CHAPTER 5

Troubleshooting Module Issues

This chapter describes how to troubleshoot various issues that could occur while Cisco VSG is communicating with the Virtual Supervisor Module (VSM), Virtual Ethernet Module (VEM), Cisco Prime Network Services Controller (Prime NSC), or Hyper-V Server.

This chapter includes the following sections:

Troubleshooting Cisco VSG and VSM Interactions

This section describes how to troubleshoot issues with the Cisco VSG and VSM interactions.

The port profile used to bring up the data interface of the Cisco VSG should not have any vn service or org configured.

This example shows how to use a port profile to bring up the Cisco VSG data interface:

```
vsm# show port-profile name vsg-data
port-profile vsg-data
 type: Vethernet
 description:
 status: enabled
 max-ports: 32
 inherit:
 config attributes:
  switchport mode access
  switchport access vlan 754
  no shutdown
 evaluated config attributes:
  switchport mode access
  switchport access vlan 754
  no shutdown
 assigned interfaces:
  Vethernet4
  Vethernet6
 port-group: vsg-data
 system vlans: none
 capability l3control: no
 capability iscsi-multipath: no
 port-profile role: none
 port-binding: static
```

Make sure that you add the Cisco VSG service VLAN and HA VLAN as part of the allowed VLAN. Without adding this information into the allowed VLAN, Cisco VSGs may not pair. If you have a Cisco VSG on one VEM and the VMs to be firewalled are on another VEM, you must make sure that the Cisco VSG service VLAN is added as the allowed VLAN.

This example shows how to display the VLAN configurations:

```
vsm# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
501  VLAN0501                         active    Po1, Po2, Po3, Po4, Veth3
```

For the port profiles that are used to protect the VMs, make sure that you provide the correct vn service IP (the exact data 0 IP address of the Cisco VSG), and the service VLAN and the security profile name. Make sure that the tenant name is configured correctly under the org, for example, root/Tenant-cisco.

Troubleshooting Cisco VSG and VEM Interactions

This section describes how to troubleshoot issues with Cisco VSG and VEM interactions.

This section includes the following topics:

- Policies Configured on the Cisco VSG that Are Not Effective, page 5-2
- Traffic Fails to Reach Destination with a Permit Policy Configured on Cisco VSG, page 5-3
- Policy Decision Inconsistent with Port Profile Changes, page 5-4
- Using vPath Ping to Determine Connectivity, page 5-4

Policies Configured on the Cisco VSG that Are Not Effective

Sometimes, when policies are configured on Cisco VSG and the data traffic is sent from the VMs, traffic flows through the Cisco Nexus 1000V Series Switch as if the firewall service is not enabled on the port.

Possible reason:

- VMs are not bound to the proper port profiles.

Verifications:

Go to the prompt to execute the vemcmd commands, for example, `cd \\Program File(x86)\Cisco\Nexus1000V` and do the following:

- Check if the VMs to be protected are bound to proper port profiles. The port profiles are expected to have the org/vn-service identified.
- On the VEM, enter the **vemcmd show vsn binding** command to check if the VM is protected by the firewall.
- To get the lower threshold limit (LTL) of the VM on the VEM, enter the **vemcmd show port** command as follows:

  ```
  vem# vemcmd show port | Select-String w2k-client_110.eth2 <--- VM name
  50 Veth5 UP UP FWD 0 w2k-client_110.eth2
  ```

  Verify if the LTL is found as follows:

```
vem# vemcmd show vsn binding
VSG Services Enabled  | VSG Licenses Available   2 <--- should be nonzero
LTL PATH VSN  SWBD     IP      P-TYPE  P-ID
50     1   1   101  10.1.1.230    1       3
```

The VSG Licenses Available message should display a nonzero value in the output.

Note All **vemcmd** commands can be executed by logging into the Hyper-V.

Traffic Fails to Reach Destination with a Permit Policy Configured on Cisco VSG

When policies are configured on the Cisco VSG to permit a certain type of traffic, but the traffic does not reach the destination, a complete failure can result.

Possible reason:

The Virtual Ethernet Modules (VEMs) have not learned the MAC address of the Cisco VSG.

Verifications:

Check if the Cisco VSG MAC address is learned on all the VEMs that host the protected VMs involved in the communication by entering the **vemcmd show L2 all** command on the VEM.

This example shows how to display the Cisco VSG MAC configuration:

```
VEM>vemcmd show L2 all
Bridge domain 6 brtmax 4096, brtcnt 6, timeout 300
VLAN 576, swbd 576, ""
Flags: P - PVLAN S - Secure D - Drop
Type MAC Address LTL timeout Flags PVLAN
Dynamic 00:1e:bd:45:5f:00 17 48
Dynamic 00:1d:d8:b7:1c:12 17 2
Dynamic 00:1d:d8:b7:1c:11 17 6
Static 00:1d:d8:b7:1c:31 52 0
Static 00:15:5d:48:da:2b 51 0
Static 00:15:5d:48:da:31 50 0
```

To troubleshoot, you should manually check if the VSG service (data 0) interface is bound to the correct port profile and VLAN configured.

You can check the Cisco VSG service interface assignment on the VEM by entering the **vemcmd show** command.

This example shows how to check the Cisco VSG service interface assignment on the VEM:

```
vem# vemcmd show vlan 576
VLAN 576, vdc 1, swbd 576, hwbd 6, 3 ports
Portlist:
Multicast Group Table:Group 0.0.0.0 Multicast LTL 4413305
```

You can display the port profile that is associated with the Cisco VSG service interface by entering the **show port-profile name** *pp-name* command on the VSM.

