



VSM and VSE Modules

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

- [Information About Modules, page 7-1](#)
- [Troubleshooting a Module Not Coming Up on the VSM, page 7-1](#)
- [Problems with the VSM, page 7-4](#)
- [VSM and VSE Troubleshooting Commands, page 7-14](#)

Information About Modules

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

The Cisco Nexus 1000VE implementation has two parts:

- **Virtual Supervisor Module (VSM)**—Control software of the Cisco Nexus 1000VE distributed virtual switch. It runs on a virtual machine (VM) and is based on NX-OS software.
- **Virtual Service Engine (VSE)**—Part of the Cisco Nexus 1000VE that actually switches data traffic. It runs as a VM on a VMware ESX host. Several VSEs are controlled by one VSM. All the VSEs 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 includes the following topics:

- [Guidelines for Troubleshooting Modules, page 7-2](#)
- [Flowchart for Troubleshooting Modules, page 7-3](#)
- [Verifying the VSM Is Connected to vCenter Server, page 7-6](#)
- [Verifying Internal Port Group \(IPG\) Information, page 7-8](#)
- [Verifying the VSM Is Configured Correctly, page 7-9](#)
- [Checking the vCenter Server Configuration, page 7-10](#)
- [Checking Network Connectivity Between the VSM and the VSE, page 7-11](#)

- [Checking the VSM Configuration, page 7-12](#)
- [Collecting Logs, page 7-13](#)

Guidelines for Troubleshooting Modules

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

- You must have a VSE VM and a VSM up and running.
- Make sure that you are running compatible versions of vCenter Server and VSM.
For more information, see the [Cisco Nexus 1000VE Compatibility Information](#).
- To verify network connectivity between the VSM and vCenter Server, ping the IP address of vCenter Server. If you are using a domain name service (DNS) name, use the DNS name in the ping. If a ping to vCenter Server fails, check to see if you can ping the gateway. Otherwise, check the mgmt0 interface configuration settings.
- Make sure that the firewall settings are OFF on the vCenter Server. If you want the firewall settings, and 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 verify that the extension or plugin was created, see the [“Finding the Extension Key on the Cisco Nexus 1000VE” section on page 3-6](#).

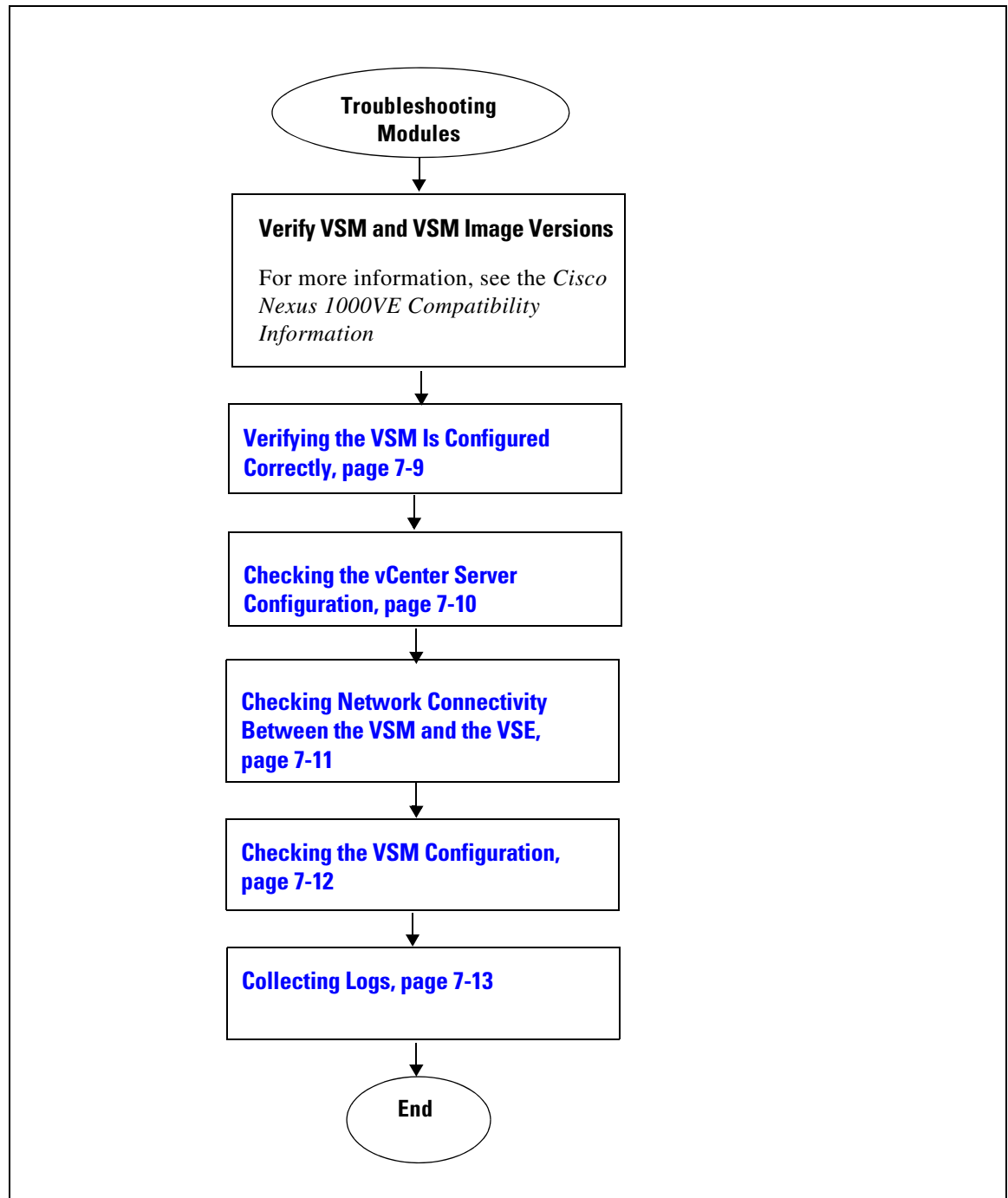
For more information about extension keys or plugins, see the [“Managing Extension Keys” section on page 3-5](#).

