SAN-Engineer   Govindagouda Ranganagoudar

CISCO Nexus 5000 FCOE to Brocade 48000   Leave a comment

Best Practice Design Technology Considerations

Notes:

•Each virtual Fibre Channel interface must be bound to an FCoE-enabled Ethernet interface.

FCoE is supported on 10-Gigabit Ethernet interfaces.

•Each virtual Fibre Channel interface is associated with only one VSAN.

•Any VSAN with associated virtual Fibre Channel interfaces must be mapped to a dedicated FCOE-enabled VLAN.

•FCoE is not supported on private VLANs. •Enable NPV feature

Design Example

Nexus-brocade.png (http://docwiki.cisco.com/wiki/File:Nexus-brocade.png)

Configuration Example(s)

!configure FCoE enabled vlan to assosiate with the vsan (vsan to vlan mapping) !

```
Create VSAN 30

vlan 30
 fcoe vsan 30
 name FCoE
! !configure the layer 2 server vlan !

vlan 1200
 name servers_test
! !configure the trunks connecting to the storage system (ethernet trunk) !

interface Ethernet1/30
 description HP Chassis C7000
 switchport mode trunk
 switchport trunk native vlan 1200
 switchport trunk allowed vlan 30,1200
 spanning-tree port type edge trunk
!

interface Ethernet1/32
 description HP Chassis C7000-NIC2
 switchport mode trunk
 switchport access vlan 1200
 switchport trunk native vlan 1200
 switchport trunk allowed vlan 30,1200
 spanning-tree port type edge trunk
! !configure the virtual fiber channel –The FC portion of FCoE is configured as a vfc interface. !

interface vfc30
 bind interface Ethernet1/30
 no shutdown
!

interface vfc32
 bind interface Ethernet1/32
 no shutdown
! !create the vsan, give it a name and associate ports with it (vsan to vlan mapping) !

vsan database
 vsan 30 name "FCoE"
!

vsan database
 vsan 30 interface vfc30
 vsan 30 interface vfc32
 vsan 30 interface fc2/1
 vsan 30 interface fc2/2
!!

interface fc2/1
 switchport mode NP
 switchport description Brocade_48000
 no shutdown
!
```

```
interface fc2/2
 switchport mode F
 switchport description C7000
 no shutdown
```

Upgrade the Cisco NEXUS Switches This one I followed for the 5548UP

ping 1101.36.139.102 vrf management

Remarks: Copy the file from the FTP server to the Boot Flash

copy ftp://anonymous@101.36.139.102/n5000-uk9-kickstart.5.2.1.N1.3.bin bootflash: vrf management
copy ftp://anonymous@101.36.139.102/n5000-uk9.5.2.1.N1.3.bin bootflash: vrf management

Remarks: Check the Compatibility of the New Code on the HArdware

show incompatibility system bootflash:n5000-uk9.5.2.1.N1.3.bin

Remarks: Check the checksum

show file n5000-uk9-kickstart.5.2.1.N1.3.bin md5sum
Remarks: Check the current Upgrade Method which will be impacting the host
show span issu-impact

Remarks: check the Install Impact with Features

sh install all impact system bootflash:n5000-uk9.5.2.1.N1.3.bin kickstart bootflash:n5000-uk9-kickstart.5.2.1.N1.3.bin

Remarks: Install the code

install all system bootflash:n5000-uk9.5.2.1.N1.3.bin kickstart bootflash:n5000-uk9-kickstart.5.2.1.N1.3.bin

```
Remarks:

show span issu-impact
sh run | i boot
sh run | i image
```

Unified Port Configurations on Cisco Nexus 5500 Platform Switches

Unified ports allow you to configure ports as Ethernet, native Fibre Channel or FCoE ports. By default, the ports are Ethernet ports but you can change the port mode to Fibre Channel on the following unified ports:

- Any port on the Cisco Nexus 5548UP switch or the Cisco Nexus 5596UP switch.

- The ports on the Cisco N55-M16UP expansion module that is installed in a Cisco Nexus 5548P switch.

This example shows how to configure a unified port on a Cisco Nexus 5548UP switch or Cisco Nexus 5596UP switch:

```
switch# config t
switch(config)# slot 1
switch(config-slot)# port 32 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

This example shows how to configure a unified port on a Cisco N55-M16UP expansion module:

```
switch# config t
switch(config)# slot 2
switch(config-slot)# port 32 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

Port Order

You must configure Ethernet ports and FC ports in a specified order:

- FC ports must be configured from the last port of the module.

