CHAPTER 6

Restricting Port Profile Visibility

This chapter describes the commands used to restrict visibility of port profiles to a user or a group of users and includes the following sections:

Information About Port Profile Visibility

You can restrict which vCenter users or user groups have visibility into specific port groups on the Cisco Nexus 1000V.

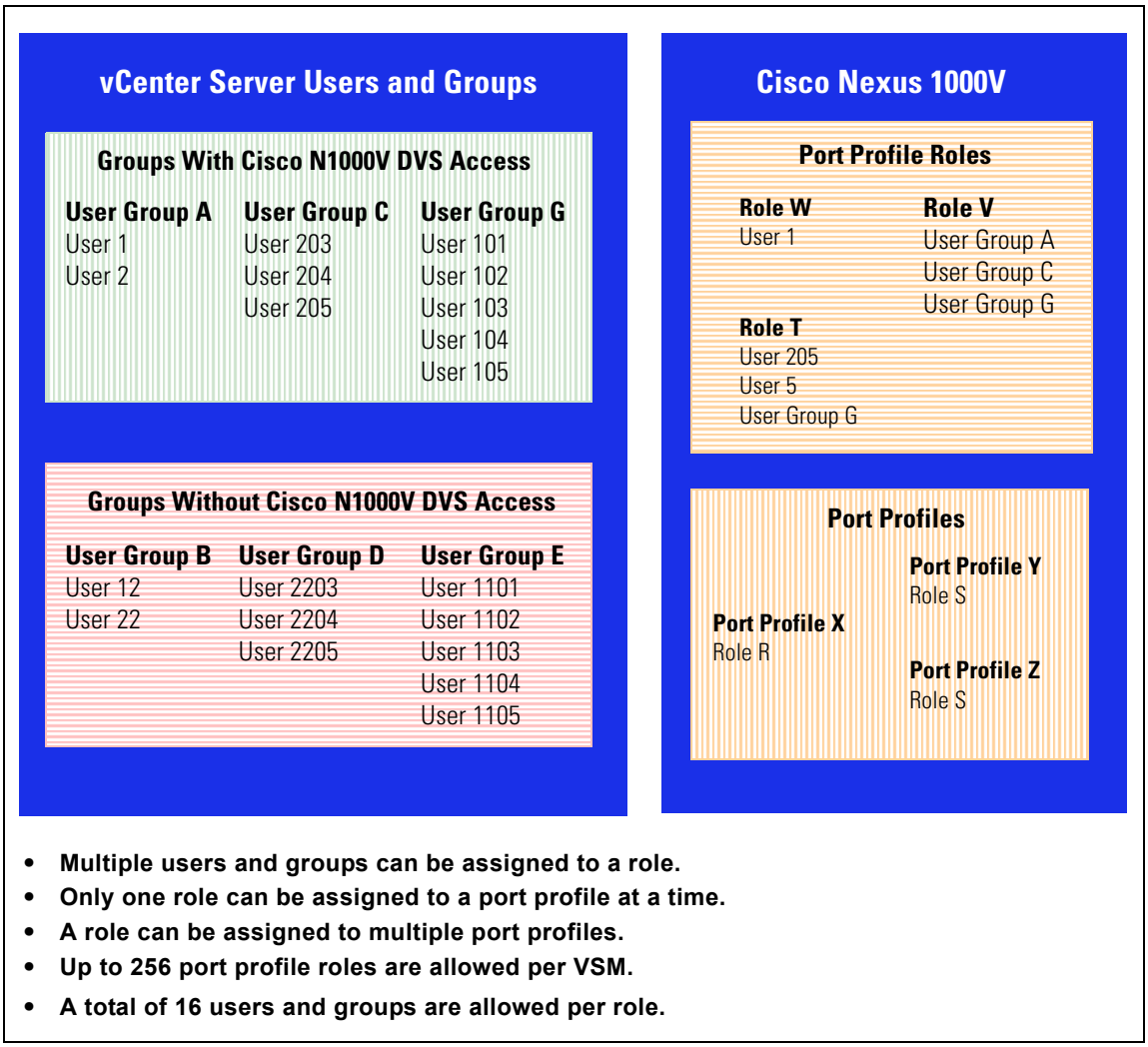
Before you can restrict the visibility of a port group, the server administrator must define which vCenter users and user groups have access to the Cisco Nexus 1000V DVS top level folder in vCenter server. Once this is done, the network administrator can further define the visibility of specific port groups on the VSM. This configuration on the VSM is then published to the vCenter server so that access to specific port groups is restricted.

