CHAPTER 5

Troubleshooting Module Interactions

This chapter describes various problems that could happen while the Cisco VSG is communicating with the Virtual Supervisor Module (VSM), Virtual Ethernet Module (VEM), Cisco Virtual NeteworkManagement Center (VNMC), and the vCenter Server.

This chapter includes the following sections:

Troubleshooting 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 the port profile used 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
vsm#
```

Make sure that you add the Cisco VSG service VLAN and HA VLAN as part of the allowed VLAN under the uplink port profile. 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 under the uplink port profile.

The example output shows VLAN 753 and 754 are added as part of the trunk. The VLAN 751 is used for control (VSM), the VLAN 752 for packet, the VLAN 754 for the Cisco VSG service, and the VLAN 753 for the Cisco VSG high availability.

```
vsm# show port-profile name perf-uplink
port-profile perf-uplink
 type: Ethernet
 description:
 status: enabled
 max-ports: 32
 inherit:
 config attributes:
  switchport mode trunk
  switchport trunk allowed vlan 751-754
  no shutdown
 evaluated config attributes:
  switchport mode trunk
  switchport trunk allowed vlan 751-754
  no shutdown
 assigned interfaces:
  Ethernet3/4
  Ethernet4/4
 port-group: perf-uplink
 system vlans: 751-752
 capability l3control: no
 capability iscsi-multipath: no
 port-profile role: none
 port-binding: static
vsm#
```

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 under the org that you have configured the tenant name as "root/Tenant-cisco".

Troubleshooting Cisco VSG and VEM Interactions

This section describes commonly found problems with VSG and VEM interactions and ways to troubleshoot them.

This section includes the following topics:

Note All **vemcmd** commands can be executed by logging into the ESX via SSH.

Policies Configured on the Cisco VSG but Not Effective

Sometimes, when the policies are configured on the Cisco VSG and the data traffic is sent from the VMs, there is a passthrough behavior. Traffic flows through the Cisco Nexus 1000V switch as if the firewall service is not enabled on the port.

Possible reasons:

- VMs are not bound to the proper port profiles.
- The license is not available or is not installed/configured on the module.

Verifications:

- 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.
- Enter the **show vsg ip-binding** command on the Cisco VSG to see if the VM IP to service profile binding is present.
- Enter the **vemcmd show vsn binding** command on the VEM 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:

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

Verify if that LTL is found:

```
# vemcmd show vsn binding
VNS Enabled  | VNS Licenses Available   1      <--- should be nonzero
LTL   VSN  VLAN       IP         STATIC-MAC       LEARNED-MAC
50     1   501        10.1.1.61  00:00:00:00:00:00  00:50:56:9c:3c:c5
The Learned Mac should not be 00:00:00:00:00:00. It should be a valid mac.
#
```

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

Traffic Fails to Reach Destination with a Permit Policy Configured on the 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 is learned on all the VEMs that host the protected VMs involved in communication. On the VEM, enter the **vemcmd show vsn config** command.

This example shows the results of the command:

```
# vemcmd show vsn config
VNS Enabled | VNS Licenses Available 1
VSN# VLAN IP STATIC-MAC LEARNED-MAC LTLs
1 501 10.1.1.61 00:00:00:00:00:00 00:50:56:9c:3c:c5 0
```

```
#
```

The following conditions should be displayed:

- The VNS Licenses Available message should display a nonzero value.
- The learned-mac in the above output should not be 00:00:00:00:00:00.
- The learned-mac should match with the MAC address of the Cisco VSG that is intended to protect the VMs.

The MAC address of the Cisco VSG can be found on the corresponding Cisco VSG by entering the **show interface data 0** command.

This example shows the results of the command:

```
vsg# show interface data 0
data0 is up
Hardware: Ethernet, address: 0050.569c.3cc5 (bia 0050.569c.3cc5) <----
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA
full-duplex, 10 Gb/s
Auto-Negotiation is turned on
Rx
0 input packets
Tx
8084 output packets
vsg#
```

If the learned-mac in the **vemcmd show vsn config** command is 00:00:00:00:00:00, manually check if the Cisco VSG service (data) interface is bound to the proper port-profile and has the right VLAN configured.

To check Cisco VSG service interface assignment on the VEM, enter the **vemcmd show** command.

This example shows the result of the command:

```
# vemcmd show bd 501 <--- 501 is the service vlan
BD 501, vdc 1, vlan 501, 4 ports
Portlist:
6 vns
18 vmnic1
58 tenant1-primary ethernet0 <--- VSG VM name
#
```

The Cisco VSG VM name should be displayed as part of the output.

To see the output of the port-profile associated with the Cisco VSG service interface on the VSM, enter the **show port-profile name** *pp-name* command.

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

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

This example shows the results of the command:

```
vsm# show vlan

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

```
vsm#
```

Make sure that the following occurs:

- Service VLAN (501) is configured in the uplink port profile on the VSM.
- Service VLAN is not configured as a system VLAN on the uplink port profile)

To confirm the configuration, enter the **show running-config port-profile system-data-uplink** command.

This example shows the results of the command:

```
vsm# show running-config port-profile system-data-uplink

!Command: show running-config port-profile system-data-uplink
!Time: Thu Feb 24 13:06:30 2011

version 4.2(1)SV1(4)
port-profile type ethernet system-data-uplink
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 51-53,501
  no shutdown
  system vlan 51-52
  state enabled
vsm#
```

Security Posture Not Maintained After the vMotion of the VM to the new ESX Host

After performing vMotion of the traffic VM, the security posture as defined by the policies in the Cisco VSG can be disrupted.