- Ethernet ports must be configured from the first port of the module.

If the order is not followed, the following errors are displayed:

```
ERROR: Ethernet range starts from first port of the module
ERROR: FC range should end on last port of the module
```

On a Cisco Nexus 5548UP switch, the 32 ports of the main slot (slot1) are unified ports. The Ethernet ports start from port 1/1 to port 1/32. The FC ports start from port 1/32 backwards to port 1/1.

This example shows how to configure 20 ports as Ethernet ports and 12 as FC ports:

```
switch# config t
switch(config)# slot 1
switch(config-slot)# port 21-32 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

Configuring Switch Port Attribute Default Values

You can configure attribute default values for various switch port attributes. These attributes will be applied globally to all future switch port configurations, even if you do not individually specify them at that time.To configure switch port attributes, perform this task:

SUMMARY STEPS1. switch# configuration terminal

2. switch(config)# no system default switchport shutdown san

3. switch(config)# system default switchport shutdown san

4. switch(config)# system default switchport trunk mode auto

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configuration terminal	Enters configuration mode.
Step 2	switch(config)# no system default switchport shutdown san	Configures the default setting for administrative state of an interface as Up. (The factory default setting is Down). **Tip** This command is applicable only to interfaces for which no user configuration exists for the administrative state.
Step 3	switch(config)# system default switchport shutdown san	Configures the default setting for administrative state of an interface as Down. This is the factory default setting. **Tip** This command is applicable only to interfaces for which no user configuration exists for the administrative state.
Step 4	switch(config)# system default switchport trunk mode auto	Configures the default setting for administrative trunk mode state of an interface as Auto. **Note** The default setting is trunk mode on.

About N Port Identifier Virtualization

N port identifier virtualization (NPIV) provides a means to assign multiple FC IDs to a single N port. This feature allows multiple applications on the N port to use different identifiers and allows access control, zoning, and port security to be implemented at the application level. The following figure shows an example application using NPIV.

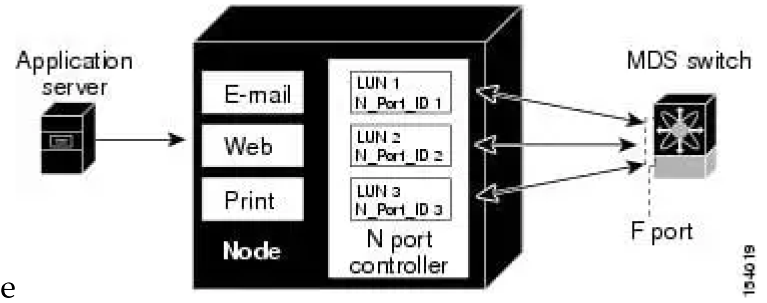

Figure 1. NPIV Example

Enabling N Port Identifier Virtualization

To enable or disable NPIV on the switch, perform this task:
Before You Begin You must globally enable NPIV for all VSANs on the switch to allow the NPIV-enabled applications to use multiple N port identifiers.

Note All of the N port identifiers are allocated in the same VSAN.

SUMMARY STEPS1. switch# configuration terminal

2. switch(config)# feature npiv

3. switch(config)# no feature npiv

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configuration terminal	Enters configuration mode.
Step 2	switch(config)# feature npiv	Enables NPIV for all VSANs on the switch.
Step 3	switch(config)# no feature npiv	Disables (default) NPIV on the switch.

Example Port Channel Configurations

This section shows examples on how to configure an F port channel in shared mode and how to bring up the link between F ports on the NPIV core switches and NP ports on the NPV switches. Before you configure the F port channel, ensure that F port trunking, F port channeling, and NPIV are enabled. This example shows how to create the port channel:

```
switch(config)# interface port-channel 2
switch(config-if)# switchport mode F
switch(config-if)# switchport  dedicated
switch(config-if)# channel mode active
switch(config-if)# exit
```

This example shows how to configure the port channel member interfaces on the core switch in dedicated mode:

```
switch(config)# interface fc1/4-6
switch(config-if)# shut
switch(config-if)# switchport mode F
switch(config-if)# switchport speed 4000
switch(config-if)# switchport rate-mode dedicated
switch(config-if)# switchport trunk mode on
switch(config-if)# channel-group 2
switch(config-if)# no shut
switch(config-if)# exit
```

This example shows how to create the port channel in dedicated mode on the NPV switch:

```
switch(config)# interface san-port-channel 2
switch(config-if)# switchport mode NP
switch(config-if)# no shut
switch(config-if)# exit
```

This example shows how to configure the port channel member interfaces on the NPV switch:

```
switch(config)# interface fc2/1-2
switch(config-if)# shut
switch(config-if)# switchport mode NP
switch(config-if)# switchport trunk mode on
switch(config-if)# channel-group 2
switch(config-if)# no shut
switch(config-if)# exit
```

Verifying Fibre Channel Interfaces

Verifying SFP Transmitter Types

The SPF transmitter type can be displayed for a physical Fibre Channel interface (but not for a virtual Fibre Channel).The small form-factor pluggable (SFP) hardware transmitters are identified by their acronyms when displayed in the show interface briefcommand. If the related SFP has a Cisco-assigned extended ID, then the show interface and show interface brief commands display the ID instead of the transmitter type. The show interface transceiver command and the show interface fc *slot*/*port* transceiver command display both values for Cisco supported SFPs.

Verifying Interface Information

The show interface command displays interface configurations. If no arguments are provided, this command displays the information for all the configured interfaces in the switch.You can also specify arguments (a range of interfaces or multiple, specified interfaces) to display interface information. You can specify a range of interfaces by entering a command with the following example format: interface fc2/1 – 4 , fc3/2 – 3The following example shows how to display all interfaces:

```
switch# show interface

fc3/1 is up
...
fc3/3 is up
...
Ethernet1/3 is up
...
mgmt0 is up
...
vethernet1/1 is up
...
vfc 1 is up
```

The following example shows how to display multiple specified interfaces:

```
switch# show interface fc3/1 , fc3/3
fc3/1 is up
...
fc3/3 is up
...
```

The following example shows how to display a specific interface:

```
switch# show interface vfc 1

vfc 1 is up
...
```

The following example shows how to display interface descriptions:

```
switch# show interface description
-------------------------------------------------
Interface          Description
-------------------------------------------------
fc3/1              test intest
Ethernet1/1              --
vfc 1              --
...
```

The following example shows how to display all interfaces in brief:

```
switch# show interface brief
```

The following example shows how to display interface counters:

```
switch# show interface counters
```

The following example shows how to display transceiver information for a specific interface:

```
switch# show interface fc3/1 transceiver
```

Information About User Accounts

Access to the Cisco Nexus 1000V is accomplished by setting up user accounts that define the specific actions permitted by each user. You can create up to 256 user accounts. Each user account includes the following criteria:

- Role (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1366476)

- User Name (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1362573)

- Password (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1366627)

- Expiration Date (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1367889)

Role

A role is a collection of rules that define the specific actions that can be shared by a group of users. The following broadly defined roles, for example, can be assigned to user accounts. These roles are predefined in the Cisco Nexus 1000V and cannot be modified:

```
role: network-admin
  description: Predefined network admin role has access to all commands
  on the switch
  -------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  -------------------------------------------------------------------
  1       permit  read-write
role: network-operator
  description: Predefined network operator role has access to all read
  commands on the switch
  -------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  -------------------------------------------------------------------
  1       permit  read
```

You can create an additional 64 roles that define access for users.

Each user account must be assigned at least one role and can be assigned up to 64 roles.

You can create roles that, by default, permit access to the following commands only. You must add rules to allow users to configure features.

- **show**
- **exit**
- **end**
- **configure terminal**

Table 2-1 (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1362524) describes the components that make up a role.

Table 2-1 Role Components

Component	**Description**

Rule	One of the defined role criteria, such as a command that is permitted or denied. You can add up to 256 rules to each role.The following are the rules for the predefined roles:• role: network-admin
	`---------------------------------------------------------`
	`  Rule    Perm    Type        Scope               Entity`
	`  ---------------------------------------------------------`
	`  1       permit  read-write`
	• role: network-operator
	`---------------------------------------------------------`
	`  Rule    Perm    Type        Scope               Entity`
	`  ---------------------------------------------------------`
	`  1       permit  read-only`

Feature	An individual feature, such as syslog or TACACS+, whose access can be defined in a rule. To see a list of available features, use the **show role feature** command.
Feature Group	A grouping of features whose access can be defined in a rule. You can create up to 64 such groupings. To see a list of available feature groups, use the **show role feature-group** command.
Command	A single command, or group of commands collected in a regular expression, whose access can be defined in a rule.A role permitting access to a command takes precedence over a role that denies access to the command. For example, if a user is assigned a role that denies access to the configuration command, but is also assigned a role that permits access to this command, then access is permitted.

User Name

A user name identifies an individual user by a unique character string, such as daveGreen. User names are case sensitive and can consist of up to 28 alphanumeric characters. A user name consisting of all numerals is not allowed. If an all numeric user name exists on an AAA server and is entered during login, the user is not logged in.

Password

A password is a case-sensitive character string that enables access by a specific user and helps prevent unauthorized access. You can add a user without a password, but they may not be able to access the device. Passwords should be strong so that they cannot be easily guessed for unauthorized access.

The following characters are not permitted in clear text passwords:

- dollar signs ($)

- spaces

The following special characters are not permitted at the beginning of the password:

- quotation marks (" or ')

- vertical bars (|)

- right angle brackets (>)

Table 2-2 (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1377280) lists the characteristics of strong passwords.

Table 2-2 Characteristics of strong passwords

Strong passwords have:	**Strong passwords do not have:**
• At least eight characters• Uppercase letters• Lowercase letters • Numbers • Special characters	• Consecutive characters, such as "abcd"• Repeating characters, such as "aaabbb"• Dictionary words • Proper names

The following are examples of strong passwords:

- If2CoM18

- 2004AsdfLkj30

- Cb1955S21

Check of Password Strength

The device checks password strength automatically by default. When you add a user name and password, the strength of the password is evaluated. If it is a weak password, then the error message below displays to notify you.

