



Upgrades

This chapter describes how to identify and resolve problems related to upgrading the Virtual Supervisor Module (VSM) software and includes the following sections:

- [Information About Upgrades, page 5-1](#)
- [Problems with the In-Service Software Upgrade, page 5-1](#)
- [Problems with the VEM Upgrade, page 5-5](#)
- [Problems with the GUI Upgrade, page 5-6](#)
- [Problems with VSM-VEM Layer 2 to 3 Conversion Tool, page 5-16](#)
- [Upgrade Troubleshooting Commands, page 5-16](#)

Information About Upgrades

The upgrade for the Cisco Nexus 1000V involves upgrading software on both the VSM and the Virtual Ethernet Module (VEM).

An in service software upgrade (ISSU) is available for a stateful upgrade of the Cisco Nexus 1000V image(s) running on the VSM. A stateful upgrade is one without noticeable interruption of data plane services provided by the switch.

For detailed information, see the *Cisco Nexus 1000V Installation and Upgrade Guide*.

Problems with the In-Service Software Upgrade

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

Table 5-1 **Problems with the ISSU**

Symptom	Possible Causes	Solution
Error Message: Pre-Upgrade check failed. Return code 0x40930062 (free space in the filesystem is below threshold).	This error indicates that there is not enough space in the /var/sysmgr partition.	1. Reboot the system.

Table 5-1 (continued) Problems with the ISSU


Symptom	Possible Causes	Solution
<p>Error message:</p> <p>Pre-Upgrade check failed. Return code 0x4093000A (SRG collection failed)</p>	A module is removed during the upgrade.	<ol style="list-style-type: none"> 1. Make sure that the module removal is complete. 2. Restart the software upgrade using the instructions in the <i>Cisco Nexus 1000V Installation and Upgrade Guide</i>.
<p>Error message:</p> <p>Pre-Upgrade check failed. Return code 0x40930076 (Standby sup is offline. ISSU will not proceed)</p>	The standby VSM is not present or is not synchronized with the active VSM, and the VSMs do not form a stable HA pair.	<ol style="list-style-type: none"> 1. Verify the HA synchronization state. show system redundancy status The output of the show command must indicate the following: Active VSM: Active with HA standby Standby VSM: HA standby 2. If the output of the show command indicates that the VSMs are not synchronized, see the “Problems with High Availability” section on page 6-2. 3. When the VSMs are synchronized, restart the software upgrade using the detailed instructions in the <i>Cisco Nexus 1000V Installation and Upgrade Guide</i>.
<p>Error message:</p> <p>Pre-Upgrade check failed. Return code 0x807B0002 (No such file or directory)</p> <p>Error message:</p> <p>Pre-Upgrade check failed. Return code 0x4093000F (Failed to copy image)</p>	<p>The software image files required for the upgrade are not present or were not copied to the bootflash: repository.</p> <p>There may not be enough room in the bootflash: repository for the files to be copied.</p>	<ol style="list-style-type: none"> 1. Verify that there is enough space in bootflash for the image files. dir 2. Do one of the following: <ul style="list-style-type: none"> – If additional space is needed, delete other files from the bootflash: repository to make room for the software image files. delete <p> Caution Do not delete kickstart or system image files from bootflash. If there are no image files in bootflash, the system cannot reboot if required.</p> <ul style="list-style-type: none"> – If not, continue with the next step. <ol style="list-style-type: none"> 3. Download the required images from www.cisco.com to the bootflash: repository. 4. Verify that the correct images are in the bootflash: repository. show boot 5. When the correct software images are in the bootflash: repository, restart the software upgrade using the instructions in the <i>Cisco Nexus 1000V Installation and Upgrade Guide</i>.

Table 5-1 (continued) Problems with the ISSU

Symptom	Possible Causes	Solution
<p>The install command fails with the following error:</p> <pre>Return code 0x4045001F (image MD5 checksum error) Pre-Upgrade check failed. Return code 0x40930011 (Image verification failed)</pre>	<p>The software image file(s) required for the upgrade do not pass the MD5 checksum verification, indicating that the correct file(s) are not present in bootflash: repository for the upgrade to proceed.</p> <p>A file can be truncated when copied.</p>	<ol style="list-style-type: none"> Using the README file from the upgrade zip folder at www.cisco.com, verify the MD5 checksum for each of the image files. show file bootflash: filename md5sum Replace the file(s) that do not match. Verify that the correct images are in the bootflash: repository and that the checksums match. show file bootflash: filename md5sum When the correct software images are in the bootflash: repository, restart the software upgrade using the instructions in the <i>Cisco Nexus 1000V Installation and Upgrade Guide</i>.
<p>Error message:</p> <pre>Install has failed. Return code 0x40970001 (Incompatible image)</pre>	<p>You might have used an incorrect filename when entering the install all command.</p>	<p>Restart the software upgrade using the correct filenames for the new software images.</p> <pre>install all kickstart filename1 system filename2</pre>
<p>After upgrading, the VSMS are not running the new software version.</p>	<p>The boot variables were not set properly.</p>	<ol style="list-style-type: none"> Verify that the running images and boot variables match the upgrade version. show version show boot If needed, download the required images from www.cisco.com to your local bootflash: repository. Verify that the correct images are in the bootflash: repository. show boot Restart the software upgrade using the instructions in the <i>Cisco Nexus 1000V Installation and Upgrade Guide</i>. If the problem persists, collect details of the upgrade and open a support case. show system internal log install details
<p>Performing the configuration copy process fails and stops the upgrade.</p> <pre>Performing configuration copy. [####-----] 30%</pre>	<p>Service or system errors.</p>	<ol style="list-style-type: none"> Manually copy the configuration. copy running-config startup-config Do one of the following: <ul style="list-style-type: none"> If the progress bar gets stuck before 100% for over one minute, collect details of the upgrade and open a support case. show system internal log install details If the copy succeeds without delays, restart the software upgrade using the instructions in the <i>Cisco Nexus 1000V Installation and Upgrade Guide</i>.