- If you see the following error, see the [“Checking the vCenter Server Configuration” section on page 7-10](#).
 - ERROR: Datacenter not found
- For a list of terms used with the Cisco Nexus 1000VE, see the [Cisco Nexus 1000V Getting Started Guide](#).

Flowchart for Troubleshooting Modules

Use the following flowchart to troubleshoot modules.

Flowchart: Troubleshooting Modules



Problems with the VSM

The following are symptoms, possible causes, and solutions for problems with the VSM.

Symptom	Possible Causes	Solution
<p>You see the following error on the VSM:</p> <pre>ERROR: [VMware vCenter Server 4.0.0 build-150489] Extension key was not registered before its use</pre>	A extension or plug-in was not created for the VSM.	<ol style="list-style-type: none"> 1. Verify that the extension or plugin was created. “Finding the Extension Key Tied to a Specific DVS” procedure on page 3-7 2. If the plug-in is not found, create one using the following procedure in the <i>Cisco Nexus 1000V Getting Started Guide</i>: Creating a Cisco Nexus 1000VE Plug-In on the vCenter Server
<p>Following a reboot of the VSM, the system stops functioning in one of the following states and does not recover on its own. Attempts to debug fail.</p>		
<p>After boot, VSM is in loader prompt.</p>	Corrupt VSM kickstart image.	<ol style="list-style-type: none"> 1. Boot the VSM from the CD ROM. 2. From the CD Boot menu, choose Option 1, Install Nexus1000ve and bring up new image. Follow the VSM installation procedure.
	Boot variables are not set.	<ol style="list-style-type: none"> 1. Boot the VSM from the CD ROM. 2. From the CD Boot menu, choose Option 3, Install Nexus1000ve only if the disk unformatted and bring up new image. 3. Set the boot variables used to boot the VSM: boot system bootflash:system-boot-variable-name boot kickstart bootflash:kickstart-boot-variable-name 4. Reload the VSM. reload
<p>After boot, VSM is in boot prompt.</p>	Corrupt VSM system image.	<ol style="list-style-type: none"> 1. Boot the VSM from the CD ROM. 2. From the CD Boot menu, choose Option 1, Install Nexus1000ve and bring up new image. 3. Follow the VSM installation procedure.

Symptom	Possible Causes	Solution
After boot, VSM is reconfigured.	Startup configuration is deleted.	<p>Do one of the following:</p> <ul style="list-style-type: none"> If you have a saved backup copy of your configuration file, restore the configuration on the VSM. copy source filesystem: filename system:running-config If not, reconfigure the VSM using the following section in the <i>Cisco Nexus 1000V Getting Started Guide</i>: Setting Up the Software
After boot, VSM is stopped at “Loader Loading.”	Corrupt boot menu file.	<ol style="list-style-type: none"> Boot the VSM from the CD ROM. From the CD Boot menu, choose Option 3, Install Nexus1000ve only if the disk unformatted and bring up new image. Do one of the following: <ul style="list-style-type: none"> If you have a saved backup copy of your configuration file, restore the configuration on the VSM. copy source filesystem: filename system:running-config If not, reconfigure the VSM using the following section in the <i>Cisco Nexus 1000V Getting Started Guide</i>: Setting Up the Software
After boot, the secondary VSM reboots continuously.	Control VLAN or control interface down	Check control connectivity between the active and the standby VSM.
	Active and standby VSMs fail to synchronize.	<p>From the active VSM, check system manager errors to identify which application caused the failure.</p> <p>show system internal sysmgr event-history errors</p> <p>show logging</p>

Verifying the VSM Is Connected to vCenter Server

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

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

show svcs connections

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

Example:

```
switch# show svcs connections
connection vc:
  hostname: -
  ip address: 172.23.43.170
  ipv6 address: -
  remote port: 80
  transport type: ipv4
  vrf: management
  protocol: vmware-vim https
  certificate: default
  datacenter name: hamilton-DC
  admin:
  max-ports: 12000
  extension key: Cisco_Nexus_1000V_342482929
  DVS uuid: 50 12 e0 5d 1c 63 22 76-7b 77 69 b7 27 dc 0c 2e
  dvs version: 5.0.0
  config status: Enabled
  operational status: Connected
  sync status: Complete
  version: VMware vCenter Server 6.5.0 build-4602587
  vc-uuid: d06e96b6-55e7-4cf8-9f85-511b4bdafe06
  ssl-cert: self-signed or not authenticated
switch#
```

