmd show trunk** command to verify the following:

- The control and packet VLANs are shown in the command output, indicating that the DV port groups are successfully pushed from the vCenter Server to the host.
- The correct physical trunk port vmnic is used.

Example:

```
~ # vemcmd show trunk
Trunk port 16 native_vlan 1 CBL 4vlan(1) cbl 4, vlan(3002) cbl 4, vlan(3003) cbl 4,
```

At least one physical uplink must be carrying the control and packet VLANs. If more than one uplink is carrying the control and packet VLANs, the uplinks must be in a port channel profile. The port channel itself would not be visible because the VEM is not yet added to the VSM.

Step 7 Use the following commands to restore connectivity that is lost due to incorrect port and system VLAN settings:

vemcmd show port *port-ltl-number*

vemcmd set system-vlan *vlan_id* **ltl** *port-ltl-number*

Example:

```
~ # vemcmd show port 48
LTL    IfIndex   Vlan    Bndl  SG_ID Pinned_SGID  Type  Admin State  CBL Mode
Name   . . .
48   1b030000     1       0     32           1  VIRT     UP DOWN DOWN    0 Access vmk1
~ # vemcmd set system-vlan 99 ltl 48
```

Note Use these **vemcmds** only as a recovery measure and then update the port profile configuration with correct system VLANs.

Collecting Logs

After you have verified network connectivity between the VEM and the VSM, you can use the following procedure to collect log files to help identify the problem.

Step 1 On the VEM, use the following command to verify its UUID.

vemcmd show card info

Example:

```
~ # module vem 3 vemcmd show card info
Card UUID type  0: 4908a717-7d86-d28b-7d69-001a64635d18
Card name: sfish-srvr-7
Switch name: N1000v
Switch uuid: 50 84 06 50 81 36 4c 22-9b 4e c5 3e 1f 67 e5 ff
Card domain: 11
Card slot: 12
Control VLAN MAC: 00:02:3d:10:0b:0c
Inband MAC: 00:02:3d:20:0b:0c
SPAN MAC: 00:02:3d:30:0b:0c
USER DPA MAC: 00:02:3d:40:0b:0c
Management IP address: 172.28.30.56
Max physical ports: 16
Max virtual ports: 32
Card control VLAN: 3002
Card packet VLAN: 3003
```

Step 2 On the VSM, use the following command to verify the module number to which the corresponding UUID entry is mapped.

show server_info

Example:

```
n1000v# show server_info
Mod     Status          UUID
---     -----------     ----
13      absent          4908a717-7d86-d28b-7d69-001a64635d18
```

Step 3 Using the module number from Step 2, collect the output of the following commands:

- **show platform internal event-history module 13**
- **show module internal event-history module 13**
- **show system internal im event-history module 13**

- **show system internal vmm event-history module 13**
- **show system internal ethpm event-history module 13**

Note If you need to contact Cisco TAC for assistance in resolving an issue, you will need the output of the commands listed in Step 3.

Commands

Use the following commands to troubleshoot bringing the VSM module into service:

- **show svs neighbors** – to show all svs neighbors
- **show platform internal event-history module** – to display platform manager module state machines

Use the following commands to troubleshoot problems with the VSM:

- **show platform internal event-history module** *module-number*
- **show module internal event-history module** *module-number*
- **show system internal im event-history module** *module-number*
- **show system internal vmm event-history module** *module-number*
- **show system internal ethpm event-history module** *module-number*
- **show system internal ethpm event-history int** *type slot*