Allow Groups or Users

You can save the time of defining access on the VSM per user by, instead, adding new users to groups in vCenter where access is already defined. Group members defined in vCenter automatically gain access to the port groups defined for the group.

You can see in Figure 6-1 the relationship between users and groups in vCenter server and port profiles and port profile roles in Cisco Nexus 1000V.

Figure 6-1 Port Profile Visibility: Users, Groups, Roles, and Port Profiles



- **Multiple users and groups can be assigned to a role.**
- **Only one role can be assigned to a port profile at a time.**
- **A role can be assigned to multiple port profiles.**
- **Up to 256 port profile roles are allowed per VSM.**
- **A total of 16 users and groups are allowed per role.**

Guidelines and Limitations

Use the following guidelines and limitations when restricting port profile visibility:

- The server administrator does not propagate access from the DVS down to lower folders. Instead, port group access is defined by the network administrator on the VSM and then published to the vCenter server.
- The Cisco Nexus 1000V VSM must be connected to the vCenter Server before port profile roles are created or assigned. If this connection is not in place when port profile visibility is updated on the VSM, it is not published to vCenter server and is not affected.
- The following are guidelines for port profile roles on the VSM:
  - You cannot remove a port profile role if a port profile is assigned to it. You must first remove the role from the port profile.
  - Multiple users and groups can be assigned to a role.

  - Only one role can be assigned to a port profile.
  - A role can be assigned to multiple port profiles.
- You can define up to 256 port-profile-roles per VSM.
- You can define a total of 16 users and groups per role.

Defining DVS Access in vSphere Client

The server administrator can use this procedure to allow access to the top level Cisco Nexus 1000V DVS folder in vSphere client.

BEFORE YOU BEGIN

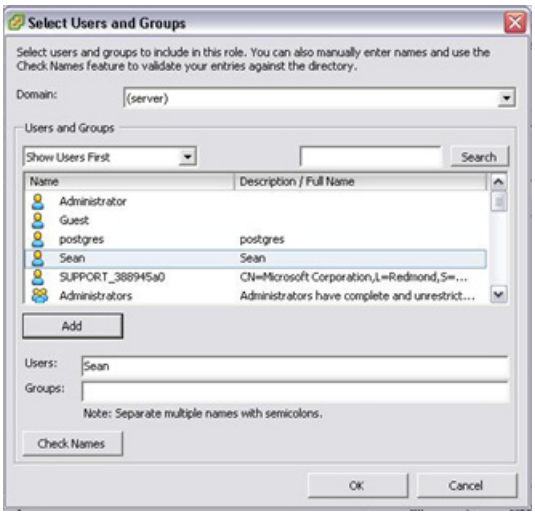
Before beginning this procedure, you must know or do the following:

- You are logged in to vSphere client.
- You know which users or groups need access to the DVS.
- This procedure defines who can access the Cisco Nexus 1000V DVS. Access to individual port groups is done on the VSM, using the "Restricting Port Profile Visibility on the VSM" procedure on page 6-6.

DETAILED STEPS

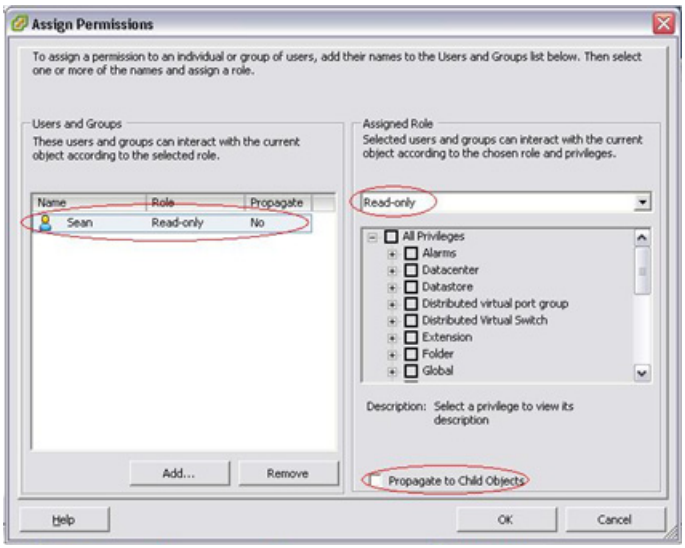
Step 1 From Inventory > Networking, right-click the Cisco Nexus 1000V DVS folder, and choose **Add Permission**.

