Managing Server Connections

This chapter contains the following sections:

Information About Server Connections

- A connection name
- The protocol used
- The server IP address
- The server DNS name
- Transport mode: IPv4
- All communication with vCenter Server is secured by the Transport Layer Security (TLS) protocol.

Guidelines and Limitations

Follow these guidelines and limitations while configuring server connections:

- A single Virtual Supervisor Module (VSM) can only connect to one vCenter Server at a time.

- A single VSM cannot connect to multiple vCenter Server at once.
- When the SVS connection is in connected state, you can not reconfigure the IP address of the vCenter Server. To the change the IP address, you need to disconnect the SVS connection and change the IP address.

Connecting to the vCenter Server

Before you begin

- Log in to the CLI in EXEC mode.
- You must know the following:
  - The datacenter name.
  - The vCenter Server IP address (IPv4) or hostname.
- You must be sure the following is set up:
  - The vCenter Server management station is installed and running.
  - The ESX servers are installed and running.
  - The Cisco Nexus 1000VE appliance is installed.
  - The management port is configured.
  - The DNS is already configured if you are configuring a connection using a hostname.

Procedure

Step 1 switch# **configure terminal**

Enters global configuration mode.

Step 2 switch(config)# **svs connection** *name*

Enters connection configuration mode for adding this connection between the Cisco Nexus 1000VE and a vCenter Server. By using a name, information for multiple connections can be stored in the configuration.

Step 3 switch(config-svs-conn)# **protocol vmware-vim**

Use this command to specify that this connection uses the VIM protocol.

The default is to use HTTP over SSL (HTTPS).

Step 4 Do one of the following:

- If you are configuring an IP address, go to Step 5.
- If you are configuring a hostname, go to Step 6.

Step 5 switch(config-svs-conn)# **remote ip address** *ipaddress* [vrf {*vrf-name* | `default|management`}

Specifies the IP address of the ESX server or vCenter Server for this connection. This command is stored locally. *vrf-name* is case sensitive and can be a maximum of 32 characters. If a VRF option is not specified, the management VRF is taken by default.

Go to Step 8 to configure the datacenter name.

Step 6 switch(config-svs-conn)# **remote hostname** *hostname*

Specifies the DNS name of the ESX server or vCenter Server for this connection. This command is stored locally.

Note DNS is already configured.

Step 7 switch(config-svs-conn)# **remote port** *port number*

Specifies the HTTP port number of vCenter for this connection. The default port number is 80. Though the communication is HTTPS, vCenter receives the packets on its HTTP port.

Step 8 switch(config-svs-conn)# **vmware dvs datacenter-name** [*folder/*] *name*

Identifies the datacenter name in the vCenter Server where the Cisco Nexus 1000VE is to be created as a distributed virtual switch (DVS). The datacenter name is stored locally.

Note The Cisco Nexus 1000VE folder name must be the same in the vCenter Server and in the VSM. If the Cisco Nexus 1000VE folder is renamed in the vCenter Server, you must manually rename the folder name in the VSM. The names are not automatically synchronized, and if they are not the same, the DVS connection between the VSM and vCenter Server is broken.

Step 9 Do one of the following:

- To use login and password to connect to the vCenter, go to Step 10.
- To register VSM's extension key to connect to the vCenter, go to Step 11

Step 10 switch(config-svs-conn)# **remote username** *user_name* **password** *pwd*

Specifies the DNS name of the ESX server or vCenter Server for this connection. This command is stored locally.

Note DNS is already configured.

Step 11 switch(config-svs-conn)# **register-plugin remote username** *user_name* **password** *pwd*

CLI to register the VSM's extension key with the VMware vCenter.

Step 12 switch(config-svs-conn)# **connect**

Initiates the connection. If the username and password is not configured or the plugin is not registered, then connect will fail indicating the same.

The default is no connect. There can be only one active connection at a time. If a previously defined connection is up, an error message appears and the command is rejected until you close the previous connection by entering no connect.