This output indicates the ipg created

```
1. ng-vsm# sh ipg-info
-----
Name VlanId PortGroupKey
-----
~ipg47 47 dvportgroup-1469
~ipg3 3 dvportgroup-1425
~ipg2058 2058 dvportgroup-1484
~ipg4 4 dvportgroup-1426
~ipg2059 2059 dvportgroup-1485
~ipg5 5 dvportgroup-1427
~ipg6 6 dvportgroup-1428
~ipg7 7 dvportgroup-1429
~ipg43 43 dvportgroup-1465
~ipg8 8 dvportgroup-1430.....

****IPG Creation is complete****
```

The output indicate the IPG range

```
ng-vsm# sh dc clusters
Global Internal IPG tags:
inside-trunk 1:1-50,
inside-trunk 2:2047-2096,
Cluster DefaultCluster free IPG tags:
```

```

inside-trunk 1:1-50,
inside-trunk 2:2047-2096,
Cluster DefaultCluster used IPG tags:
inside-trunk 1:,
inside-trunk 2:,
ng-vsm#

```

Step 2 Do one of the following:

- If the status is **Connected**, return to the “[Flowchart: Troubleshooting Modules](#)” section on page 7-3.
- If not, continue with the next step.

Step 3 Connect to vCenter Server.

config t

svs connection *connection_name*

connect

Example:

```

switch# conf t
switch(config)# svs connection HamiltonDC
switch(config-svs-conn)# connect
ERROR: [VMWARE-VIM] Extension-key/username-password pair needs to be configured before
connect
switch# register-plugin remote username XXX password XXX

```

Step 4 Do one of the following:

- If you see an error message about the username-password or extension key, continue with the next [Step 8](#).
- If you see an error indicating that the DVS already exists in the show vms internal error output, go to [Step 8](#).
- If there are no errors, go to [Step 8](#).

Step 5 Do the following:

- Unregister the extension key using the “[Unregistering the Extension Key in the vCenter Server](#)” section on page 3-11.
- If the vCenter's login credentials were used to create NIKVE DVS, go to Step 6, else go to Step 7.

Step 6 Use the **remote username** CLI to provide vCenter credentials to the VSM and go to Step 9.

Example

```

switch# conf t
switch# svs connection HamiltonDC
switch (config-svs-conn)# remote username administrator@vsphere.local password Abcd@1234

```

Step 7 Use the **register-plugin** CLI to register VSM extension key with the vCenter and go to Step 9.

```

switch# conf t
switch# svs connection HamiltonDC
switch (config-svs-conn)# register-plugin remote username administrator@vsphere.local
password Abcd@1234

```

Step 8 Use the **vmware dvs** CLI to provide the UUID and datacenter name of the existing DVS. The DVS UUID can be obtained by pointing your web browser to <https://your-vCenter-IP/mob> and then navigating to the VmwareDistributedVirtualSwitch object corresponding to your DVS.

```

switch# conf t
switch# svs connection HamiltonDC
switch (config-svs-conn)# vmware dvs uuid "50 12 e0 5d 1c 63 22 76-7b 77 69 b7 27 dc 0c
2e" datacenter-name hamilton-dc

```

Step 9 Verify the connection between the VSM and vCenter Server.

show svcs connections

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

Example:

```
switch# show svcs connections
connection vc:
  hostname: -
  ip address: 172.23.43.170
  ipv6 address: -
  remote port: 80
  transport type: ipv4
  vrf: management
  protocol: vmware-vim https
  certificate: default
  datacenter name: hamilton-DC
  admin:
  max-ports: 12000
  extension key: Cisco_Nexus_1000V_342482929
  DVS uuid: 50 12 e0 5d 1c 63 22 76-7b 77 69 b7 27 dc 0c 2e
  dvs version: 5.0.0
  config status: Enabled
  operational status: Connected
  sync status: Complete
  version: VMware vCenter Server 6.5.0 build-4602587
  vc-uuid: d06e96b6-55e7-4cf8-9f85-511b4bdafe06
  ssl-cert: self-signed or not authenticated
switch#
```

Step 10 Do one of the following:

- If the status is **Connected**, you have completed this procedure.
- If not, return to the [“Flowchart: Troubleshooting Modules”](#) section on page 7-3.

Verifying Internal Port Group (IPG) Information

You can verify the information about the internal group (IGP).

BEFORE YOU BEGIN

- Log in to the CLI in EXEC mode.

Step 1 On the VSM, verify the IPG configuration.

This command helps in checking if the IPG was created on the VC.

show ipg-info

```
switch# sh ipg-info
-----
Name VlanId PortGroupKey
-----
~ipg47 47 dvportgroup-1469
~ipg3 3 dvportgroup-1425
~ipg2058 2058 dvportgroup-1484
~ipg4 4 dvportgroup-1426
```



```
~ipg2059 2059 dvportgroup-1485
~ipg5 5 dvportgroup-1427
~ipg6 6 dvportgroup-1428
~ipg7 7 dvportgroup-1429 .....
****IPG Creation is complete****
```

Verifying the VSM Is Configured Correctly

This section includes the following topics:

- [Verifying the Domain Configuration, page 7-9](#)
- [Verifying the System Port Profile Configuration, page 7-10](#)

Verifying the Domain Configuration

You can verify the domain configuration.