Possible reasons:

- License was not checked out on the new module
- VEM did not learn the MAC address of the Cisco VSG

Verifications:

- Check if the Cisco VSG MAC is learned on all the VEMs that host the protected VMs involved in communication. On the VEM, enter the following command:

```
# vemcmd show vsn config
VNS Enabled  | VNS Licenses Available   1
VSN#  VLAN    IP         STATIC-MAC       LEARNED-MAC  LTLs
1   501     10.1.1.61  00:00:00:00:00:00  00:50:56:9c:3c:c5     0
#
```

  - The VNS Licenses Available message should display a nonzero value.
  - The learned-mac should not be 00:00:00:00:00:00.
  - The learned-mac should match with the MAC address of the Cisco VSG that is intended to protect the VMs.

  This example shows how to find the MAC address of the Cisco VSG on the corresponding Cisco VSG:

```
vsg# show interface data 0
data0 is up
  Hardware: Ethernet, address: 0050.569c.3cc5 (bia 0050.569c.3cc5) <----
```

```
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  full-duplex, 10 Gb/s
  Auto-Negotiation is turned on
  Rx
    0 input packets
  Tx
    8084 output packets
vsg#
```

- If the learned MAC address in the **vemcmd show vsn config** command is 00:00:00:00:00:00, manually check if the Cisco VSG service (data) interface is bound to the proper port profile and has the right VLAN configured.

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

```
# vemcmd show bd 501  <--------- 501 is the service vlan
BD 501, vdc 1, vlan 501, 4 ports
Portlist:
      6  vns
     18  vmnic1
     58  tenant1-primary ethernet0 <------ VSG VM name
#
```

  The Cisco VSG VM name should be displayed as part of the output.

To see the output of the port-profile associated with the Cisco VSG's service interface, on the VSM, enter the **show port-profile name <pp-name>** command.

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

Policy Decision Inconsistent with the Port Profile Changes

Either of these conditions can exist:

- User changed the port profile of the traffic VM from one firewall PP 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

Troubleshooting VSM and Cisco VNMC Interactions

After registering the VSM to the Cisco VNMC, enter the **show vnm-pa status** comamand to check the status.

This example shows the results of a successful installation:

```
vsm# show vnm-pa status
VNM Policy-Agent status is - Installed Successfully.
```

```
vsm#
```

If there is a failure, there can be several reasons. One failure could be because the Cisco VNMC is unreachable or dead. Ping to the Cisco VNMC 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. The below example shows the results of this type of failure. Provide the correct password and register again.

```
vsm# show vnm-pa status
VNM Policy-Agent status is - Installation Failure
Incorrect shared secret.
vsm#
```

On the Cisco VNMC GUI, on the Administration > Service Registery > Clients tab, make sure that the registered VSM is shown as "registered" under the Oper State column.

On the Cisco VNMC GUI, make sure that the org is configured in the same way as in the port profile. The registered VSM should also be available under the Resources > Virtual Supervisor Modules. If the org is not properly configured on the port profile, the Config State will be org-not-found under the port profiles tab of the registered VSM. After editing the port profile with the correct org name, the Config State changes to OK.

Troubleshooting Cisco VSG and Cisco VNMC Interaction

After registering the Cisco VSG to the Cisco VNMC, enter the **show vnm-pa status** comamand to check the status.

This example shows the results of a successful registration:

```
vsg# show vnm-pa status
VNM Policy-Agent status is - Installed Successfully.
vsg#
```

If there is a failure, there can be several reasons. One failure could be because the Cisco VNMC is unreachable or dead. Ping to the Cisco VNMC 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. The below example shows the results of this type of failure. Provide the correct password and register again.

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

On the Cisco VNMC GUI, on the Administration > Service Registery > Clients tab, make sure that the registered VSM is shown as registered under the Oper State column.

Troubleshooting Cisco VNMC and vCenter Server Interaction

To all the Cisco VNMC to communicate with the vCenter Server, you must access. You must have installed the Cisco VNMC's vCenter extension XML plug-in.

The vCenter Server is added to the Cisco VNMC with the provided IP address and name under Administration > VM Managers > Add VM manager. The Operational State of the newly added vCenter Server indicates that it is up.

Other possible operational states could be unreachable or bad-credentials. If the state is unreachable, the vCenter Server is down or could not be reached. To check if you can access the vCenter Server on the Cisco VNMC, use SSH to the Cisco VNMC with the user as admin and the VNMC password.

To check reachability, enter the **connect local-mgmt** command.

This example shows how to access the vCenter Server:

```
vnmc# connect local-mgmt
Cisco Virtual Network Management Center
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2010, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
vnmc(local-mgmt)#
```

Use the **ping** command to check if you can reach the vCenter Server (assuming that the vCenter Server does not block the **ping** command).

On the Cisco VNMC GUI, go to Administration > VMManagers tab and expand the VM Managers. Click on the vCenter Server object and review the right pane. If the state shows as bad-credentials, you have not registered the vCenter Server extension XML plugin for that vCenter Server. Go to the vCenter Server that is being added and install the vCenter Server extension XML plugin. For instructions, see the *Cisco Virtual Network Management Center GUI Configuration Guide*, “Chapter 7 - Configuring VM Managers”.