Note The **connect** command may return the following message, `SVS connection service is busy. Please try again later.`

Example

This example shows how to connect to the vCenter server using IPv4 address:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)#
switch(config)# svs connection vc
switch(config-svs-conn)#
switch(config-svs-conn)# protocol vmware-vim
switch(config-svs-conn)# remote ip address 110.23.43.170
switch(config-svs-conn)# vmware dvs datacenter-name dataCTR

switch(config-svs-conn)# remote username administrator password pwd
switch(config-svs-conn)#
switch(config-svs-conn)# connect



switch#
```

Validating vCenter Server Certificates

The VSM can validate the certificate presented by vCenter Server to authenticate it. The certificate may be self-signed or signed by a Certificate Authority (CA). The validation is done every time the VSM connects to the vCenter Server. If the certificate authentication fails, a warning is generated but the connection is not impaired.

Installing Certificates

Before you begin

Check if a vCenter Server certificate can be received:

1. Enter the following command and store the output of this command in a file, for example, `sconnect_out`.

   ```
   openssl s_client -connect vCenterServer_IPaddress:443 -showcerts
   ```

2. Add information about the certificates in a file named `cacerts.pem`.
3. Verify that a certificate is received from vCenter Server:

   ```
   openssl verify -CAfile cacerts.pem sconnect_out
   ```

For more information about the OpenSSL commands, go to www.openssl.org.

Procedure

Step 1 Create a file named `cacerts.pem` in `bootflash:`.

Step 2 Add a list of trusted certificates in the `cacerts.pem` file.

You can add the self-signed certificate of vCenter Server or the list of root certificate authorities that your security policy allows. The information about each certificate must be included within the following lines:

```
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
```

Verifying vCenter Server Certificates

You can verify the authentication of the vCenter certificates.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

Step 2	switch#(config) **show svs connections**	Verifies the vCenter server certificate.
		If the authentication fails or the `bootflash:/cacerts.pem` file is not present, the following message is displayed:
		`ssl-cert: self-signed or not authenticated`
		In addition, the following warning message is displayed five times or less after every 3 minutes:
		`VMS-1-CONN_SSL_NOAUTH: SSL AUTHENTICATION failure`

Step 3	(Optional) switch#(config) **vmware cert warning disable**	Disables the display of the warning messages. **Note** Although this command is hidden in the CLI, the command is available for use.

Example

This example shows how to verify the vCenter server certificate and how to disable the display of warning messages, if the authentication fails.

```
switch# configure terminal
switch#(config) show svs connections
```

```
connection vc:
    ip address: 110.23.43.170
    remote port: 80
    protocol: vmware-vim https
    certificate: default
    ssl-cert: ssl-cert: self-signed or not authenticated
VMS-1-CONN_SSL_NOAUTH: SSL AUTHENTICATION failure
VMS-1-CONN_SSL_NOAUTH: SSL AUTHENTICATION failure
VMS-1-CONN_SSL_NOAUTH: SSL AUTHENTICATION failure
VMS-1-CONN_SSL_NOAUTH: SSL AUTHENTICATION failure
VMS-1-CONN_SSL_NOAUTH: SSL AUTHENTICATION failure
switch#(config) vmware cert warning disable
switch#(config)

. . .
```

Disconnecting From the vCenter Server

You can disconnect from vCenter Server, for example, after correcting a vCenter Server configuration.

Before you begin

- Log in to the Cisco Nexus 1000VE in EXEC mode.
- Configure a Cisco Nexus 1000VE connection.
- Connect the Cisco Nexus 1000VE to vCenter Server/ESX.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **svs connection** *name*	Enters global configuration submode for the connection to vCenter Server.
Step 3	switch(config-svs-conn)# **no connect**	Closes the connection.

Example

This example shows how to disconnect from vCenter Server:

```
switch# configure terminal
switch# (config#) svs connection vcWest
switch# (config-svs-conn)# no connect
```

Removing the DVS from the vCenter Server

You can use remove the Distributed Virtual Switch (DVS) from the vCenter Server.

Before you begin

- Log in to the Cisco Nexus 1000VE in EXEC mode.
- Configure a connection to the vCenter Server.
- Connect the Cisco Nexus 1000VE to the vCenter Server/ESX.
- Check that the server administrator has removed all of the hosts that are connected to the Cisco Nexus 1000VE from the VM client. For more information, see the VMware documentation.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **svs connection** *name*	Enters global configuration submode for the connection to the vCenter Server.
Step 3	switch(config-svs-conn)# **no vmware dvs**	Removes the DVS associated with the specified connection from the vCenter Server.

Example

