Troubleshooting Module Issues

This chapter describes how to troubleshoot various issues that could occur while the Cisco VSG is communicating with the Virtual Supervisor Module (VSM), Virtual Ethernet Module (VEM), Cisco Virtual Netework Management Center (VNMC), or the vCenter 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 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 shows that 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
```

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 how to troubleshoot issues with Cisco VSG and VEM interactions.

This section includes the following topics:

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, 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.
- On the Cisco VSG, enter the **show vsg ip-binding** command to see if the VM IP to service profile binding is present.
- 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 | grep 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
ASA Services Disabled | ASA Licenses Available   0
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 ESX via SSH.

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 address is learned on all the VEMs that host the protected VMs involved in the communication by entering the **vemcmd show vsn config** command on the VEM.

This example shows how to display the Cisco VSG configuration:

```
vem# vemcmd show vsn config
VSG Services Enabled | VNS Licenses Available 2
ASA Services Disabled| ASA Licenses Available 0
VSN#  SWBD IP         MAC               LTLs   VER  VER-BITMAP
```

```
1    101   10.1.1.230 00:50:56:be:4f:c6     1       2   1,2
```

The following conditions should be displayed on the command output:

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

You can find the MAC address of the Cisco VSG by entering the **show interface data 0** command.

This example shows how to display information on the interface for the 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
```

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.

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 501         <------------- 501 is the service VLAN
VLAN 501, vdc 1, swbd 501, hwbd 11, 5 ports
Portlist:
6 vns
18 vmnic1
58 tenant1-primary ethernet0      <------------- Cisco VSG VM name
```

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

You can display the port profile that is associated with the Cisco VSG's 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 that 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
```

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.

You can confirm the configuration by entering the **show running-config port-profile system-data-uplink** command.

This example shows how to confirm the configuration:

```
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
```

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:

- The license was not checked out on the new module.
- The 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 by entering the **vemcmd show vsn config** command.

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

```
vem# vemcmd show vsn config
VSG Services Enabled  | VSG Licenses Available   2
ASA Services Enabled  | ASA Licenses Available   2
    VSN#  SWBD              IP               MAC  LTLs VER     VER-BITMAP
      2  3756     10.10.10.202  00:50:56:83:00:1e     2   2           1,2
     27  3770       172.31.2.1  00:50:56:a4:0f:36     1   2           1,2
     28  3756     10.10.11.202  00:50:56:a4:0f:3d     1   2           1,2
```

  – The VNS Licenses Available message should display a nonzero value.

  – The learned MAC address should not be 00:00:00:00:00:00 for the layer 2 adjacent node.

  – The learned MAC address 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
```

- 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:

```
vem# vemcmd show vlan 501         <------------- 501 is the service VLAN
VLAN 501, vdc 1, swbd 501, hwbd 11, 5 ports
Portlist:
6 vns
18 vmnic1
58 tenant1-primary ethernet0      <------------- Cisco VSG VM name
```

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

You can view the port-profile information for the Cisco VSG's 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 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

When policy decisions are inconsistent with the 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 to determine the connectivity between the Cisco VSG and the VEM.

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

```
VSM-1# ping vsn all src-module all
ping vsn 106.1.1.1 vlan 54 from module 3 5, seq=0 timeout=1-sec
  module(usec)   :  3(156)  5(160)
ping vsn 110.1.1.1 vlan 54 from module 3 5, seq=0 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)
```

```
ping vsn 106.1.1.1 vlan 54 from module 3 5, seq=1 timeout=1-sec
  module(usec)   :  3(230)  5(151)
ping vsn 110.1.1.1 vlan 54 from module 3 5, seq=1 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)

ping vsn 106.1.1.1 vlan 54 from module 3 5, seq=2 timeout=1-sec
  module(usec)   :  3(239)  5(131)
ping vsn 110.1.1.1 vlan 54 from module 3 5, seq=2 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)

ping vsn 106.1.1.1 vlan 54 from module 3 5, seq=3 timeout=1-sec
  module(usec)   :  3(248)  5(153)
ping vsn 110.1.1.1 vlan 54 from module 3 5, seq=3 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)

ping vsn 106.1.1.1 vlan 54 from module 3 5, seq=4 timeout=1-sec
  module(usec)   :  3(259)  5(126)
ping vsn 110.1.1.1 vlan 54 from module 3 5, seq=4 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)
```

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
  vxlan VXLAN
```

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 VNMC Interactions

After registering the VSM to the Cisco VNMC, you can check the status of the VSM and Cisco VNMC policy agents by entering the **show vnm-pa status** comamand.

This example shows how to check the status:

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

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.

This example shows the results of this type of failure:

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

Provide the correct password and register again.

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 display as “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 Interactions

After registering the Cisco VSG to the Cisco VNMC, you can check the status by entering the **show vnm-pa status** command.

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

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

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.

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

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

Provide the correct password and register again.

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 Interactions

To enable the Cisco VNMC to communicate with the vCenter Server, 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.

You can check reachability by entering 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) 2002-2011, 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
```

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 "Chapter 7 - Configuring VM Managers" of the *Cisco Virtual Network Management Center GUI Configuration Guide*.

Troubleshooting the Cisco VSG and VEM Interactions When the Cisco VSG is on a VXLAN in a Service-Chain

You can run a series of checks to ensure that interactions between the Cisco VSG and VEM are seamless.

Run the following verifications:

- Check if the Cisco VSG is alive by using the **show vservice brief** command from the VSM.

  This example shows how to display the Cisco VSG configuration:

```
vsm# show vservice brief
#License Information
Type      In-Use
vsg         7
asa         7

#Node Information
ID  Name                        Type   IP-Address      Mode   State   Module
1   node_10.1.1.40_l3_fclose    vsg    10.1.1.40        l3     Unreach 3,9,
3   node_10.1.1.40_501_fclose   vsg    10.1.1.40        vxlan  Alive   4,9,11,
5   node_10.1.1.45_502_fclose vsg    10.1.1.45        vxlan  Unreach 9,
9   VASA1                       asa    192.168.200.221 v-53   Alive   3,9,11,
13  VASA-vxlan-222              asa    192.168.200.222 vxlan  Alive   4,9,11,
16  EL1                         vsg    7.1.1.1         v-501  Unreach 4,
17  EL2                         vsg    7.1.1.1         v-502  Unreach 3,
```

  If a specific Cisco VSG is not alive (wherein ‘Unreach’ or ‘??’ is displayed), use the **show vservice detail node_ipaddr** *node ip* command for further analysis.

- Check if the Cisco VSG node definition has “adjacency l2 vxlan” in the output. For example:

```
vservice node node_10.1.1.40_501_fclose type vsg
  ip address 10.1.1.40
  adjacency l2 vxlan bridge-domain segment2
  fail-mode close
```

- Check the port profile attached to the VM. It should be pointing to either the vsevice node VSG directly or to a service path that contains the corresponding Cisco VSG.
- Check the port profile attached to the Cisco VSG data interface, which should be on a bridge domain. It must not have any org/vservice configuration. For example:

```
port-profile type vethernet segment-5001-nofw
  vmware port-group
  switchport mode access
  switchport access bridge-domain segment2
  no shutdown
  state enabled
```