The Select Users and Groups dialog box opens.



Step 2 Choose the name from the list of users and groups and click **Add**. Then click **OK**.

The Assign Permissions dialog box opens.



Step 3 From the Assigned Role selection list, choose a role for this user or group.

The user is granted the same access to the DVS object. In the example shown, user Sean is granted read-only access to the DVS folder object and eventually the DVS object.

Step 4 Make sure that the Propagate to Child Objects box is unchecked.

Note Do not propagate the role definition here. Specific port group access is configured on the VSM which is then pushed to vSphere client.

Step 5 Click **OK**.

The user may now access the top level Cisco Nexus 1000V DVS folder according to the assigned role.

Step 6 To restrict access to specific port groups, go to the "Restricting Port Profile Visibility on the VSM" procedure on page 6-6.

Enabling the Port Profile Role Feature

The network administrator can use this procedure to enable the port profile role feature on the VSM.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **config t**
2. **feature port-profile-role**
3. (Optional) **show feature**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Description
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**feature port-profile-role** **Example:** n1000v(config)# **feature port-profile-role adminUser** n1000v(config)#	Enables the port profile roles feature to restrict user and group access.

	Command	Description
Step 3	**show feature** **Example:** n1000v (config)# **show feature** Feature Name Instance State -------------------- -------- -------- dhcp-snooping 1 enabled http-server 1 enabled ippool 1 enabled lacp 1 enabled lisp 1 enabled lisphelper 1 enabled netflow 1 disabled port-profile-roles 1 enabled private-vlan 1 disabled sshServer 1 enabled tacacs 1 enabled telnetServer 1 enabled n1000v(config)#	(Optional) Displays the configuration for verification.
Step 4	**copy running-config startup-config** **Example:** n1000v(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Restricting Port Profile Visibility on the VSM

The network administrator can use this procedure to create a role for restricting port profile visibility on the VSM which is then pushed to vCenter server.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You know which users or groups should have access to the role you are creating.
- You have already created the users and groups to be assigned to this role in vCenter and have access to the Cisco Nexus 1000V DVS folder where the VSM resides. See the "Defining DVS Access in vSphere Client" procedure on page 6-3.
- You have enabled the port profile role feature using the "Enabling the Port Profile Role Feature" procedure on page 6-5.
- You have identified the characteristics needed for this role:
  - role name
  - role description
  - users to assign
  - groups to assign
  - port profile to assign

SUMMARY STEPS

1. **config t**
2. **port-profile-role** *role-name*
3. (Optional) **description** *role-description*
4. (Optional) **show port profile role users**
5. (Optional) **user** *user-name*

   (Optional) **group** *group-name*
6. **exit**
7. **port-profile** [**type** {**ethernet** | **vethernet**}] *profile-name*
8. **assign port-profile-role** *role-name*
9. (Optional) **show port-profile-role** [**name** *role-name*]
10. **copy running-config startup-config**

DETAILED STEPS

	Command	Description
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**port-profile-role** *role-name* **Example:** n1000v(config)# **port-profile-role adminUser** n1000v(config-port-prof-role)#	Enters port profile role configuration mode for the named role. If the role does not already exist, it is created with the following characteristic: • *role-name*—The role name can be up to 32 characters and must be unique for each role on the Cisco Nexus 1000V.
Step 3	**description** *role-description* **Example:** n1000v(config-port-profile-role)# **description adminOnly** n1000v(config-port-profile-role)#	(Optional) Adds a description of up to 32 characters to the role. This description is automatically pushed to vCenter Server.

Step 4	**show port-profile-role users**
	
	Example:
	n1000v(config-port-profile-role)# **show port-profile-role users**
	Groups:
	  Administrators
	  TestGroupB
	Users:
	  dbaar
	  fgreen
	  suchen
	  mariofr
	n1000v(config-port-profile-role)#
		(Optional) Displays all the users on vCenter Server who have access to the DVS parent folder and who can be assigned to the role.