```
n1000v# config t
n1000v(config)# username daveGreen password davey
password is weak
Password should contain characters from at least three of the classes:
 lower case letters,upper case letters, digits, and special characters
```

Password strength-checking can be disabled.

Expiration Date

By default, a user account does not expire. You can, however, explicitly configure an expiration date on which the account will be disabled.

Guidelines and Limitations

User access has the following configuration guidelines and limitations:

- You can create up to 64 roles in addition to the two predefined user roles.
- You can create up to 256 rules in a user role.
- You can create up to 64 feature groups.
- You can add up to 256 users.
- You can assign a maximum of 64 user roles to a user account.
- If you have a user account that has the same name as a remote user account on an AAA server, the user roles for the local user account are applied to the remote user, not the user roles configured on the AAA server.

Default Settings

Table 2-3 (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1377358) lists the default settings for user access.

Table 2-3 User Access Defaults

Parameters	**Default**
User account password	Undefined
User account expiration date.	None
User account role	Network-operator
Interface policy	All interfaces are accessible.
VLAN policy	All VLANs are accessible.

Configuring User Access

This section includes the following topics:

- Enabling the Check of Password Strength (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1340882)

- Disabling the Check of Password Strength (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1363337)

- Creating a User Account (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1330442)

- Creating a Role (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1076741)

- Creating a Feature Group (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1373370)

- Configuring Interface Access (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1244194)

- Configuring VLAN Access (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1373158)

Enabling the Check of Password Strength

Use this procedure to enable the Cisco Nexus 1000V to check the strength of passwords to avoid creating weak passwords for user accounts.

BEFORE YOU BEGIN

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

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

- Checking password strength is enabled by default. This procedure can be used to enable it again should it become disabled.

SUMMARY STEPS

1. **config t**

2 **password strength-check**

3 **show password strength-check**

4 **copy running-config startup-config**

DETAILED STEPS

	Command	**Purpose**
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into the CLI Global Configuration mode.
Step 2	**password strength-check** **Example:** n1000v(config)# password strength-check	Enables password-strength checking. The default is enabled.You can disable the checking of password strength by using the**no** form of this command.

Step 3	**show password strength-check** **Example:** n1000v# show password strength-check Password strength check enabled n1000v(config)#	(Optional) Displays the configuration for checking password strength.
Step 4	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Disabling the Check of Password Strength

Use this procedure to disable the check of password strength.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- Checking password strength is enabled by default. This procedure can be used to disable it.

SUMMARY STEPS

1. **config t**

2 no password strength-check

3 show password strength-check

4 copy running-config startup-config

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into the CLI Global Configuration mode.
Step 2	**no password strength-check** **Example:** n1000v(config)# no password strength-check n1000v(config)#	Disables password-strength checking.The default is enabled.
Step 3	**show password strength-check** **Example:** n1000v# show password strength-check Password strength check not enabled n1000v(config)#	(Optional) Displays the configuration for checking password strength.
Step 4	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Creating a User Account

Use this procedure to create and configure a user account, defining access to the Cisco Nexus 1000V.

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 can add up to 256 user accounts.
- Changes to user accounts do not take effect until the user logs in and creates a new session.
- Do not use the following words in user accounts. These words are reserved for other purposes.

	admbindaemon	gdmgopherhaltlp	mtsusernewsnobody	rpcusershutdownsync
	ftp	mail	nscd	sys
	ftpuser	mailnull	operator	uucp
	games	man	rpc	xfs

- You can add a user password as either clear text or encrypted.

– Clear text passwords are encrypted before they are saved to the running configuration.

– Encrypted passwords are saved to the running configuration without further encryption.

- A user account can have up to 64 roles, but must have at least one role. For more information about roles, see the “Role” section (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1366476).
- If you do not specify a password, the user might not be able to log in.
- For information about using SSH public keys instead of passwords, see the “Configuring a User Account with a Public Key” section on page 7-5 (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_7ssh.html#wpxref11067).

SUMMARY STEPS

1. **config t**

2 **show role**

3 **username** *user-name* [password [0 | 5]*password*] [expire *date*] [role *role-name*]

4 **show user-account** *user-name*

5 **copy running-config startup-config**

DETAILED STEPS

	Command	**Purpose**
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into the CLI Global Config
Step 2	**show role** **Example:** n1000v(config)# show role	(Optional) Displays the available role (http://www.cisco.com/en/US/docs/sv

Step 3	`username` *`name`* `[`**`password`**` [`**`0`**` | `**`5`**`] `*`password`*`]`
	`[expire date] [role `*`role-name`*`]`
	Example:
	n1000v(config)# username NewUser password 4Ty18Rnt
		Creates a user account.•name: A ca undefined.
		–**0** = (the default) Specifies that the
		running configuration.
		In the example shown, the password4
		–**5** = Specifies that the password yo
		running configuration.
		User passwords are not displayed in t
		•expire date: YYYY-MM-DD. The default is no expiration date.
		•role: You must assign at least one

Step 4	**`show user-account`** `username`
	`Example:`
	`n1000v(config)# show user-account NewUser`
	`user:NewUser`
	`  this user account has no expiry date`
	`  roles:network-operator network-admin`
	`n1000v(config)#`
		Displays the new user account config

Step 5	**`copy running-config startup-config`** **Example:** n1000v# copy running-config startup-config	(Optional) Saves the running configu

