Cisco Nexus 1100 CSP or Cisco Nexus 1010 VSA to Cisco CSP 5000 Migration Guide

First Published: 2018-10-15

Migrating the Cisco Nexus 1000V VSMs

This document describes how to migrate the Cisco Nexus 1000V VSMs in high-availability (HA) pair from Cisco Nexus 1010 Virtual Services Appliance (Cisco Nexus 1010 VSA) or Cisco Nexus 1100 Cloud Services Platform (Cisco Nexus 1100 CSP) to Cisco Cloud Services Platform 5000 (Cisco CSP 5000) while keeping one VSM active at all times.

Prerequisites

Following are the prerequisites for migrating the Cisco Nexus 1000V VSMs while keeping one VSM active:

- Cisco Nexus 1010 VSA or Cisco Nexus 1100 CSP must have Release 4.2(1)SP1(4) or later.
- Layer 2 connectivity must exist between the Cisco Nexus 1010 VSA or Cisco Nexus 1100 CSP and the Cisco CSP 5000.
- Layer 2 or Layer 3 connectivity (depending upon the SVS connection mode) must exist between the Cisco CSP 5000 and the VEMs.

Migrating the Primary VSM

Exporting the Primary VSM

Before you begin

- Log in to the Cisco Nexus 1010 VSA or Cisco Nexus 1110 CSP CLI in EXEC mode.
- Make sure all prerequisites specified in Prerequisites, on page 1 are met.

Procedure

Step 1 Shut down the primary VSM.

Example:

```
n1110-x# config t
n1110-x(config)# virtual-service-blade VSM-test
n1110-x(config-vsb-config)# shutdown primary
```

Step 2 Export the primary VSM to an image file.

Example:

```
n1110-x# export primary
Note: export started..
Note:
 Export operation may take upto 100 minutes. Please be patient..
Note: please be patient..
Note: export completed...
```

Step 3 Identify the image file location and name.

Example:

```
n1110-x# dir bootflash:export-import
4096    Jan 25 20:50:12 2016  5/

Usage for bootflash://sup-local
 2266730496 bytes used
 1724649472 bytes free
 3991379968 bytes total
n1110-x# dir bootflash:export-import/5/
190632137    Jan 25 20:50:30 2016  Vdisk5.img.tar.00
```

Step 4 Copy the image file to an FTP or SFTP server.

Example:

```
n1110-x# copy bootflash:export-import/5/Vdisk5.img.tar.00
ftp://admin@10.10.10.1/share/SV-REPO/Vdisk5.img.tar.00

Enter vrf (If no input, current vrf 'default' is considered):
Password:
***** Transfer of file Completed Successfully *****
Copy complete, now saving to disk (please wait)...
```

Step 5 Make a copy of the VSM configuration. You can use this file as a reference when creating vNICs on Cisco CSP 5000.

Example:

```
n1110-x# show running-config
  virtual-service-blade vsm-test
  virtual-service-blade-type name VSM_SV3-1.6
  interface control vlan 119
  interface control uplink PortChannel1
  interface management vlan 119
  interface management uplink PortChannel1
  interface packet vlan 119
  interface packet uplink PortChannel1
  ramsize 4096
  disksize 3
  numcpu 2
  cookie 744636134
  shutdown primary
  no shutdown secondary
```

Step 6 From the CLI of the active VSM, clear the MAC address of the peer supervisor.

Example:

```
n1000v# peer-sup mac-addresses clear
```

Importing the Primary VSM

This section describes how to import the primary VSM image file to Cisco CSP 5000 by using the web interface. You can also use the Cisco CSP 2100 commands and REST APIs to import the primary VSM.

To import the primary VSM through web interface, do the following:

Procedure

Step 1 Log in to the Cisco CSP web interface.

Step 2 Click the **Configuration** tab and then click the **Repository** tab .

Step 3 On the **Repository Files** page, click **Select**.

Step 4 Select the primary VSM image file exported in the previous section (`Vdisk5.img.tar.00`), click **Open**, and then click **Upload**.

After the VSM image is uploaded, the image name and other relevant information are displayed in the Repository Files table.

Step 5 Click the **Configuration** tab and then click the **Services** tab.