Table 5-1 (continued) Problems with the ISSU

Symptom	Possible Causes	Solution
<p>Error message:</p> <p>Another install procedure may be in progress. (0x401E0007)</p>	<p>Another upgrade session is in progress from a VSM console or SSH/Telnet.</p>	<p>Do one of the following:</p> <ul style="list-style-type: none"> Continue the first upgrade session in progress. Stop the upgrade and restart one session only using the instructions in the <i>Cisco Nexus 1000V Installation and Upgrade Guide</i>.
<p>The install command fails with following error message:</p> <pre>-- FAIL. Return code 0x4093001E (Standby failed to come online) Install has failed. Return code 0x4093001E (Standby failed to come online)</pre>	<p>The standby VSM fails to boot with the new image.</p>	<p>Do one of the following:</p> <ul style="list-style-type: none"> Restart the software upgrade using the instructions in the <i>Cisco Nexus 1000V Installation and Upgrade Guide</i>. Postpone the upgrade and reset the boot variables to the original filenames. <p>boot kickstart filename [sup-1] [sup-2]</p>
<p>The install command fails with following error message:</p> <pre>Install has failed. Return code 0x4093001F (Standby installer failed to take over the installation). Please identify the cause of the failure, and try "install all" again"</pre>	<p>The standby VSM takes more than 10 minutes to come up and form a stable HA pair with the active VSM.</p>	<ol style="list-style-type: none"> Reset the boot variables to the original filenames. <p>boot kickstart filename [sup-1] [sup-2]</p> <ol style="list-style-type: none"> If the standby is still running the new software version, reload it. <p>reload</p> <p>The standby synchronizes with the active, so that both are running the original software version.</p>
<p>The install command fails with following error message:</p> <pre>Module 2: Waiting for module online. -- SUCCESS -- Install has failed. Return code 0x40930000 (Current operation failed to complete within specified time)</pre>	<p>A failure at the standby VSM caused it to reload again after the Continuing with installation, please wait message and before the switchover.</p>	<ol style="list-style-type: none"> Inspect the logs. <p>show logging</p> <ol style="list-style-type: none"> Look for standby reloads caused by process failures. <p>show cores</p> <p>If a process crash is observed, collect details of the upgrade and open a support case.</p> <p>show system internal log install details</p> <ol style="list-style-type: none"> Restart the software upgrade using the instructions in the <i>Cisco Nexus 1000V Installation and Upgrade Guide</i>.
<p>The pre-upgrade check failed:</p> <p>Return code 0x40930062 (free space in the filesystem is below threshold).</p>		<ol style="list-style-type: none">

Problems with the VEM Upgrade

The following are symptoms, possible causes, and solutions for problems with VEM software upgrade.

Table 5-2 Problems with the VEM Upgrade

Symptom	Possible Causes	Solution
After starting a VEM upgrade from the VSM console, the VMware Upgrade Manager (VUM) skips upgrading the hosts with the new VEM.	<p>One or more of the following are enabled on the host cluster.</p> <ul style="list-style-type: none"> VMware high availability (HA) VMware fault tolerance (FT) VMware Distributed Power Management (DPM) 	<ol style="list-style-type: none"> Verify the upgrade failure. show vmware vem upgrade status From vCenter Server, disable HA, FT, and DPM for the cluster. Restart the VEM software upgrade using the instructions in the <i>Cisco Nexus 1000V Installation and Upgrade Guide</i>.
VEM upgrade fails.	An incorrect VUM version is in use.	<ol style="list-style-type: none"> Identify the VUM version required for the upgrade using the <i>Cisco Nexus 1000V Compatibility Information</i>. Upgrade to the correct VUM version. Restart the software upgrade using the instructions in the <i>Cisco Nexus 1000V Installation and Upgrade Guide</i>.
After upgrading, the host is not added to the VSM.	An incorrect VEM software version is installed on the host.	<ol style="list-style-type: none"> Identify the VEM software version required for the upgrade using the <i>Cisco Nexus 1000V Compatibility Information</i>. Proceed with the upgrade using the correct VEM software version and the instructions in the <i>Cisco Nexus 1000V Installation and Upgrade Guide</i>.
A message on the ESX/ESXi command line shell and VMkernel logs notifies you that the loading and unloading of modules failed.	The modules were not placed in maintenance mode (all VMs VMotioned over) before starting the upgrade.	<ol style="list-style-type: none"> Place the host in maintenance mode. Proceed with the upgrade using the instructions in the <i>Cisco Nexus 1000V Installation and Upgrade Guide</i>.
	<p>The host does not have enough memory to load new modules.</p> <p>A host requires a minimum of 2 GB of physical RAM. If it also hosts a Cisco Nexus 1000V VSM VM, it needs a minimum of 4 GB of physical RAM. If it also hosts the vCenter Server VM, additional memory might be needed.</p>	<ol style="list-style-type: none"> Verify that the host has sufficient memory to load the new modules. For more information about allocating RAM and CPU, see the <i>Cisco Nexus 1000V Installation and Upgrade Guide</i>. Proceed with the upgrade using the instructions in the <i>Cisco Nexus 1000V Installation and Upgrade Guide</i>.

Problems with the GUI Upgrade

The following are symptoms, possible causes, and solutions for problems with software upgrade using the GUI upgrade application.