BEFORE YOU BEGIN

- Log in to the CLI in EXEC mode.
- Verify that the output of the show **svs domain** command indicates 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:

```
switch# show svs domain
SVS domain config:
Domain id: 888
Control vlan: NA
Packet vlan: NA
L2/L3 Control mode: L3
Switch guid: 3a452e9b-a777-4a1f-ab28-c7312399a9a8
L3 control interface: mgmt0
Status: Config push to Management Server successful.
Control type multicast: No
L3Sec Status: Enabled
```

Note: Control VLAN and Packet VLAN are not used in L3 mode
switch#

Verifying the System Port Profile Configuration

You can verify the port profile configuration.

BEFORE YOU BEGIN

- Log in to the CLI in EXEC mode.
- Verify that the output of the **show port-profile name** command indicates the following:
 - The control and packet VLANs are assigned.
 - The port profile is enabled.
 - If you have configured a non-default system MTU setting, check that it is the correct size.

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

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

Example:

```
switch# show port-profile name SystemUplink
port-profile SystemUplink
  description:
  type: ethernet
  status: enabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: 114,115
  port-group: SystemUplink
  max ports: 32
  inherit:
  config attributes:
    switchport mode trunk
    switchport trunk allowed vlan all
    system mtu 1500
    no shutdown
  evaluated config attributes:
    switchport mode trunk
    switchport trunk allowed vlan all
    no shutdown
  assigned interfaces:
```

Checking the vCenter Server Configuration

You can verify the configuration on vCenter Server.

-
- Step 1** Confirm that the host is added to the data center and the Cisco Nexus 1000VE DVS in that data center.
 - Step 2** Confirm that at least one pnics of the server that hosts the VSE is assigned to uplink portgroup on external vDS.
 - Step 3** Confirm that the three VSM vnics are assigned to the port groups that contain the control VLAN, packet VLAN, and management network.
-

Checking Network Connectivity Between the VSM and the VSE

You can verify the network connectivity between the VSM and the VSE.

Step 1 On the VSM, find its MAC address.

show svcs neighbors

The VSM MAC address displays as the AIPC Interface MAC.

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

Example:

```
switch# show svcs neighbors
```

```
Active Domain ID: 1030
```

```
AIPC Interface MAC: 0050-568e-58b7
```

```
inband/outband Interface MAC: 0050-568e-2a39
```

Src MAC	Type	Domain-id	Node-id	Last learnt (Sec. ago)
0002-3d44-0602	VSM	1024	0302	261058.59

Step 2 Do one of the following:

- If the output of the **show svcs neighbors** command in [Step 1](#) does not display the VSM MAC address, 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 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

```
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

```
Active Supervisor:
```

```
* 3002 00:02:3d:40:0b:0c dynamic Yes 0 Gi3/2
```

Step 4 Do one of the following:

- If the output from [Step 3](#) 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 5 Do one of the following:

- If the MAC address of the VSM does not appear in the output of [Step 3](#), check the VSM configuration as explained in “[Checking the VSM Configuration](#)” section on page 7-12.
- Otherwise, you have completed this procedure.

Checking the VSM Configuration

You can verify that the ESX host received the VSM configuration and setup.

Step 1 On the VSE, On the VSE, verify that the vemfwd and the vssdpa processes are running.

systemctl status nexus1000v

Example:

```
cisco-vse:~# systemctl status nexus1000v
? nexus1000v.service - Cisco Nexus 1000V VSE
Loaded: loaded (/usr/lib/systemd/system/nexus1000v.service; enabled; vendor preset:
disabled)
Active: active (running) since Sat 2018-06-30 00:41:11 PDT; 1 weeks 2 days ago
Process: 25378 ExecStop=/opt/cisco/nlkv/scripts/nlkv stop (code=exited, status=0/SUCCESS)
Main PID: 25411 (nlkv)
CGroup: /system.slice/nexus1000v.service
+-25411 /bin/bash /opt/cisco/nlkv/scripts/nlkv start
+-25475 /sbin/vemfwd -c 1 -- -p 7
--config="(0,0,0),(0,1,0),(1,0,0),(1,1,0),(2,0,0),(2,1,0)" --txq-per-port=4
+-25576 /sbin/vssdpa-proto.bin -f
```

Step 2 Verify that the domain ID and the other parameters are configured correctly on the VSE.

vemcmd show card

Example:

```
~ # vemcmd show card
Card UUID type 2: 58f8afd7-e1e3-3c51-85e2-6e6f2819a7b8
Card name: sfish-srvr-1
Switch name: switch
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
VSM Control (Control VLAN) MAC: 00:02:3d:14:00:03
VSM Packet (inband/outband) MAC: 00:02:3d:24:00:03
VSM Control Agent (DPA) MAC: 00:02:3d:44:00:03
VSM 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 3** 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     1    Access 120
9     0         3969   0     2      2            VIRT  UP     UP     1    Access 121
10    0         3002   0     2      2            VIRT  UP     UP     1    Access 122
11    0         3968   0     2      2            VIRT  UP     UP     1    Access 123
12    0         3003   0     2      2            VIRT  UP     UP     1    Access 124
13    0         1       0     2      2            VIRT  UP     UP     0    Access 125
14    0         3967   0     2      2            VIRT  UP     UP     1    Access 126
16    1a030100   1 T    0     2      2            PHYS  UP     UP     1    Trunk  vmnic1
```

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

- Step 4** Verify 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:
  10 122
  16 vmnic1
~ # vemcmd show bd 3003
BD 3003, vdc 1, vlan 3003, 2 ports
Portlist:
  12 124
  16 vmnic1
```