```
switch# configure terminal
switch(config)# svs connection vcWest
switch(config-svs-conn)# no vmware dvs
```

Removing the DVS from the vCenter Server when the VSM Is Not Connected

You can configure whether or not you will allow administrators to delete a DVS when the VSM is not connected to the vCenter Server.

Procedure

Step 1 Configure the admin user or group. See Configuring the Admin User or Admin Group, on page 8.

Step 2 Remove the DVS from the vCenter Server. See Removing the DVS from the vCenter Server, on page 6.

Configuring the Admin User or Admin Group

Before you begin

- Ensure that the system administrator has created an admin user or admin group on vCenter Server to manage and delete the DVS. This user should not be given any other permissions such as deploying VMs or hosts, and so on.
- The admin user name configured on the VSM is the same as the username on vCenter Server.

Procedure

Step 1 Determine the name of the DVS.

Step 2 Configure the admin user in vCenter Server.

Note You can also configure an admin group by entering the **admin group** *groupname* command.

Step 3 Verify that the admin user has been created.

Example

This example shows how to configure the admin user or an admin group on vCenter Server.

```
switch# show svs connections

connection VC:
    ipaddress: 10.104.63.16
    remote port: 80
    protocol: VMware-vim https
    certificate: default
    datacenter name: N1K-DC
    admin:
    DVS uuid: a2 …
    dvs version: 5.0
    config status: Enabled
    operational status: Connected
    sync status: Complete
    version: VMware vCenter Server 4.1.0 build 258902

switch# configure terminal
switch(config)# svs connection VC
switch(config-svs-conn) # admin user NAuser
switch(config-svs-conn) #show svs connections

connection VC:
    ipaddress: 10.104.63.16
    remote port: 80
    protocol: VMware-vim https
    certificate: default
    datacenter name: N1K-DC
    admin: NAuser(user)
    DVS uuid: a2 …
    dvs version: 5.0
    config status: Enabled
```

```
operational status: Connected
sync status: Complete
version: VMware vCenter Server 4.1.0 build 258902
```

Removing the DVS from the vCenter Server Using the Graphical User Interface

Procedure

Step 1 Log in to vCenter Server through the VMware vSphere Client with the admin user account.

Step 2 In the **vSphere Client** left pane, choose the data center.

Step 3 Choose **Hosts and Clusters** > **Networking**.

Step 4 Right-click the **DVS** and choose **Remove**.

Configuring Host Mapping

This section includes the following topics:

- Information about Host Mapping
- Removing Host Mapping from a Module
- Mapping to a New Host
- Viewing Host Mapping

Information about Host Server Connections

When a VSM detects a new Virtual Service Engine (VSE), it automatically assigns a free module number to the VSE and then maintains the mapping between the module number and the universally unique identifier (UUID) of a VSE. This mapping is used to assign the same module number to a given VSE.

Removing Host Mapping from a Module

Before you begin

- Log in to the Cisco Nexus 1000VE in EXEC mode.
- Remove the host from the Cisco Nexus 1000VE DVS on the vCenter.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **no vse** *module-number*	Removes the specified module from the software. **Note** If the module is still present in the slot, the command is rejected, as shown in this example.
Step 3	(Optional) switch(config)# **show module vse mapping**	Displays the mapping of modules to host servers.
Step 4	switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to remove a host mapping from a specified VSE module:

```
switch# configure terminal
switch(config)# no vse 4
switch(config)# no vse 3
cannot modify slot 3: host module is inserted
switch(config)# show module vse mapping
Mod     Status          UUID                                    License Status
---     ----------      ------------------------------------    --------------
  3      powered-up     93312881-309e-11db-afa1-0015170f51a8    licensed
switch(config-vse-slot)# copy running-config startup-config
```

Mapping to a New Host

Before you begin

- Log in to the CLI in EXEC mode.
- Remove the host from the Cisco Nexus 1000VE DVS on the vCenter.

Note If you do not first remove the existing host server mapping, the new host server is assigned a different module number.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **vse** *module number*	Enters VSE slot configuration mode.
Step 3	switch(config-vse-slot)# **host vmware id** *vse-uuid*	Assigns a different VSE UUID to the specified module.

	Command or Action	Purpose
Step 4	(Optional) switch(config-vse-slot)# **show module vse mapping**	Displays the mapping of modules to host servers.
Step 5	switch(config-vse-slot)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to map a host server to a module:

```
switch# configure terminal
switch(config)# vse 3
switch(config-vse-slot)# host vmware id 6dd6c3e3-7379-11db-abcd-000bab086eb6
switch(config-vse-slot)# show module vse mapping
Mod     Status          UUID                                 License Status
---     ----------      ------------------------------------ --------------
  3      powered-up     93312881-309e-11db-afa1-0015170f51a8    licensed
  4          absent     6dd6c3e3-7379-11db-abcd-000bab086eb6    licensed

switch(config-vse-slot)# copy running-config startup-config
```

Viewing Host Mapping

You can view the mapping of modules to host servers.

Command	Description
show module vse mapping	Displays the mapping on modules to host servers.

This example shows how to view the mapping of a module:

```
Mod Status      UUID                                 License Status
--- ----------- ------------------------------------ --------------
3   powered-up  93312881-309e-11db-afa1-0015170f51a8  licensed
switch(config)#
```

Verifying Connections

You can view and verify connections.

Commands	Description

show svs connections [*name*]	Displays the current connections to the Cisco Nexus 1000VE. **Note** Network connectivity issues may shut down your connection to the vCenter Server. When network connectivity is restored, the Cisco Nexus 1000VE will not automatically restore the connection. In this case, you must restore the connection manually using the following command sequence: **no connect** **connect**

Before you begin

- Log in to the CLI in any command mode.
- Configure the connection using the Connecting to the vCenter Server, on page 2 procedure.
- Know that the Cisco Nexus 1000VE is connected to vCenter Server.

Procedure

	Command or Action	Purpose
Step 1		

Example

This example shows how to verify a connection:

```
switch# show svs connections VC
Connection vc:
IP address: 172.28.15.206
Protocol: vmware-vim https
datacenter name: HamiltonDC
admin: NAuser(user)
DVS uuid: a2 …
dvs version: 5.0
config status: Enabled
operational status: Connected

n1000v#
```

Verifying the Domain

You can view and verify the configured domain.

Commands	Description
show svs domain	Display the domain configured on the Cisco Nexus 1000V.

Before you begin

- Log in to the CLI in any command mode.
- Configure a domain using the Creating a Domain procedure.

Verifying the Configuration

Use one of the following commands to verify the configuration.

Command	Description
show running-config	Displays the current configuration. If the Cisco Nexus 1000VE is not connected to a vCenter Server or ESX server, the output is limited to connection-related information.
show svs connections [*name*]	Displays the current connections to the Cisco Nexus 1000VE. **Note** Network connectivity issues might shut down your connection to the vCenter Server. When network connectivity is restored, the Cisco Nexus 1000VE will not automatically restore the connection. In this case, you must restore the connection manually using the **no connect** command followed by the **connect** command.
show svs domain	Displays the domain configured on the Cisco Nexus 1000VE.
show module	Displays module information.
show interface brief	Displays interface information.
show interface virtual	Displays virtual interface information.
show module vse mapping	Displays the mapping of modules to host servers.

Verifying the Module Information

You can display and verify module information, including a view of the DVS from the Cisco Nexus 1000VE.

Before you begin

- Log in to the CLI in any command mode.
- Configure the Cisco Nexus 1000VE connection using the Connecting to the vCenter Server procedure.
- Know that the Cisco Nexus 1000VE is connected to the vCenter Server.
- Know that the server administrator has already added the host running the Cisco Nexus 1000VE to the DVS in the vCenter Server.

Procedure

Step 1 **show module**

Example:

```
n1kve# show module
Mod  Ports  Module-Type                       Model               Status
---  -----  --------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V          active *
3    1022   Virtual Service Engine            NA                  ok
4    1022   Virtual Service Engine            NA                  ok
5    1022   Virtual Service Engine            NA                  ok