Note

If you are upgrading directly from SV1(4) to SV1(4a), the GUI is not used and this section does not apply. This section is applicable only if you use the GUI for an intermediate upgrade from a SV1(3x) release to SV1(4), prior to upgrading to SV1(4a).

Table 5-3 *Problems with the GUI Upgrade*

Symptom	Possible Causes	Solution
<p>The upgrade GUI stops and times out after 10 minutes and displays the following message:</p> <pre>Error: Could not contact the upgraded VSM at n.n.n.n. Please check the connection.</pre>	<p>During the upgrade, you configured an unreachable IP address for the mgmt0 interface.</p> <p>In this case, one VSM in the redundant pair has new software installed and is unreachable. The other VSM has the original pre-upgrade software version installed and is reachable.</p>	<ol style="list-style-type: none"> Use one of the following sets of procedures to return your VSM pair to the previous software version: <ul style="list-style-type: none"> “Recovering a Secondary VSM with Active Primary” section on page 5-7 “Recovering a Primary VSM with Active Secondary” section on page 5-12 Restart the software upgrade using the instructions in the <i>Cisco Nexus 1000V Installation and Upgrade Guide</i>.
<p>The upgrade GUI stops and times out after 10 minutes and displays the following message:</p> <pre>Error: Could not contact the upgraded VSM at 10.104.244.150. Please check the connection.</pre> <p>After timing out, one VSM comes up in switch(boot) mode.</p>	<p>You have selected incompatible or incorrect VSM software images for the upgrade.</p> <p>The software images you selected from the GUI selection list included a system image for one software version and a kickstart image for another software version. These images must be for the same software version.</p> <p>For an example of how software images are selected during the upgrade, see Example 5-1.</p>	<ol style="list-style-type: none"> To continue the upgrade, first recover the VSM using one of the following: <ul style="list-style-type: none"> “Recovering a Secondary VSM with Active Primary” section on page 5-7 “Recovering a Primary VSM with Active Secondary” section on page 5-12 Restart the software upgrade using the instructions in the <i>Cisco Nexus 1000V Installation and Upgrade Guide</i>.

Example 5-1 Upgrade: Enter Upgrade Information

This example shows how to specify system and kickstart images during the upgrade process. In this example, the images specified are from the same release, SV1.4. If you specify a kickstart image from one release, and a system image from another, then the upgrade cannot proceed.

Nexus 1000V Upgrade

Steps	Enter Upgrade Information
1. Enter VSM Credentials	Current VSM IP Address: 10.78.108.133
2. Verify Module Upgrade	Temporary Upgrade IPv4 address for interface mgmt 0: 10.78.108.134
3. Enter Upgrade Information	Temporary Upgrade IPv4 address for L3 interface control 0: 192.168.2.10
4. Summary: Please Review Configurations	New System Image: nexus-1000v-mz.4.2.1.SV1.4.bin
5. Verify Module Insertion	New Kickstart Image: nexus-1000v-kickstart-mz.4.2.1.SV1.4.bin
	Note: Please be sure to choose VSM images (New System / New Kickstart) for release version 4.2*. Failure to do so will impact the upgrade process.
	< Prev Next > Finish Cancel

Recovering a Secondary VSM with Active Primary

You can recover a secondary VSM when the primary VSM is active.

**Note**

The information in this section does not apply when upgrading from Release 4.2(1)SV1(4) to Release 4.2(1)SV2(1.1).

- Step 1** Stop the upgrade on the VSM, using the [“Stopping a VSM Upgrade”](#) section on page 5-8
- Step 2** Change the boot variables back to the previous version using the [“Changing Boot Variables”](#) section on page 5-9
- Step 3** From the vCenter Server left-hand panel, right-click the secondary VSM and then choose **Delete from Disk**.
- The secondary VSM is deleted.
- Step 4** Create a new VSM by reinstalling the software using the vSphere Client Deploy OVF Template wizard, specifying the following:
- The Cisco Nexus 1000V secondary configuration method (configures the secondary VSM in an HA pair using a GUI setup dialog).
 - The host or cluster of the primary VSM.
 - The same domain ID and password as that of the primary VSM.

For a detailed procedure, see the *Cisco Nexus 1000V Installation and Upgrade Guide*.

The VSM comes up and forms an HA pair with the newly created standalone VSM. The VSMs have the previous version of the software installed.

Stopping a VSM Upgrade

You can stop a VSM upgrade that is in progress.

BEFORE YOU BEGIN

- Log in to the CLI in EXEC mode.



Note

The information in this section does not apply when upgrading from Release 4.2(1)SV1(4) to Release 4.2(1)SV2(1.1).

DETAILED STEPS

Step 1 Display upgrade status.

show svcs upgrade status

Example:

```
switch# show svcs upgrade status
Upgrade State: Start
Upgrade mgmt0 ipv4 addr: 1.1.1.1
Upgrade mgmt0 ipv6 addr:
Upgrade control0 ipv4 addr:
```

Step 2 Stop the upgrade.

a. configure terminal

b. no svcs upgrade start

Example:

```
switch# configure terminal
switch#(config)# no svcs upgrade start
WARNING! VSM upgrade process is aborted
switch#(config)#
```

Step 3 Display the upgrade status.

show svcs upgrade status

Example:

```
switch#(config)# show svcs upgrade status
Upgrade State: Abort
Upgrade mgmt0 ipv4 addr:
Upgrade mgmt0 ipv6 addr:
Upgrade control0 ipv4 addr:
```

Step 4 You have completed this procedure. Return to one of these sections:

- [“Recovering a Secondary VSM with Active Primary”](#) section on page 5-7
- [“Recovering a Primary VSM with Active Secondary”](#) section on page 5-12

Changing Boot Variables

You can replace the software images used to boot the VSM.