	Command	Description
Step 5	**Enter one or more of the following:** **user** *user-name* **group** *group-name* **Example:** n1000v(config-port-profile-role)# **user hdbaar** n1000v(config-port-profile-role)# **Example:** n1000v(config-port-profile-role)# **group credit** n1000v(config-port-profile-role)#	(Optional) Assigns a user or a group to the role. The user or group gains the ability to use all port profiles assigned to the role. **Note** Multiple users and groups can be assigned to a role. **Note** The users and groups must exist on vCenter server and must have access to the top level Cisco Nexus 1000V DVS folder in vSphere client. For more information, see the "Defining DVS Access in vSphere Client" procedure on page 6-3.
Step 6	**exit** **Example:** n1000v(config-port-profile-role)# **exit** n1000v(config)#	Exits port-profile-role configuration mode and returns you to global configuration mode.
Step 7	**port-profile** *profile-name* **Example:** n1000v(config)# **port-profile allaccess2** n1000v(config-port-prof)#	Enters port profile configuration mode for the named port profile.
Step 8	**assign port-profile-role** *role-name* **Example:** n1000v(config-port-prof)# **assign port-profile-role adminUser** n1000v(config-port-prof)#	Assigns the role to a port profile. The port group is updated in vCenter Server and the user or group assigned to this role is granted access. The user or group can assign the port group to a vNIC in a virtual machine or vSWIF or vMKNIC on a host. **Note** Only one role can be assigned to a port profile. **Note** A role can be assigned to multiple port profiles.
Step 9	**show port-profile-role** [**name** *role-name*] **Example:** n1000v(config-port-prof)# **show port-profile-role name adminUser** Name: adminUser Description: adminOnly Users: hdbaar (user) Assigned port-profiles: allaccess2 n1000v(config-port-prof)#	(Optional) Displays the configuration for verification.
Step 10	**copy running-config startup-config** **Example:** n1000v(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

This example shows how to define access for the allaccess2 port profile by creating and assigning the adminUser port profile role.

```
config t
port-profile-role adminUser
description adminOnly
user hdbaar
exit
port-profile allaccess2
assign port-profile-role adminUser
show port-profile-role name adminUser

Name: adminUser
Description: adminOnly
Users:
    hdbaar (user)
Assigned port-profiles:
    allaccess2
copy running-config startup-config
```

Removing a Port Profile Role

You can use this procedure to remove a role that was used for restricting port profile visibility on vCenter server.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You cannot remove a port profile role if a port profile is assigned to it. You must first remove the role from the port profile. This procedure includes a step for doing this.

SUMMARY STEPS

1. **show port-profile-role** [**name** *role-name*]
1. **config t**
2. **port-profile** [**type** {**ethernet** | **vethernet**}] *profile-name*
3. **no assign port-profile-role** *role-name*
4. **exit**
5. **no port-profile-role** *role-name*
6. (Optional) **show port-profile-role** [**name** *role-name*]
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Description
Step 1	**show port-profile-role** [**name** *role-name*] **Example:** n1000v(config-port-prof)# **show port-profile-role name adminUser** Name: adminUser Description: adminOnly Users: hdbaar (user) Assigned port-profiles: allaccess2 n1000v(config-port-prof)#	(Optional) Displays the port profile role including any port profiles assigned to it. If there are port profiles assigned to the role, they must be removed before you can remove the role.
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**port-profile** *profile-name* **Example:** n1000v(config)# **port-profile allaccess2** n1000v(config-port-prof)#	Enters port profile configuration mode for the named port profile.
Step 3	**no assign port-profile-role** *role-name* **Example:** n1000v(config-port-prof)# **no assign port-profile-role adminUser** n1000v(config-port-prof)#	Removes the role from the port profile. The port group is updated in vCenter Server.
Step 4	**exit** **Example:** n1000v(config-port-profile)# **exit** n1000v(config)#	Exits port-profile configuration mode and returns you to global configuration mode.
Step 5	**no port-profile-role** *role-name* **Example:** n1000v(config)# **no port-profile-role adminUser** n1000v(config)#	Removes the role from the VSM.
Step 6	**show port-profile-role** [**name** *role-name*] **Example:** n1000v(config-port-prof)# **show port-profile-role name adminUser**	(Optional) Displays the configuration for verification.
Step 7	**copy running-config startup-config** **Example:** n1000v(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Feature History for Restricting Port Profile Visibility

This section provides the feature history for restricting port profile visibility.

Feature Name	Releases	Feature Information
Restricting Port Profile Visibility	4.2(1)SV1(4)	This feature was introduced.