Collecting Logs

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

- Step 1** On the VSM, verify its UUID.

vemcmd show card info

Example:

```
~ # vemcmd show card info
Card UUID type 0: 4908a717-7d86-d28b-7d69-001a64635d18
Card name: sfish-srvr-7
Switch name: switch
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/outband 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, verify the module number to which the corresponding UUID entry is mapped.

show module vse mapping

Example:

```

switch# show module vse mapping
Mod      Status          UUID                                     License Status
---      -
60       absent          33393935-3234-5553-4538-35314e355400  unlicensed
66       powered-up      33393935-3234-5553-4538-35314e35545a  licensed
switch#

```

Step 3 Using the module number from [Step 2](#), collect the output of the following commands:

- **show system internal vem_mgr 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](#).

VSM and VSE Troubleshooting Commands

You can use the commands in this section to troubleshoot problems related to VSM.

Command	Description
show svcs neighbors	Displays all neighbors. See Example 7-1 on page 7-16 .
show svcs connections	Displays the Cisco Nexus 1000VE connections. See Example 7-2 on page 7-16 .
show svcs domain	Displays the domain configuration. See Example 7-3 on page 7-16 .
show port-profile name <i>name</i>	Displays the configuration for a named port profile. See Example 7-4 on page 7-17 .

Command	Description
show running-config vlan <i>vlanID</i>	Displays the VLAN information in the running configuration. See Example 7-5 on page 7-17 .
show mac address-table interface	Displays the MAC address table on an upstream switch to verify the network configuration.
module vse <i>module_number</i>	Displays the VLAN configuration on the VSM to verify that the VSM MAC appears in the control and packet VLANs.
vemcmd show card	Displays information about cards on the VSM to verify that the domain ID, control VLANs, and packet VLANs are configured correctly on the host. See Example 7-7 on page 7-17 .
vemcmd show port [<i>port-LTL-number</i>]	Displays information about ports on the VSM 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. See Example 7-8 on page 7-18 .
vemcmd show bd [<i>control_vlan_id</i> <i>packet_vlan_id</i>]	Displays configured information on the VSM to verify that the VM NIC port that is supposed to carry the control VLAN and packet VLAN is present. See Example 7-10 on page 7-18 .
vemcmd show trunk	Displays configured information on the VSM to verify that the DV port groups are successfully pushed from vCenter Server to the host and that the correct physical trunk port VM NIC is used. See Example 7-11 on page 7-19 .
show module vse mapping	Displays information about the VSM that a VSM maps to, including the VSM module number, status, UUID, and license status. See Example 7-12 on page 7-19 .
show system internal vem_mgr event-history <i>module 13 module-number</i>	Displays module FSM event information.
show module internal event-history <i>module module-number</i>	Displays the event log for a module.
show system internal im event-history <i>module module-number</i>	Displays the module IM event logs for the system.
show system internal vmm event-history <i>module module-number</i>	Displays the module VMM event logs for the system.
show system internal ethpm event-history <i>module module-number</i>	Displays the module Ethernet event logs for the system.
show system internal ethpm event-history int <i>type slot</i>	Displays the Ethernet interface logs for the system.

Example 7-1 show svcs neighbors Command

```
switch# show svcs neighbors

Active Domain ID: 113

AIPC Interface MAC: 0050-56b6-2bd3
inband/outband Interface MAC: 0050-56b6-4f2d

Src MAC           Type   Domain-id   Node-id   Last learnt (Sec. ago)
-----
0002-3d40-7102    VSM    113         0302     71441.12
0002-3d40-7103    VSM    113         0402     390.77

switch#
```

Example 7-2 show svcs connections Command

```
switch# show svcs connections
connection vc:
  hostname: -
  ip address: 172.23.43.170
  ipv6 address: -
  remote port: 80
  transport type: ipv4
  vrf: management
  protocol: vmware-vim https
  certificate: default
  datacenter name: hamilton-DC
  admin:
  max-ports: 12000
  extension key: Cisco_Nexus_1000V_342482929
  DVS uuid: 50 12 e0 5d 1c 63 22 76-7b 77 69 b7 27 dc 0c 2e
  dvs version: 5.0.0
  config status: Enabled
  operational status: Connected
  sync status: Complete
  version: VMware vCenter Server 6.5.0 build-4602587
  vc-uuid: d06e96b6-55e7-4cf8-9f85-511b4bdaf06
  ssl-cert: self-signed or not authenticated

switch#
```

Example 7-3 show svcs domain Command

```
switch# show svcs domain
SVS domain config:
Domain id: 888
Control vlan: NA
Packet vlan: NA
L2/L3 Control mode: L3
Switch guid: 3a452e9b-a777-4a1f-ab28-c7312399a9a8
L3 control interface: mgmt0
Status: Config push to Management Server successful.
Control type multicast: No
L3Sec Status: Enabled
```

Note: Control VLAN and Packet VLAN are not used in L3 mode
switch#

Example 7-4 show port-profile Command

```

switch# show port-profile name SystemUplink
port-profile SystemUplink
  description:
  type: ethernet
  status: enabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: 114,115
  port-group: SystemUplink
  max ports: 32
  inherit:
  config attributes:
    switchport mode trunk
    switchport trunk allowed vlan all
    system mtu 1500
    no shutdown
  evaluated config attributes:
    switchport mode trunk
    switchport trunk allowed vlan all
    no shutdown
  assigned interfaces:

```

Example 7-5 show running-configuration vlan Command