BEFORE YOU BEGIN

- Log in to the CLI in EXEC mode.
- Know the filenames of the pre-upgrade system and kickstart image files to apply.

DETAILED STEPS

Step 1 Display the current boot variables.

show boot

Example:

```
switch# show boot
sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart-mz.4.0.4.SV1.3a.bin
system variable = bootflash:/nexus-1000v-mz.4.0.4.SV1.3a.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart-mzg.4.2.1.SV1.4.bin
system variable = bootflash:/nexus-1000v-mzg.4.2.1.SV1.4.bin
No module boot variable set
switch(config)#
```

Step 2 Remove the current system and kickstart boot variables.

- configure terminal**
- no boot system**
- no boot kickstart**

Example:

```
switch# configure terminal
switch(config)# no boot system
switch(config)# no boot kickstart
switch#(config)#
```

Step 3 Restore the system and kickstart boot variables to the original pre-upgrade filenames.

- boot system bootflash:system-boot-variable-name**
- boot system bootflash:kickstart-boot-variable-name**

Example:

```
switch#(config)# boot system bootflash:nexus-1000v-mz.4.0.4.SV1.3a.bin
switch#(config)# boot kickstart bootflash:nexus-1000v-kickstart-mz.4.0.4.SV1.3a.bin
switch#(config)#
```

Step 4 Copy the running configuration to the startup configuration.

copy run start

Example:

```
switch#(config)# copy run start
[#####] 100%e
switch#(config)#
```

Step 5 Verify the change in the system and kickstart boot variables.

show boot

Example:

```

switch#(config)# show boot
sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart-mz.4.0.4.SV1.3a.bin
system variable = bootflash:/nexus-1000v-mz.4.0.4.SV1.3a.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart-mz.4.0.4.SV1.3a.bin
system variable = bootflash:/nexus-1000v-mz.4.0.4.SV1.3a.bin
No module boot variable set
switch#(config)#

```

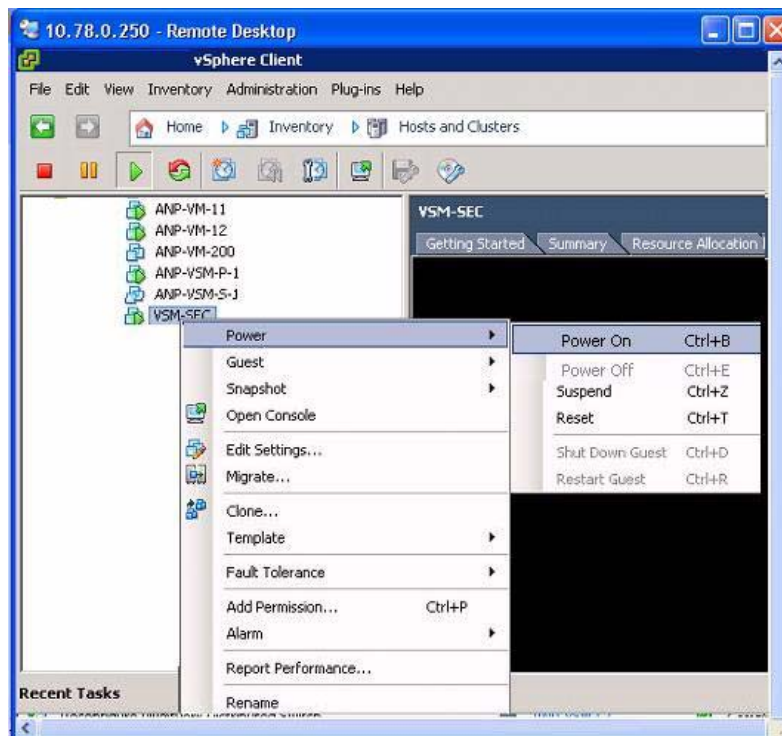
Step 6 You have completed this procedure. Return to one of these sections:

- [“Recovering a Secondary VSM with Active Primary”](#) section on page 5-7
- [“Recovering a Primary VSM with Active Secondary”](#) section on page 5-12

Powering On the VSM

You can power on the newly created VSM.

Step 1 From the vCenter Server left-hand panel, right-click the VSM and then choose **Power > Power On**. The VSM starts.



Step 2 You have completed this procedure. Return to the [“Recovering a Primary VSM with Active Secondary”](#) section on page 5-12.

Changing the HA Role

You can change the HA role of the VSM.

BEFORE YOU BEGIN

- Log in to the CLI in EXEC mode.
- Know the domain ID of the existing VSM.

DETAILED STEPS

Step 1 Go to the domain of the existing VSM.

- configure terminal**
- svs-domain**
- domain id** *domain-id*

Example:

```
switch# config t
switch(config)# svs-domain
switch(config-svs-domain)# domain id 1941
Warning: Config saved but not pushed to vCenter Server due to inactive connection!
```

Step 2 Change the HA role.

system redundancy role [primary | secondary | standalone]

Example:

```
switch(config-svs-domain)# system redundancy role secondary
Setting will be activated on next reload.
switch(config-svs-domain)#
```

Example:

```
switch(config-svs-domain)# system redundancy role primary
Setting will be activated on next reload.
switch(config-svs-domain)#
```

Step 3 Copy the running configuration to the startup configuration.

copy run start

Example:

```
switch#(config-svs-domain)# copy run start
[#####] 100%e
switch#(config-svs-domain)#
```

Step 4 You have completed this procedure. Return to the [“Recovering a Primary VSM with Active Secondary” section on page 5-12.](#)

Recovering a Primary VSM with Active Secondary

You can recover a primary VSM when the secondary VSM is active.