Step 6 On the **Services** page, click **Create** to create a new service for the primary VSM.

Step 7 Enter a name for the service in the **Enter Service Name** field and press **Enter**.

Step 8 Click **Target Host Name** and choose a target host for the primary VSM from the available hosts.

Step 9 Click **Image Name** and choose the imported image (`Vdisk5.img.tar.00`) from the list.

Step 10 Click **vNIC**, create three vNICs for each interface of the VSM, and do the following for each vNIC:

a) Click **VLAN** and enter the same VLAN ID that was used in the primary VSM configuration.
b) Click **Model** and choose **e1000**.
c) Click **Network Name** and specify the name of the uplink.

Tip For the values of these fields, you can refer to the copy of the primary VSM configuration saved in Step 5 of Exporting the Primary VSM, on page 1.

No change is required in the **VLAN Type**, **VLAN Tagged**, and **Native VLAN** fields.

Step 11 Click **Resource Config** and do the following:

a) Click **Number of Cores** and enter the same value that was used in the primary VSM configuration.
b) Click **RAM (MB)** and enter the same value that was used in the primary VSM configuration.

Tip For the values of these fields, you can refer to the copy of the primary VSM configuration saved in Step 5 of Exporting the Primary VSM, on page 1.

No change is required in the **Disk Space (GB)** field.

Step 12 (Optional) Click **VNC Password** and enter a complex alphanumeric password in the **Enter VNC Password** field and the **Repeat Password** field to secure your remote access.

Step 13 Leave the **Storage Config**, **Crypto Bandwidth**, and **Serial Port** fields as they are. No change is required in these fields.

Step 14 Click **Deploy**.

The primary VSM service is deployed and it is automatically powered on.

Verifying High Availability After Importing the Primary VSM

A few minutes after the primary VSM on Cisco CSP 5000 is powered on, the console of the secondary VSM displays messages of the system entering the HA mode as shown in the following example. If these messages are not displayed, verify the layer 2 connectivity between the vnic1 interface on both primary and secondary VSMs.

```
nexus-1000v# 2016 Apr 21 15:14:07 nexus-1000v redun_mgr[2397]:
%REDUN_MGR-4-CTRL_COMM_STATUS_UP:
Control Connectivity is UP with Primary VSM after 114 seconds. Stopping heartbeats on Mgmt
 Interface
2016 Apr 21 15:14:07 nexus-1000v platform[2357]: %PLATFORM-2-MOD_DETECT: Module 1 detected
 (Serial number T4E11773D0D)
Module-Type Virtual Supervisor Module Model Nexus1000V
2016 Apr 21 15:14:34 nexus-1000v bootvar[2441]: %BOOTVAR-5-NEIGHBOR_UPDATE_AUTOCOPY: auto-copy
 supported by neighbor supervisor,
starting...
2016 Apr 21 16:01:33 nexus-1000v %SYSMGR-STANDBY-4-READCONF_STARTED: Configuration update
started (PID 3192).
2016 Apr 21 16:01:37 nexus-1000v %SYSMGR-STANDBY-4-READCONF_STARTED: Configuration update
started (PID 3347).
2016 Apr 21 16:01:38 nexus-1000v %SYSMGR-STANDBY-4-READCONF_STARTED: Configuration update
started (PID 3423).
2016 Apr 21 15:14:57 nexus-1000v module[2436]: %MODULE-5-STANDBY_SUP_OK: Supervisor 1 is
standby
2016 Apr 21 16:01:39 nexus-1000v %SYSMGR-STANDBY-5-MODULE_ONLINE: System Manager has received
 notification of local module
 becoming online.
```

On the secondary (active) VSM, use the **show module** and **show system redundancy status** commands to verify that the VSMs have entered the Active/Standby status.

```
nexus-1000v# sh module
od  Ports  Module-Type                       Model               Status
---  -----  --------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V          ha-standby
2    0      Virtual Supervisor Module         Nexus1000V          active *
[…]

nexus-1000v# sh system redundancy status
Redundancy role
---------------
      administrative:   secondary
         operational:   secondary

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

This supervisor (sup-2)
-----------------------
    Redundancy state:   Active
    Supervisor state:   Active
      Internal state:   Active with HA standby

Other supervisor (sup-1)
------------------------
    Redundancy state:   Standby
    Supervisor state:   HA standby
      Internal state:   HA standby

Peer Sup Mac Adddreses Learnt
--------------------------------------------
   Control Interface:   02:3e:11:77:3d:0d
      Mgmt Interface:   02:4e:11:77:3d:0d

HA Packet Drops Due to Domain id Collision
--------------------------------------------
   Control Interface:   920
      Mgmt Interface:   866
```

Migrating the Secondary VSM

Exporting the Secondary VSM

After verifying that the primary VSM is stable, export the secondary VSM.