```

switch# show running-config vlan 260-261
version 4.0(4)SV1(3)
vlan 260
  name cp_control
vlan 261
  name cp_packet

switch#

```

Example 7-6 VSM-health check Command

```

switch# VSM-health check
switch# show running-config vlan 220-221

version 5.2(1)SV5(1.1)
vlan 220-221
vlan 220
  name mgmt
vlan 221
  name system

switch#

```

Example 7-7 vemcmd show card Command

```

switch# vemcmd show card
Card UUID type 2: 58f8afd7-e1e3-3c51-85e2-6e6f2819a7b8
Card name: sfish-srvr-1
Switch name: switch
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
VSM Control (Control VLAN) MAC: 00:02:3d:14:00:03

```

```

VSM Packet (inband/outband) MAC: 00:02:3d:24:00:03
VSM Control Agent (DPA) MAC: 00:02:3d:44:00:03
VSM 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

```

Example 7-8 *vemcmd show port Command*

```

switch# vemcmd show port
switch# vemcmd show port
LTL VSM Port Admin Link State PC-LTL SGID Vem Port Type ORG svcpath Owner
21 Eth3/1 UP UP F/B* 0 eth1 0 0 dpdk-outside
53 Veth2 UP UP FWD 0 test-vm1.eth1 0 0 test-vm1
54 Veth1 UP UP FWD 0 test-vm2.eth1 0 0 test-vm2

* F/B: Port is BLOCKED on some of the vlans.
One or more vlans are either not created or
not in the list of allowed vlans for this port.
Please run "vemcmd show port vlans" to see the details.
switch#::~$

```

Example 7-9 *vemcmd show port vlans Command*

```

switch# vemcmd show port vlans
switch# vemcmd show port vlans
Native VLAN Allowed
LTL VSM Port Mode VLAN State* Vlans
21 Eth3/1 T 1 FWD 220-229
53 Veth2 A 222 FWD 222
54 Veth1 A 223 FWD 223

* VLAN State: VLAN State represents the state of allowed vlans.
switch #

```



Note

The output *F/B The port is blocked on some of the VLANs means that the trunk is not forwarding all VLANs. This might be a normal situation depending on the port profile allowed VLAN list. Compare the output of the **vemcmd show port vlans** command against the port profile trunk allowed VLANs. If the lists match, all of the expected VLANs are forwarding and the Cisco Nexus 1000VE is blocking nonallowed VLANs.

Example 7-10 *vemcmd show vlan Command*

```

switch# vemcmd show vlan
switch# vemcmd show vlan 222
VLAN 222, vdc 1, swbd 222, hwbd 6, 2 ports

Portlist:
21 eth1
53 test-vm1.eth1

switch#

```

Example 7-11 vemcmd show trunk Command

```

switch# vemcmd show trunk
switch# vemcmd show trunk
Trunk port 6 native_vlan 1 CBL 1
vlan(1) cbl 1, vlan(3972) cbl 1, vlan(3970) cbl 1, vlan(3968) cbl 1, vlan(3971) cbl 1,
vlan(222) cbl 1, vlan(220) cbl 1, vlan(221) cbl 1, vlan(223) cbl 1, vlan(224) cbl 1,
vlan(225) cbl 1, vlan(226) cbl 1, vlan(227) cbl 1, vlan(228) cbl 1, vlan(229) cbl 1,
Trunk port 16 native_vlan 1 CBL 1
vlan(1) cbl 1, vlan(3972) cbl 1, vlan(3970) cbl 1, vlan(3968) cbl 1, vlan(3971) cbl 1,
vlan(222) cbl 1, vlan(220) cbl 1, vlan(221) cbl 1, vlan(223) cbl 1, vlan(224) cbl 1,
vlan(225) cbl 1, vlan(226) cbl 1, vlan(227) cbl 1, vlan(228) cbl 1, vlan(229) cbl 1,
Trunk port 21 native_vlan 1 CBL 0
vlan(222) cbl 1, vlan(220) cbl 1, vlan(221) cbl 1, vlan(223) cbl 1, vlan(224) cbl 1,
vlan(225) cbl 1, vlan(226) cbl 1, vlan(227) cbl 1, vlan(228) cbl 1, vlan(229) cbl 1,
switch#

```

Example 7-12 show module vse mapping Command

```

switch# show module vse mapping
Mod      Status           UUID                               License Status
---      -
60       absent           33393935-3234-5553-4538-35314e355400  unlicensed
66       powered-up       33393935-3234-5553-4538-35314e35545a  licensed
switch#

```

Example 7-13 show ipg-info