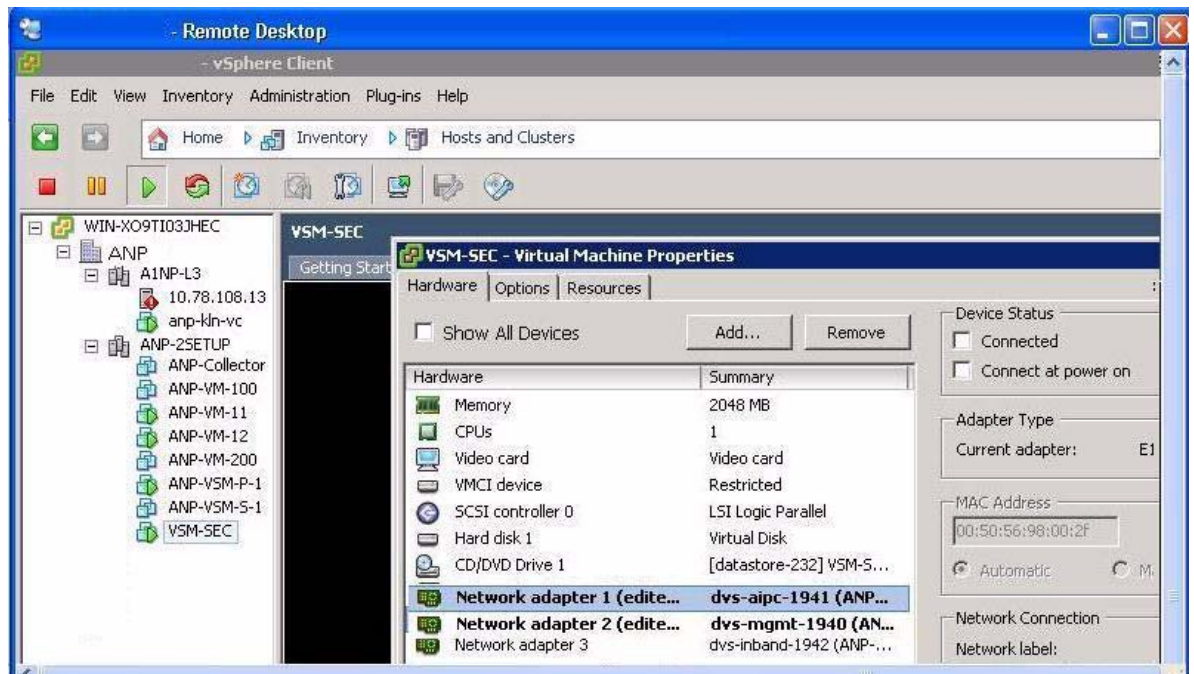
-
- Step 1** Stop the upgrade on the secondary VSM by completing the [“Stopping a VSM Upgrade” procedure on page 5-8](#)
- Step 2** Change the boot variables back to the previous version by completing the [“Changing Boot Variables” procedure on page 5-9](#)
- Step 3** From the vCenter Server left-hand panel, right-click the primary VSM and then choose **Delete from Disk**.
The primary VSM is deleted.
- Step 4** Create a new VSM by reinstalling the software from the OVA and specifying the following:
- Manual (CLI) configuration method instead of GUI.
 - The host or cluster of the existing secondary VSM.
- For detailed installation procedures, see the *Cisco Nexus 1000V Installation and Upgrade Guide*.
- Step 5** Make sure that the port groups between the host server and VSM are not connected when the new VSM is powered on by completing the [“Disconnecting the Port Groups” procedure on page 5-12](#).
- Step 6** Power on the newly-created VSM by completing the [“Powering On the VSM” procedure on page 5-10](#).
The VSM comes up with the standalone HA role.
- Step 7** Change the HA role of the newly created standalone VSM to primary and save the configuration by completing the [“Changing the HA Role” procedure on page 5-11](#).
- Step 8** Power off the newly created VSM by completing the [“Powering Off the VSM” procedure on page 5-14](#).
- Step 9** Make sure that the port groups between the host server and VSM are connected when the new VSM is powered on by completing the [“Connecting the Port Groups” procedure on page 5-14](#).
- Step 10** Power on the newly created VSM by completing the [“Powering On the VSM” procedure on page 5-10](#).
The VSM comes up, connects with the host server, and forms an HA pair with the existing primary VSM.
-

Disconnecting the Port Groups

You can disconnect and prevent port groups to the VSM from connecting to the host server.

-
- Step 1** In vCenter Server, select the VSM and then choose **Edit > Settings**.
The Virtual Machine Properties dialog box opens.
- Step 2** Select the Control port group and uncheck the following Device Settings:
- Connected
 - Connect at Power On