Mod  Sw                Hw
---  ----------------  ------------------------------------------------
1    5.2(1)SV5(1.1)    0.0
3    5.2(1)SV5(1.1)    NA
4    5.2(1)SV5(1.1)    NA
5    5.2(1)SV5(1.1)    NA

Mod  Server-IP        Server-UUID                          Server-Name
---  ---------------  -----------------------------------  --------------------
1    10.197.128.101   NA                                   NA
3    10.197.128.122   4213D2CA-1D9A-FE4E-6368-9E4B4F74B3AE  localhost.localdomai
n
4    10.197.128.123   42136761-CB7A-7AE8-B81B-7504E7309AF8  localhost.localdomai
n
5    10.197.128.124   4213B1A8-6CCB-5C5B-ACF0-064C7900F3C5  localhost.localdomai
n

Mod  VSE-IP           Host-IP
---  ---------------  -----------------------------------
3    10.197.128.122   10.197.128.89
4    10.197.128.123   10.197.128.93
5    10.197.128.124   10.197.128.90

* this terminal session
================================================================================
```

Displays module information.

Step 2 show interface brief

Example:

```
n1kve# show interface brief
--------------------------------------------------------------------------------
Port     VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0    --           up     16.1.0.103                              1000     1500

--------------------------------------------------------------------------------
Ethernet     VLAN    Type Mode    Status  Reason                     Speed    Port
Interface                                                                    Ch #
--------------------------------------------------------------------------------
Eth3/1       1       eth  trunk   up      none                       10G
Eth4/1       1       eth  trunk   up      none                       10G
Eth5/1       1       eth  trunk   up      none                       10G

--------------------------------------------------------------------------------
Vethernet    VLAN/    Type Mode    Status  Reason                      MTU  Module
             Segment
```

```
--------------------------------------------------------------------------------
Veth1         1602     virt access  up      none                    1500 4
Veth2         1602     virt access  up      none                    1500 4
Veth3         1602     virt access  up      none                    1500 5
Veth4         1602     virt access  up      none                    1500 5

--------------------------------------------------------------------------------
Port     VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
control0 --           up     --                                      1000     1500

NOTE : * Denotes ports on modules which are currently offline on VSM
```

Displays interface information, including the uplinks to the vCenter Server.

Step 3 **show interface virtual**

Example:

```
n1kve# show interface virtual
-------------------------------------------------------------------------------
Port        Adapter        Owner                    Mod Host
-------------------------------------------------------------------------------
Veth1       Net Adapter 1  vm14                      4   localhost.localdomain
Veth2       Net Adapter 1  vm12                      4   localhost.localdomain
Veth3       Net Adapter 1  vm13                      5   localhost.localdomain
Veth4       Net Adapter 1  vm11                      5   localhost.localdomain
n1kve#
```

Displays virtual interface information.

Verifying the Module Information Using the vCenter Server

You can display and verify module information using the vCenter Server. The following alarms are raised in the vCenter Server based on the condition.

All alarms are cleared when the VSM disconnects from the vCenter Server.

Alarm	Description
<*Host-Ref_Name*> Online	This alarm is raised as a warning on the host object. It indicates that the VSE is online in the VSM. This alarm persists as long as the VSE is communicating with the VSM and the VSE is online.
<*Host-Ref_Name*> Offline	This alarm is raised as an alert on the host object. It indicates that the VSE is offline in the VSM. This alarm is cleared when the VSE comes online.
<*Host-Ref_Name*> Deleted from VSM	This alarm is raised as a warning on the host object. It indicates that the VSE is being removed from the VSM but it is not removed from the DVS. This alarm is cleared when the VSE is detected as a module in the VSM.

Alarm	Description
<*Host-Ref_Name*> Update failed in VSM	This alarm is raised as an alert on the host object. It indicates that the VSE has already been removed from the VSM but updates are still being received from the vCenter Server. There can be connectivity issues between the VSM and the VSE. This alarm can coexist with the <*Host-Ref_Name*> Deleted from VSM alarm. This alarm is cleared when the VSE is detected as a module in the VSM.