```

switch# show ipg-info
Desc : shows internal port-group info created on VC

```

```

-----
Name      VlanId    PortGroupKey
-----
~ipg47    47        dvportgroup-1469
~ipg3     3         dvportgroup-1425
~ipg2058  2058     dvportgroup-1484
~ipg4     4         dvportgroup-1426
~ipg2059  2059     dvportgroup-1485
~ipg5     5         dvportgroup-1427
~ipg6     6         dvportgroup-1428
~ipg7     7         dvportgroup-1429
~ipg43    43        dvportgroup-1465
~ipg8     8         dvportgroup-1430
~ipg2070  2070     dvportgroup-1496
~ipg1     1         dvportgroup-1423
~ipg2     2         dvportgroup-1424
~ipg46    46        dvportgroup-1468
~ipg9     9         dvportgroup-1431
~ipg2071  2071     dvportgroup-1497
~ipg10    10        dvportgroup-1432
~ipg2068  2068     dvportgroup-1494
~ipg11    11        dvportgroup-1433
~ipg2069  2069     dvportgroup-1495
~ipg2084  2084     dvportgroup-1510
~ipg12    12        dvportgroup-1434
~ipg2066  2066     dvportgroup-1492
~ipg2056  2056     dvportgroup-1482
~ipg2057  2057     dvportgroup-1483

```

~ipg2065	2065	dvportgroup-1491
~ipg15	15	dvportgroup-1437
~ipg2067	2067	dvportgroup-1493
~ipg13	13	dvportgroup-1435
~ipg2072	2072	dvportgroup-1498
~ipg50	50	dvportgroup-1472
~ipg2073	2073	dvportgroup-1499
~ipg2095	2095	dvportgroup-1521
~ipg2074	2074	dvportgroup-1500
~ipg2075	2075	dvportgroup-1501
~ipg2076	2076	dvportgroup-1502
~ipg2077	2077	dvportgroup-1503
~ipg2078	2078	dvportgroup-1504
~ipg19	19	dvportgroup-1441
~ipg2079	2079	dvportgroup-1505
~ipg18	18	dvportgroup-1440
~ipg2080	2080	dvportgroup-1506
~ipg21	21	dvportgroup-1443
~ipg2081	2081	dvportgroup-1507
~ipg20	20	dvportgroup-1442
~ipg2082	2082	dvportgroup-1508
~ipg2083	2083	dvportgroup-1509
~ipg44	44	dvportgroup-1466
~ipg45	45	dvportgroup-1467
~ipg48	48	dvportgroup-1470
~ipg49	49	dvportgroup-1471
~ipg26	26	dvportgroup-1448
~ipg27	27	dvportgroup-1449
~ipg28	28	dvportgroup-1450
~ipg29	29	dvportgroup-1451
~ipg30	30	dvportgroup-1452
~ipg31	31	dvportgroup-1453
~ipg32	32	dvportgroup-1454
~ipg14	14	dvportgroup-1436
~ipg16	16	dvportgroup-1438
~ipg17	17	dvportgroup-1439
~ipg33	33	dvportgroup-1455
~ipg34	34	dvportgroup-1456
~ipg35	35	dvportgroup-1457
~ipg36	36	dvportgroup-1458
~ipg37	37	dvportgroup-1459
~ipg38	38	dvportgroup-1460
~ipg22	22	dvportgroup-1444
~ipg23	23	dvportgroup-1445
~ipg24	24	dvportgroup-1446
~ipg25	25	dvportgroup-1447
~ipg39	39	dvportgroup-1461
~ipg40	40	dvportgroup-1462
~ipg41	41	dvportgroup-1463
~ipg2055	2055	dvportgroup-1481
~ipg2060	2060	dvportgroup-1486
~ipg2047	2047	dvportgroup-1473
~ipg2061	2061	dvportgroup-1487
~ipg2062	2062	dvportgroup-1488
~ipg2063	2063	dvportgroup-1489
~ipg2064	2064	dvportgroup-1490
~ipg42	42	dvportgroup-1464
~ipg2048	2048	dvportgroup-1474
~ipg2049	2049	dvportgroup-1475
~ipg2050	2050	dvportgroup-1476
~ipg2051	2051	dvportgroup-1477
~ipg2052	2052	dvportgroup-1478
~ipg2053	2053	dvportgroup-1479
~ipg2054	2054	dvportgroup-1480

```

~ipg2085      2085      dvportgroup-1511
~ipg2086      2086      dvportgroup-1512
~ipg2087      2087      dvportgroup-1513
~ipg2088      2088      dvportgroup-1514
~ipg2089      2089      dvportgroup-1515
~ipg2090      2090      dvportgroup-1516
~ipg2091      2091      dvportgroup-1517
~ipg2092      2092      dvportgroup-1518
~ipg2093      2093      dvportgroup-1519
~ipg2094      2094      dvportgroup-1520
~ipg2096      2096      dvportgroup-1522

```

```

****IPG Creation is complete****
show dc hosts vse

```

Example 7-14 show dc hosts vse

```

switch# show dc hosts vse
Desc: Show VSE IP and Host IP/Name mapping info

```

```

Internal IPG tags:
inside-trunk 1:1-50,
inside-trunk 2:2047-2096,
-----
HOST NAME: 10.197.148.227
HOST IP: 10.197.148.227
VSE IP: 202.1.1.227
VSE UUID : 564D5218-113F-3E4E-D034-E911AAC7FF0A
-----

```

Example 7-15 show vms internal info host-table

```

switch# show vms internal info host-table
Desc : Display host info which are added to N1KVE-VDS

```

```

Host Table:
-----
Lock acquired [0]
Hosts added/removed flag: [0]
Pending host filter update: [0]
Notification of hosts info pending flag: [0]
Hosts filter spec created flag: [1]
Hosts filter spec reference:
[session[5206c9d7-e0d5-68e6-9586-ffcc815e2b05]527d4768-76d4-578d-b382-08773e162514]
VC checkforupdate version: [19]
# of host entries = 256