Before you begin

- Log in to the Cisco Nexus 1010 VSA or Cisco Nexus 1110 CSP CLI in EXEC mode.
- Make sure all prerequisites specified in Prerequisites, on page 1 are met.

Procedure

Step 1 Shut down the secondary VSM.

Example:

```
n1110-x# config t
n1110-x(config)# virtual-service-blade VSM-test
n1110-x(config-vsb-config)# shutdown secondary
```

Step 2 Delete the existing export files from the `bootflash: export-import` directory.

Example:

```
n1110-x(config-vsb-config)# delete bootflash:export-import/5/
 This is a directory.  Do you want to continue (yes/no)?  [y] y
```

Step 3 Export the secondary VSM to an image file.

Example:

```
n1110-x# export secondary
Note: export started..
Note:
 Export operation may take upto 100 minutes. Please be patient..
Note: please be patient..
Note: export completed...
```

Step 4 Identify the image file location and name.

Example:

```
n1110-x# dir bootflash:export-import
4096    Jan 25 20:50:12 2016  5/
```

```
Usage for bootflash://sup-local
 2266730496 bytes used
 1724649472 bytes free
 3991379968 bytes total
n1110-x# dir bootflash:export-import/5/
190632137    Jan 25 20:50:30 2016  Vdisk5.img.tar.00
```

Step 5 Rename the image file from `Vdisk5.img.tar.00` to `Vdisk5b.img.tar.00`.

Step 6 Copy the image file to an FTP or SFTP server.

Example:

```
n1110-x# copy bootflash:export-import/5/Vdisk5b.img.tar.00
ftp://admin@10.10.10.1/share/SV-REPO/Vdisk5b.img.tar.00

Enter vrf (If no input, current vrf 'default' is considered):
Password:
***** Transfer of file Completed Successfully *****
Copy complete, now saving to disk (please wait)...
```

Step 7 Make a copy of the VSM configuration. You can use this file as a reference when creating vNICs on Cisco CSP 5000.

Example:

```
n1110-x# show running-config
  virtual-service-blade vsm-test
  virtual-service-blade-type name VSM_SV3-1.6
  interface control vlan 119
  interface control uplink PortChannel1
  interface management vlan 119
  interface management uplink PortChannel1
  interface packet vlan 119
  interface packet uplink PortChannel1
  ramsize 4096
  disksize 3
  numcpu 2
  cookie 744636134
  shutdown primary
  shutdown secondary
```

Step 8 From the CLI of the active VSM, clear the MAC address of the peer supervisor.

Example:

```
n1000v# peer-sup mac-addresses clear
```

Importing the Secondary VSM

This section describes how to import the secondary VSM image to Cisco CSP 5000 by using the web interface. You can also use the Cisco CSP 2100 commands and REST APIs to import the secondary VSM.

To import the secondary VSM through web interface, do the following:

Procedure

Step 1 Log in to the Cisco CSP web interface.

Step 2 Click the **Configuration** tab and then click the **Repository** tab .

Step 3 On the **Repository Files** page, click **Select**.

Step 4 Select the secondary VSM image file exported in the previous section (`Vdisk5b.img.tar.00`), click **Open**, and then click **Upload**.

After the VSM image is uploaded, the image name and other relevant information are displayed in the Repository Files table.

Step 5 Click the **Configuration** tab and then click the **Services** tab.

Step 6 On the **Services** page, click **Create** to create a new service for the secondary VSM.

Step 7 Enter a name for the service in the **Enter Service Name** field and press **Enter**.

Step 8 Click **Target Host Name** and choose a target host for the secondary VSM from the available hosts. This host should be different from host for the primary VSM.