If the Cisco VSG is bound to the proper port profile and has the correct service VLAN, check the upstream switches. Ensure that this service VLAN is configured across all ports in all upstream switches to which all the VEMs (those talking to Cisco VSG) are connected.

You can ensure that the service VLAN is configured and enabled (active) on the VSM by entering the **show vlan** command.

This example shows how to display the VLAN configurations:

```
vsm# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
501  VLAN0501                         active    Po1, Po2, Po3, Po4, Veth3
```

Policy Decision Inconsistent with Port Profile Changes

When policy decisions are inconsistent with port-profile changes, either of these conditions can exist:

- A user changed the port profile of the traffic VM from one Cisco VSG port profile to another (having a different security profile).
- A policy is modified and the newer policy does not take immediate effect.

Reason:

Because of the existing flows, the old policy decision is continued.

Action:

Administrators must clear the flows in the vPath and Cisco VSG when the policy is modified.

Using vPath Ping to Determine Connectivity

You can use the vPath **ping** command on VSM to determine the connectivity between the Cisco VSG and the VEM.

This example shows how to ping the Cisco VSG connections and determine if they are reachable:

```
VSM-1# ping vsn all src-module all
VSM1# ping vsn all src-module all
ping vsn 192.161.0.85 vlan 0 from module 3 4, seq=0 timeout=1-sec
module(usec) : 3(0) 4(0)

ping vsn 192.161.0.85 vlan 0 from module 3 4, seq=1 timeout=1-sec
module(usec) : 3(0) 4(0)

ping vsn 192.161.0.85 vlan 0 from module 3 4, seq=2 timeout=1-sec
module(usec) : 3(0) 4(0)

ping vsn 192.161.0.85 vlan 0 from module 3 4, seq=3 timeout=1-sec
module(usec) : 3(0) 4(0)
```

This example shows how to display VSN ping options:

```
VSM-1# ping vsn ?
  all   All VSNs associated to VMs
  ip    IP Address
  vlan  VLAN Number
```

This example shows how to display VSN ping options for all source modules:

```
VSM-1# ping vsn all src-module ?
  <3-66>     Module number
  all        All modules in VSM
  vpath-all  All modules having VMs associated to VSNs
```

This example shows how to set up a ping for all source modules from a specified IP address:

```
VSM-1# ping vsn ip 10.1.1.60 src-module all
ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=0 timeout=1-sec
  module(usec)   :  4(301)  5(236)
  module(failed) :  7(VSN ARP not resolved)

ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=1 timeout=1-sec
  module(usec)   :  4(241)  5(138)  7(270)

ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=2 timeout=1-sec
  module(usec)   :  4(230)  5(155)  7(256)

ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=3 timeout=1-sec
  module(usec)   :  4(250)  5(154)  7(284)

ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=4 timeout=1-sec
  module(usec)   :  4(231)  5(170)  7(193)
```

This example shows to set up a ping for all vPath source modules for a specified IP address:

```
VSM-1# ping vsn ip 10.1.1.60 src-module vpath-all
ping vsn 10.1.1.60 vlan 501 from module 4 5, seq=0 timeout=1-sec
  module(usec)   :  4(223)  5(247)

ping vsn 10.1.1.60 vlan 501 from module 4 5, seq=1 timeout=1-sec
  module(usec)   :  4(206)  5(167)

ping vsn 10.1.1.60 vlan 501 from module 4 5, seq=2 timeout=1-sec
  module(usec)   :  4(241)  5(169)
```

This example shows how to set up a ping for all source modules of a specified IP address with a time-out and a count:

```
VSM-1# ping vsn ip 10.1.1.60 src-module all timeout 2 count 3
ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=0 timeout=2-sec
  module(usec)   :  4(444)  5(238)  7(394)

ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=1 timeout=2-sec
  module(usec)   :  4(259)  5(154)  7(225)

ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=2 timeout=2-sec
  module(usec)   :  4(227)  5(184)  7(216)
```

Troubleshooting VSM and Cisco Prime NSC Interactions

After registering the VSM to the Cisco Prime NSC, you can check the status of the VSM and Cisco Prime NSC policy agents by entering the **show nsc-pa status** command.

This example shows how to check the status:

```
vsm# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 3.2(1c)-vsm
```

If there is a failure, there can be several reasons. One failure could be because Cisco Prime NSC is unreachable or dead. Ping the Cisco Prime NSC IP to check for a response. If there is no response, look at the network connectivity.

Another reason could occur because of the wrong shared secret.

This example shows the results of this type of failure:

```
vsm# show nsc-pa status
NSC Policy-Agent status is - Installation Failure
```

```
Incorrect shared secret.
```

Provide the correct password and register again.

On the Cisco Prime NSC GUI, on the Resource Management > Resources > VSM tab, make sure that the registered VSM is shown as registered under the Status column.

On the Cisco Prime NSC GUI, make sure that the org is configured in the same way as in the port profile. Org should be configured properly on the port profile.

Troubleshooting Cisco VSG and Cisco Prime NSC Interactions

After registering the Cisco VSG to the Cisco Prime NSC, you can check the status by entering the **show nsc-pa status** command.

This example shows how to check the Cisco VSG registration status:

```
vsg# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(1e)-vsg
```

If there is a failure, there can be several reasons. One failure could be because Cisco Prime NSC is unreachable or dead. Ping the Cisco Prime NSC IP to check for a response. If there is no response, look at the network connectivity.

Another reason could occur because of the wrong shared secret.

This example shows how to display the results of this type of failure:

```
vsg# show nsc-pa status
NSC Policy-Agent status is - Installation Failure
Incorrect shared secret.
```

Provide the correct password and register again.

On the Cisco Prime NSC GUI, on the Resource Management > Resources > VSM tab, make sure that the registered VSG is shown as registered under the Status column.