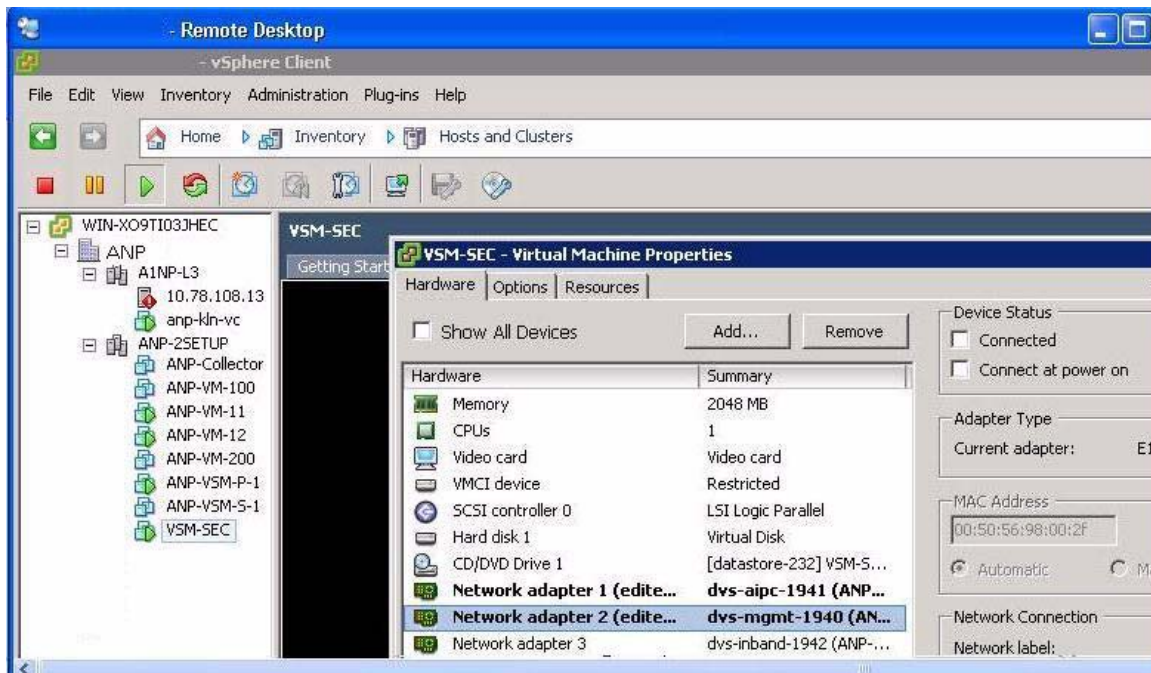
The connection from the VSM to the host server through the control port is dropped and is not restored when you power on the VSM.



Step 3 Select the Management port group and uncheck the following Device Settings:

- Connected
- Connect at Power On

The connection from the VSM to the host server through the management port is dropped and is not restored when you power on the VSM.

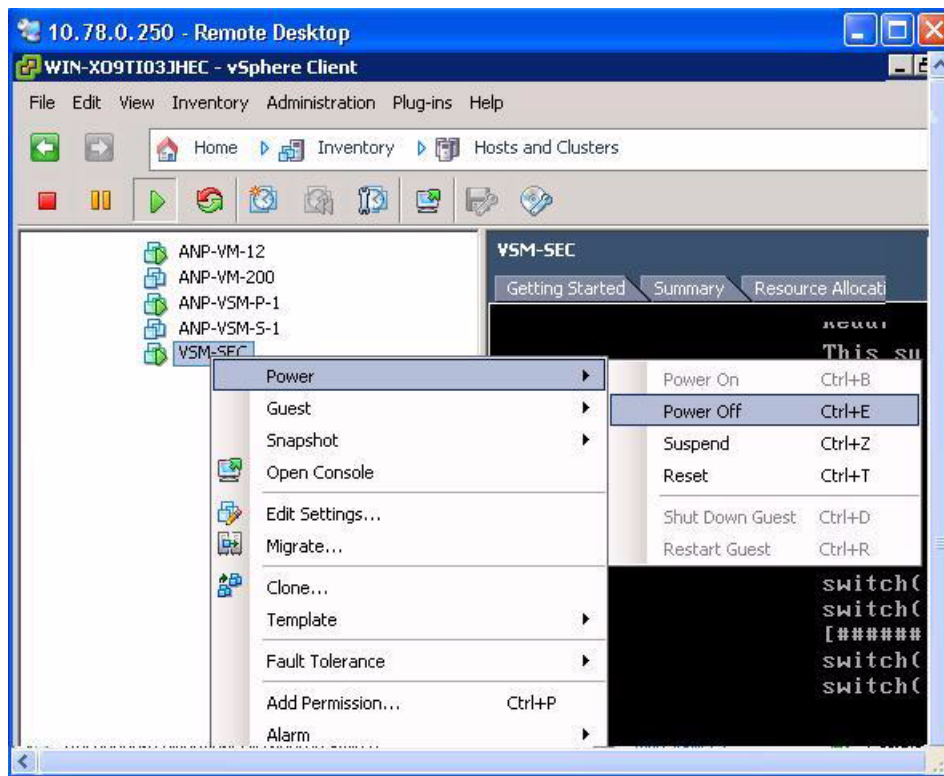


- Step 4** You have completed this procedure. Return to the [“Recovering a Primary VSM with Active Secondary” section on page 5-12.](#)

Powering Off the VSM

You can power off the newly created VSM.

- Step 1** From the vCenter Server left-hand panel, right-click the VSM and then choose **Power > Power Off**. The VSM shuts down.