Step 9 Click **Image Name** and choose the imported image (`Vdisk5b.img.tar.00`) from the list.

Step 10 Click **vNIC**, create three vNICs for each interface of the VSM, and do the following for each vNIC:

a) Click **VLAN** and enter the same VLAN ID that was used in the secondary VSM configuration.

b) Click **Model** and choose **e1000**.

c) Click **Network Name** and specify the name of the uplink.

Tip For the values of these fields, you can refer to the copy of the secondary VSM configuration saved in Step 7 of Exporting the Secondary VSM, on page 5.

No change is required in the **VLAN Type**, **VLAN Tagged**, and **Native VLAN** fields.

Step 11 Click **Resource Config** and do the following:

a) Click **Number of Cores** and enter the same value that was used in the secondary VSM configuration.

b) Click **RAM (MB)** and enter the same value that was used in the secondary VSM configuration.

Tip For the values of these fields, you can refer to the copy of the secondary VSM configuration saved in Step 7 of Exporting the Secondary VSM, on page 5.

No change is required in the **Disk Space (GB)** field.

Step 12 (Optional) Click **VNC Password** and enter a complex alphanumeric password in the **Enter VNC Password** field and the **Repeat Password** field to secure your remote access.

Step 13 Leave the **Storage Config**, **Crypto Bandwidth**, and **Serial Port** fields as they are. No change is required in these fields.

Step 14 Click **Deploy**.

The secondary VSM service is deployed and it is automatically powered on.

Verifying High Availability After Importing the Secondary VSM

A few minutes after the secondary VSM on Cisco CSP 5000 is powered on, the console of the secondary VSM displays messages of the system entering the HA mode as shown in the following example. If these messages are not displayed, verify the layer 2 connectivity between the vnic1 interface on both primary and secondary VSMs.

```
nexus-1000v# 2016 Apr 21 16:46:35 nexus-1000v redun_mgr[2576]:
%REDUN_MGR-4-CTRL_COMM_STATUS_UP:
Control Connectivity is UP with Secondary VSM after 1017 seconds. Stopping heartbeats on
Mgmt Interface
```

```
2016 Apr 21 16:46:37 nexus-1000v platform[2331]: %PLATFORM-2-MOD_DETECT: Module 2 detected
 (Serial number )
Module-Type Virtual Supervisor Module Model
2016 Apr 21 16:46:50 nexus-1000v bootvar[2726]: %BOOTVAR-5-NEIGHBOR_UPDATE_AUTOCOPY: auto-copy
 supported by neighbor supervisor,
starting...
2016 Apr 21 10:32:23 nexus-1000v %SYSMGR-STANDBY-4-READCONF_STARTED: Configuration update
started (PID 3192).
2016 Apr 21 10:32:27 nexus-1000v %SYSMGR-STANDBY-4-READCONF_STARTED: Configuration update
started (PID 3335).
2016 Apr 21 10:32:28 nexus-1000v %SYSMGR-STANDBY-4-READCONF_STARTED: Configuration update
started (PID 3411).
2016 Apr 21 16:47:12 nexus-1000v module[2721]: %MODULE-5-STANDBY_SUP_OK: Supervisor 2 is
standby
2016 Apr 21 16:47:12 nexus-1000v %SYSMGR-STANDBY-5-MODULE_ONLINE: System Manager has received
 notification of local module
becoming online.
```

On the secondary (active) VSM, use the **show module** and **show system redundancy status** commands to verify that the VSMs have entered the Active/Standby status.

```
nexus-1000v# sh module
Mod  Ports  Module-Type                       Model               Status
---  -----  --------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V          active *
2    0      Virtual Supervisor Module         Nexus1000V          ha-standby
3    1022   Virtual Ethernet Module           NA                  ok
4    1022   Virtual Ethernet Module           NA                  ok
5    1022   Virtual Ethernet Module           NA                  ok
6    4      Virtual Service Module            VXLAN Gateway       ok
7    4      Virtual Service Module            VXLAN Gateway       ok
8    4      Virtual Service Module            VXLAN Gateway       ok
9    4      Virtual Service Module            VXLAN Gateway       ok
10   1022   Virtual Ethernet Module           NA                  ok


nexus-1000v# 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
```