Creating a Role

Use this procedure to create a role defining a set of specific actions that are permitted or denied. This role will be assigned to users whose access requirements match the actions defined.

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 can configure up to 64 user roles.

- You can configure up to up to 256 rules for each role.

- You can assign a single role to more that one user.

- The rule number specifies the order in which it is applied, in descending order. For example, if a role has three rules, rule 3 is applied first, rule 2 is applied next, and rule 1 is applied last.

- By default, the user roles that you create allow access only to the **show**, **exit**, **end**, and **configure terminal** commands. You must add rules to allow users to configure features.

SUMMARY STEPS

1. **config t**

2 **role name** *role-name*

3 (Optional) **description** string

4 **rule** *number* {**deny** | **permit**} **command** command-string

rule *number* {**deny** | **permit**} {**read** | **read-write**}

rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature** feature-name

rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** group-name

5 **Repeat** 4 (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1330702) **to create all needed rules for this role.**

6 **show role**

7 **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**`config t`** **Example:** n1000v# config t n1000v(config)#	Places you into the CLI Global Configuratio
Step 2	**`role name`** *`role-name`* **Example:** n1000v(config)# role name UserA n1000v(config-role)#	Names a user role and places you in Role C alphanumeric string of up to 16 characters.
Step 3	**`description`** *`description-string`* **Example:** n1000v(config-role)# description Prohibits use of clear commands	(Optional) Configures the role description,

Step 4	**rule** number {**deny** | **permit**} **command** *command-string* **Example:** n1000v(config-role)# rule 1 deny command clear users	Creates a rule to permit or deny a specific co expressions. For example, "interface etherne denies access to the **clear users**command.
	rule number {**deny** | **permit**} {**read** | **read-write**} **Example:** n1000v(config-role)# rule 2 deny read-write	Creates a blanket rule to permit or deny all operation.
	rule number {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name* **Example:** n1000v(config-role)# rule 3 permit read feature eth-port-sec	Creates a rule for feature access.Use the **sho** example rule permits users read-only access
	rule number {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name* **Example:** n1000v(config-role)# rule 4 deny read-write feature-group eth-port-sec	Creates a rule for feature group access.Use t groups.This example configures a rule deny
Step 5	Repeat Step 4 (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/securi create all needed rules for the specified role.	
Step 6	**show role** **Example:** n1000v(config)# show role	(Optional) Displays the user role configurat
Step 7	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	(Optional) Saves the running configuration configuration.

Creating a Feature Group

Use this procedure to create and configure a feature group.

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 can create up to 64 custom feature groups.

SUMMARY STEPS

1. **config t**

2 **role feature-group name** group-name

3 show role feature

4 **feature** feature-name

5 Repeat 4 (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1330976) for all features to be added to the feature group.

6 **show role feature-group**

7 **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into the CLI Global Configuratio

Step 2	**role feature-group name**group-name **Example:** n1000v(config)# role feature-group name GroupA n1000v(config-role-featuregrp)#	Places you into the Role Feature Group Con sensitive, alphanumeric string of up to 32 ch
Step 3	**show role feature** **Example:** n1000v(config-role-featuregrp)# show role feature feature: aaa feature: access-list feature: cdp feature: install . . . n1000v(config-role-featuregrp)#	Displays a list of available features for use ir
Step 4	**feature** feature-name **Example:** n1000v(config-role-featuregrp)# feature syslog n1000v(config-role-featuregrp)#	Adds a feature to the feature group.
Step 5	Repeat Step 6 (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/securi all features to be added to the feature group.	

Step 6	**show role feature-group** **Example:** n1000v(config-role-featuregrp)# show role feature-group feature group: GroupA feature: syslog feature: snmp feature: ping n1000v(config-role-featuregrp)#	(Optional) Displays the feature group config
Step 7	**copy running-config startup-config** **Example:** n1000v(config-role-featuregrp)# copy running-config startup-config	(Optional) Saves the running configuration configuration.

Configuring Interface Access

Use this procedure to configure interface access for a specific role.

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 have already created one or more user roles using the "Creating a Role" procedure (http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security_2useracct.html#wp1076741). In this procedure, you will be modifying a role you have already created.

- By default, a role allows access to all interfaces. In this procedure you will, first, deny access to all interfaces and then permit access to selected interfaces.

SUMMARY STEPS

1. **config t**

2 **role name** role-name

3 **interface policy deny**

4 **permit interface** interface-list

5 **show role**

6 **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into the CLI Global Configuration mode.
Step 2	**role name** *role-name* **Example:** n1000v(config)# role name network-observer n1000v(config-role)#	Specifies a user role and enters Role Configuration mode for the named role.
Step 3	**interface policy deny** **Example:** n1000v(config-role)# interface policy deny n1000v(config-role-interface)#	Enters the Interface Configuration mode, and denies all interface access for the role.Access to any interface must now be explicitly defined for this role using the **permit interface** command.

Step 4	**permit interface** *interface-list* **Example:** n1000v(config-role-interface)# permit interface ethernet 2/1-4	Specifies the interface(s) that users assigned to this role can access.Repeat this command to specify all interface lists that users assigned to this role are permitted to access.
Step 5	**show role** *role-name* **Example:** n1000v(config-role-interface)# show role name network-observer role: network-observer description: temp Vlan policy: permit (default) Interface policy: deny Permitted interfaces: Ethernet2/1-4	(Optional) Displays the role configuration.
Step 6	**copy running-config startup-config** **Example:** n1000v(config-role-featuregrp)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Posted January 12, 2013 by g6237118