- Step 2** You have completed this procedure. Return to the [“Recovering a Primary VSM with Active Secondary” section on page 5-12.](#)

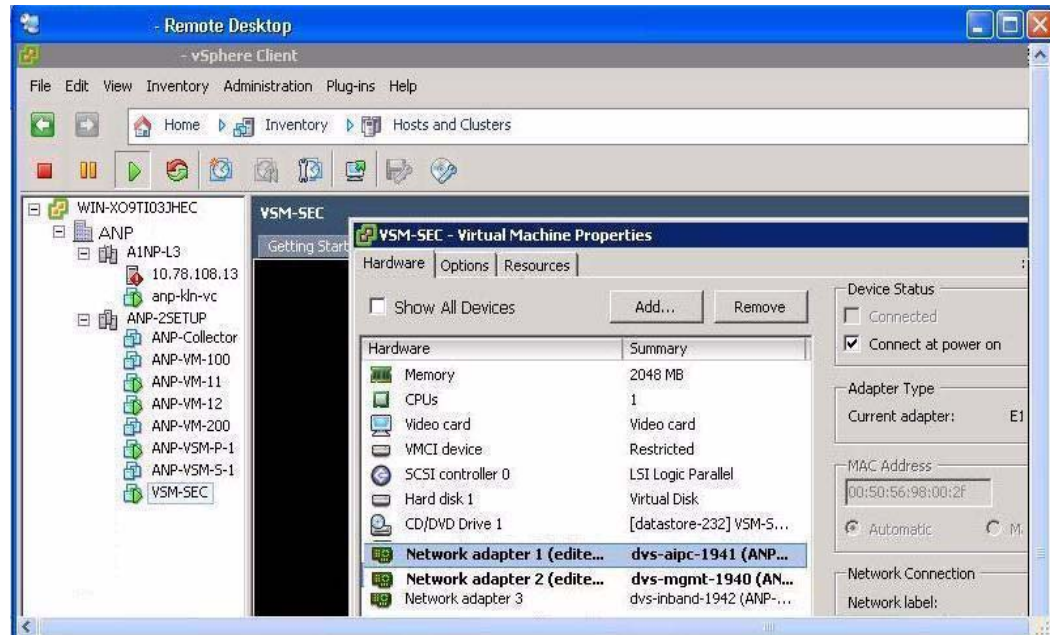
Connecting the Port Groups

You can make sure that the port groups to the host connect when you power on the VSM.

- Step 1** In vCenter Server, select the VSM and then choose **Edit > Settings**. The Virtual Machine Properties dialog box opens.
- Step 2** Select the Control port group and check the following Device Settings:

- Connect at Power On

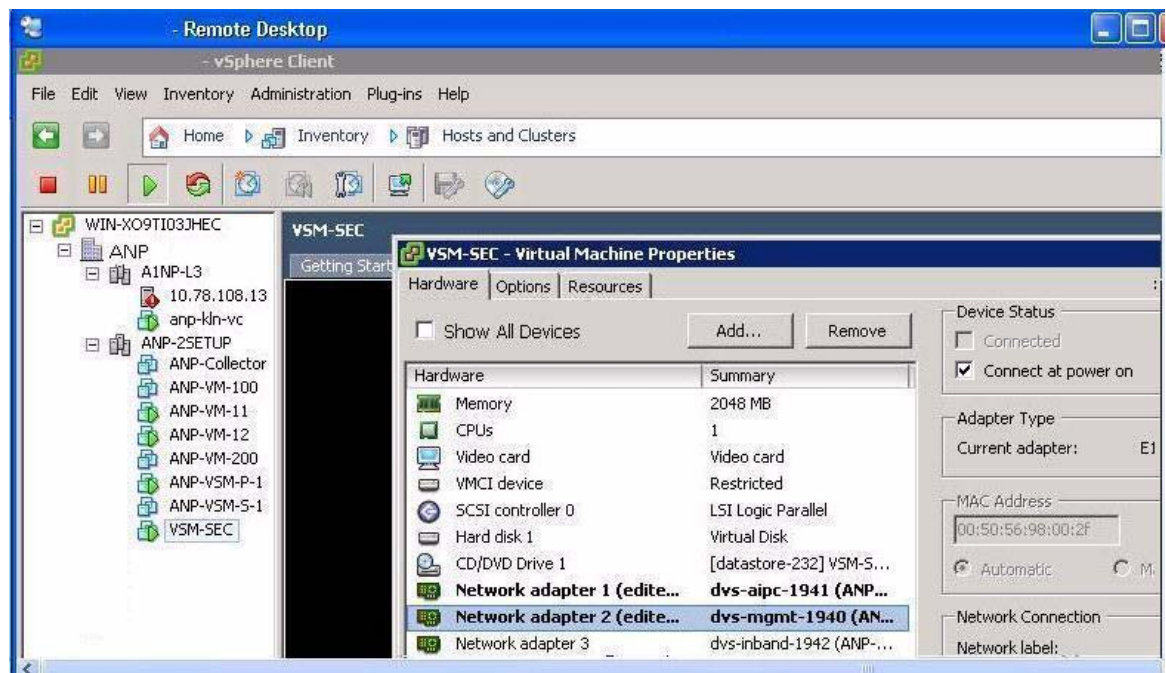
When you power on the VSM, it will connect to the host server through the control port.



Step 3 Select the Management port group and check the following Device Setting:

- Connect at Power On

When you power on the VSM, it will connect to the host server through the management port.



- Step 4** You have completed this procedure. Return to the [“Recovering a Primary VSM with Active Secondary” section on page 5-12.](#)

Problems with VSM-VEM Layer 2 to 3 Conversion Tool

The following is a symptom and solution for a problem with logging in to VSM when using the conversion tool:

Symptom	Solution
<p>When you enter your VSM and VC login credentials for the first time, the VSM-VEM Layer 2 to 3 Conversion Tool might display:</p> <pre>Timeout error. Is device down or unreachable?? ssh_expect</pre>	<ol style="list-style-type: none"> 1. Open a command line window and run an ssh command on the VSM (ssh username@vsmIPAddress). 2. When prompted, <i>Are you sure you want to continue connecting?</i>, enter yes. 3. Rerun the VSM-VEM Layer 2 to 3 Conversion Tool by reopening the .bat file. Ensure that the error does not reappear.

Upgrade Troubleshooting Commands

You can troubleshoot problems related to upgrades.

Command	Description
show boot	Displays boot variable definitions, showing the names of software images used to boot the VSM. See Example 5-2 on page 5-17 .
show module	Displays module status for active and standby VSMs. See Example 5-4 on page 5-17 (ISSU) . See Example 5-4 on page 5-17 .
show running-config include boot	Displays the boot variables currently in the running configuration. See Example 5-5 on page 5-18 .
show startup-config include boot	Displays the boot variables currently in the startup configuration. See Example 5-6 on page 5-18 .
show svcs connections	Displays the current connections between the VSM and the VMware host server. See Example 5-7 on page 5-18 .

Command	Description
show svcs upgrade status	Displays the upgrade status. See Example 5-8 on page 5-18 .
show system redundancy status	Displays the current redundancy status for the VSM. See Example 5-9 on page 5-19 .
show vmware vem upgrade status	Displays the upgrade status. See Example 5-10 on page 5-19 .

Example 5-2 show boot Command

```
switch# show boot
sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart-mz.4.0.4.SV1.3a.bin
system variable = bootflash:/nexus-1000v-mz.4.0.4.SV1.3a.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart-mzg.4.2.1.SV1.4.bin
system variable = bootflash:/nexus-1000v-mzg.4.2.1.SV1.4.bin
No module boot variable set
switch#
```

Example 5-3 show module Command (VSM upgraded first with ISSU, VEM upgrade pending)

```
switch# show module
Mod Ports Module-Type Model Status
-----
1 0 Virtual Supervisor Module Nexus1000V ha-standby
2 0 Virtual Supervisor Module Nexus1000V active *
3 248 Virtual Ethernet Module NA ok
Mod Sw Hw
-----
1 4.2(1)SV1(4a) 0.0
2 4.2(1)SV1(4a) 0.0
3 4.2(1)SV1(4) 1.9
Mod MAC-Address(es) Serial-Num
-----
1 00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8 NA
2 00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8 NA
3 02-00-0c-00-03-00 to 02-00-0c-00-03-80 NA
Mod Server-IP Server-UUID Server-Name
-----
1 10.78.109.43 NA NA
2 10.78.109.43 NA NA
3 10.78.109.51 4220900d-76d3-89c5-17d7-b5a7d1a2487f 10.78.109.51
switch#
```

Example 5-4 show module Command (VEM and VSM upgraded)

```
switch# show module
Mod Ports Module-Type Model Status
-----
1 0 Virtual Supervisor Module Nexus1000V ha-standby
2 0 Virtual Supervisor Module Nexus1000V active *
3 248 Virtual Ethernet Module NA ok
Mod Sw Hw
-----
```

```

1    4.0(4)SV1(3)    0.0
2    4.0(4)SV1(3)    0.0
3    4.2(1)SV1(4)    1.9

Mod  MAC-Address(es)                               Serial-Num
---  -
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA

Mod  Server-IP      Server-UUID                               Server-Name
---  -
1    10.78.109.43    NA                                         NA
2    10.78.109.43    NA                                         NA
3    10.78.109.51    4220900d-76d3-89c5-17d7-b5a7d1a2487f  10.78.109.51
switch#

```

Example 5-5 show running-config | include boot Command

```

switch# show running-config | include boot
boot kickstart bootflash:/nexus-1000v-kickstart-mzg.4.2.1.SV1.4a.bin sup-1
boot system bootflash:/nexus-1000v-mzg.4.2.1.SV1.4a.bin sup-1
boot kickstart bootflash:/nexus-1000v-kickstart-mzg.4.2.1.SV1.4a.bin sup-2
boot system bootflash:/nexus-1000v-mzg.4.2.1.SV1.4a.bin sup-2
switch#

```

Example 5-6 show startup-config | include boot Command

```

switch# show startup-config | include boot
boot kickstart bootflash:/nexus-1000v-kickstart-mzg.4.2.1.SV1.4a.bin sup-1
boot system bootflash:/nexus-1000v-mzg.4.2.1.SV1.4a.bin sup-1
boot kickstart bootflash:/nexus-1000v-kickstart-mzg.4.2.1.SV1.4a.bin sup-2
boot system bootflash:/nexus-1000v-mzg.4.2.1.SV1.4a.bin sup-2
switch#

```

Example 5-7 show svcs connections Command

```

switch# show svcs connections

connection vc:
  hostname: 172.23.232.139
  remote port: 80
  protocol: vmware-vim https
  certificate: default
  datacenter name: Hamilton-DC
  DVS uuid: 9b dd 36 50 2e 27 27 8b-07 ed 81 89 ef 43 31 17
  config status: Enabled
  operational status: Connected
  sync status: -
  version: -
switch#

```

Example 5-8 show svcs upgrade status Command

```

switch# show svcs upgrade status
Upgrade State: Start
Upgrade mgmt0 ipv4 addr: 1.1.1.1
Upgrade mgmt0 ipv6 addr:
Upgrade control0 ipv4 addr:
switch#

```

Example 5-9 show system redundancy status Command

```
switch# show system redundancy status
Redundancy role
-----
      administrative: primary
      operational:    primary

Redundancy mode
-----
      administrative: HA
      operational:    HA

This supervisor (sup-1)
-----
      Redundancy state: Active
      Supervisor state: Active
      Internal state:   Active with HA standby

Other supervisor (sup-2)
-----
      Redundancy state: Standby
      Supervisor state: HA standby
      Internal state:   HA standby

switch#
```

Example 5-10 show vmware vem upgrade status Command

```
switch# show vmware vem upgrade status
Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
      VSM: VEM400-201007101-BG
      DVS: VEM400-201007101-BG

switch#
```