Host Index = 2
Host entry flags = [OLD], [4]
Host info for slot no = 2
Module Number : 3
Host UUID: [b7371ff4-f03f-3c40-b2b7-049ee68fc8a9]
VSE UUID: [564D5218-113F-3E4E-D034-E911AAC7FF0A]
IPv4 address: [10.197.148.227], IPv6 address: [fe80::56a2:74ff:fe59:9b96], Hostname:
[10.197.148.227]
VSE IPv4 address: [202.1.1.227], VSE Hostname: [localhost.localdomain]
ref: [host-18]

```

```
Cluster mor: [domain-s16], Cluster name: [10.197.148.227]
```

Example 7-16 show vms internal info host-view

```
switch# show vms internal info host-view
```

```
Desc : Display all N1KVE port details from VC point of view
```

```
-----
Slot #2
-----
Host Name      : 10.197.148.227
Host Ref       : host-18
Host UUID      : b7371ff4-f03f-3c40-b2b7-049ee68fc8a9
Host VSE IP    : 202.1.1.227
Host Slot Num  : 2
Module Num     : 3
Host ID        : 1
Cluster ID     : 1
Host ID        : 1
Cluster ID     : 1
ipg_count for trunk 1 (1)
ipg_count for trunk 2 (1)
-----
List VM(s)
-----
VM Name        : App-3
VM Ref         : vm-25
VM UUID        : 42087cc1-8aa7-c511-81e7-6423cf483e84
VM Inst UUID   : 50082799-4901-f00e-49f7-9cd61d9913b1
VM ID          : 1
VM Host Id     : 1
VM ID          : 1
VM Host Id     : 1
-----
Adapter List
-----
State          : IPG allocated
MAC Address    : 00:50:56:88:44:59
Adapter Name   : Network adapter 1
Port Key       : Port-4000
DvPort        : Portgroup-356
VLAN TAG       : 1
Port-Group Name : vm-313
-----
State          : IPG allocated
MAC Address    : 00:50:56:88:52:d4
Adapter Name   : Network adapter 2
Port Key       : Port-4001
DvPort        : Portgroup-388
VLAN TAG       : 2047
Port-Group Name : vm-314
-----
```

Example 7-17 show vms internal info ipg-profile-mapping

```
switch# show vms internal info ipg-profile-mapping
```

```
Desc : Show mapping between internal port-group and port-profile
```

```
Cluster id : 1, Cluster_ref : DefaultCluster
```

```
IpgName ~ipg1 , Profile Id 8
IpgName ~ipg2047 , Profile Id 9
```

Example 7-18 show dc clusters

```
switch# show dc clusters
Desc : Show ipg info per cluster basis
```

```
Global Internal IPG tags:
inside-trunk 1:1-50,
inside-trunk 2:2047-2096,
Cluster DefaultCluster free IPG tags:
inside-trunk 1:2-50,
inside-trunk 2:2048-2096,
Cluster DefaultCluster used IPG tags:
inside-trunk 1:1,
inside-trunk 2:2047,
```

Example 7-19 show vms internal info cluster-view

```
switch# show vms internal info cluster-view
Desc : Show cluster info as well as show mapping between internal port-group and port-mac
```

```
-----
Cluster #1
-----
Cluster Id      : 1
Cluster Name    : DefaultCluster
Cluster sync_flag : 1
Cluster Ref     : DefaultCluster
Print the list of used cluster bits
1,

-----
Printing Mac address and ipg info of each cluster
-----

-----
Cluster Id: 1
Cluster Ref: DefaultCluster
-----
-----
~ipg          Mac-address
-----
~ipg1          00:50:56:88:44:59
~ipg2047       00:50:56:88:52:d4
```

Example 7-20 show vms internal info host-view module 3

```
switch# show vms internal info host-view module 3
Desc : Display all N1KVE port details on particular module from VC point of view
```

```
-----
Slot #2
-----
```

```

Host Name      : 10.197.148.227
Host Ref      : host-18
Host UUID     : b7371ff4-f03f-3c40-b2b7-049ee68fc8a9
Host VSE IP   : 202.1.1.227
Host Slot Num : 2
Module Num    : 3
Host ID       : 1
Cluster ID    : 1
Host ID       : 1
Cluster ID    : 1
ipg_count for trunk 1 (1)
ipg_count for trunk 2 (1)

```

List VM(s)

```

VM Name       : App-3
VM Ref        : vm-25
VM UUID       : 42087cc1-8aa7-c511-81e7-6423cf483e84
VM Inst UUID  : 50082799-4901-f00e-49f7-9cd61d9913b1
VM ID         : 1
VM Host Id    : 1
VM ID         : 1
VM Host Id    : 1

```

Adapter List

```

State         : IPG allocated
MAC Address   : 00:50:56:88:44:59
Adapter Name  : Network adapter 1
Port Key      : Port-4000
DvPort        : Portgroup-356
VLAN TAG      : 1
Port-Group Name : vm-313

```

```

State         : IPG allocated
MAC Address   : 00:50:56:88:52:d4
Adapter Name  : Network adapter 2
Port Key      : Port-4001
DvPort        : Portgroup-388
VLAN TAG      : 2047
Port-Group Name : vm-314

```

Example 7-21 show vms internal info ipg-duplicate

Desc : Show any duplicate internal port-group assigned to multiple ports per cluster

Cluster DefaultCluster: