CHAPTER 6

Configuring User Accounts and RBAC

This chapter describes how to configure user accounts and role-based access control (RBAC) on NX-OS devices.

This chapter includes the following sections:

Information About User Accounts and RBAC

You can create and manage users accounts and assign roles that limit access to operations on the NX-OS device. RBAC allows you to define the rules for an assign role that restrict the authorization that the user has to access management operations.

This section includes the following topics:

About User Accounts

You can configure up to a maximum of 256 user accounts. By default, the user account does not expire unless you explicitly configure it to expire. The expire option determines the date when the user account is disabled.

Users can have user accounts on multiple VDCs. These users can move between VDCs after an initial connection to a VDC.

Tip The following words are reserved and cannot be used to configure users: bin, daemon, adm, lp, sync, shutdown, halt, mail, news, uucp, operator, games, gopher, ftp, nobody, nscd, mailnull, root, rpc, rpcuser, xfs, gdm, mtsuser, ftpuser, man, and sys.

Note User passwords are not displayed in the configuration files.

Caution The Cisco NX-OS software does not support all numeric usernames, whether created with TACACS+ or RADIUS, or created locally. Local users with all numeric names cannot be created. If an all numeric user name exists on an AAA server and is entered during login, the user is not logged in.

Characteristics of Strong Passwords

A strong password has the following characteristics:

- At least eight characters long
- Does not contain many consecutive characters (such as “abcd”)
- Does not contain many repeating characters (such as “aaabbb”)
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

The following are examples of strong passwords:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

Note Clear text passwords cannot contain dollar signs ($) or spaces anywhere in the password. Also, they cannot include these special characters at the beginning of the password: quotation marks (" or '), vertical bars (|), or right angle brackets (>).

Tip If a password is trivial (such as a short, easy-to-decipher password), the NX-OS software will reject your password configuration if password-strength checking is enabled (see the "Enabling Password-Strength Checking" section on page 6-5). Be sure to configure a strong password as shown in the sample configuration. Passwords are case sensitive.

About User Roles

User roles contain rules that define the operations allowed for the user who is assigned the role. Each user role can contain multiple rules and each user can have multiple roles. For example, if role1 allows access only to configuration operations, and role2 allows access only to debug operations, then users who belong to both role1 and role2 can access configuration and debug operations. You can also limit access to specific VLANs, virtual routing and forwarding instances (VRFs), and interfaces.

The Cisco NX-OS software provides four default user roles:

- network-admin—Complete read-and-write access to the entire NX-OS device (only available in the default VDC)
- network-operator—Complete read access to the entire NX-OS device (only available in the default VDC)
- vdc-admin—Read-and-write access limited to a VDC
- vdc-operator—Read access limited to a VDC

Note You cannot change the default user roles.

You can create custom roles within a VDC. 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 display or configure features.

The VDCs do not share user roles. Each VDC maintains an independent user role database. Within a VDC, roles are configured by rule and attribute assignment.

Note If you belong to multiple roles, you can execute a combination of all the commands permitted by these roles. Access to a command takes priority over being denied access to a command. For example, suppose a user has RoleA, which denied access to the configuration commands. However, the user also has RoleB, which has access to the configuration commands. In this case, the user has access to the configuration commands.

About User Role Rules

The rule is the basic element of a role. A rule defines what operations the role allows the user to perform. You can apply rules for the following parameters:

- Command—A command or group of commands defined in a regular expression.
- Feature—Commands that apply to a function provided by the NX-OS software.
- Feature group—Default or user-defined group of features.

These parameters create a hierarchical relationship. The most basic control parameter is the command. The next control parameter is the feature, which represents all commands associated with the feature. The last control parameter is the feature group. The feature group combines related features and allows you to easily manage the rules. The NX-OS software also supports the predefined feature group L3 that you can use.

You can configure up to 256 rules for each role. The user-specified rule number determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

Virtualization Support

The users with the network-admin and network-operator roles can operate in all virtual device contexts (VDCs) when logged in from the default VDC and use the **switchto vdc** command to access other VDCs. All other user roles are local to the VDC. Roles are not shared between VDCs. Each VDC maintains an independent user role database. For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.0*.

Licensing Requirements for User Accounts and RBAC

The following table shows the licensing requirements for this feature:

Product	License Requirement
NX-OS	User accounts and RBAC require no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0*.

Guidelines and Limitations

User accounts and RBAC have the following configuration guidelines and limitations:

- You can create up to 64 user-defined roles in a VDC in addition to the four default user roles in the default VDC and the two default user roles in the nondefault VDCs.
- You can add up to 256 rules to a user role.
- You can add up to 64 user-defined feature groups to a VDC in addition to the default feature group, L3.
- You can configure up to 256 users in a VDC.
- You can assign a maximum of 64 user roles to a user account.
- If you have a user account configured on the local Cisco NX-OS device that has the same name as a remote user account on an AAA server, the Cisco NX-OS software applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Note A user account must have at least one user role.

Enabling Password-Strength Checking

In Cisco NX-OS Release 4.0(3) and later releases, you can enable password-strength checking which prevents you from creating weak passwords for user accounts. For information about strong passwords, see the "Characteristics of Strong Passwords" section on page 6-2.

BEFORE YOU BEGIN

Ensure that you are in the desired VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **password strength-check**
3. **exit**
4. **show password strength-check**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**password strength-check** **Example:** `switch(config)# password strength-check`	Enables password-strength checking. The default is enabled. You can disable password-strength checking by using the **no** form of this command.

Step 3	**exit**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	**show password strength-check** **Example:** `switch# show password strength-check`	(Optional) Displays the password-strength check configuration.
Step 5	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring User Accounts

You can create a maximum of 256 user accounts on an NX-OS device. User accounts have the following attributes:

- Username
- Password
- Expiry date
- User roles

You can enter the password in clear text format or encrypted format. The Cisco NX-OS password encrypts clear text passwords before saving them to the running configuration. Encrypted format passwords are saved to the running configuration without further encryption.

User accounts can have a maximum of 64 user roles. For more information on user roles, see the "Configuring RBAC" section on page 6-8.

User accounts are local to a VDC. However, users with the network-admin or network-operator role can log in to the default VDC and access other VDCs using the **switchto vdc** command.

Note Changes to user account attributes do not take effect until the user logs in and creates a new session.

BEFORE YOU BEGIN

Ensure that you are in the desired VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **show role**
3. **username** *user-id* [**password** [**0** | **5**]*password*] [**expire** *date*] [**role** *role-name*]
4. **exit**
5. **show user-account**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**show role** **Example:** `switch(config)# show role`	(Optional) Displays the user roles available. You can configure other user roles, if necessary (see the "Creating User Roles and Rules" section on page 6-8)

	Command	Purpose
Step 3	**username** *user-id* [**password** [**0** | **5**] *password*] [**expire** *date*] [**role** *role-name*] **Example:** `switch(config)# username NewUser password 4Ty18Rnt`	Configure a user account. The *user-id* argument is a case-sensitive, alphanumeric character string with a maximum length of 28 characters. **Note** Do not include the "#" or "@" character in the *user-id* argument. These characters are reserved for special use in the command-line interface (CLI). The default password is undefined. The **0** option indicates that the password is clear text and the **5** option indicates that the password is encrypted. The default is **0** (clear text). **Note** If you do not specify a password, the user might not be able to log in to the NX-OS device. For information about using SSH public keys instead of passwords, see the "Specifying the SSH Public Keys for User Accounts" section on page 5-5. The **expire** *date* option format is YYYY-MM-DD. The default is no expiry date. User accounts can have a maximum of 64 user roles. In the default VDC, the default role is **network-operator** if the creating user has the network-admin role, or the default role is **vdc-operator** if the creating user has the vdc-admin role. In non-default VDCs, the default user role is **vdc-operator**. **Note** The network-admin and network-operator roles are only available in the default VDC.

Step 4	**exit**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 5	**show user-account** **Example:** `switch# show user-account`	(Optional) Displays the role configuration.
Step 6	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring RBAC

This section includes the following topics:

Creating User Roles and Rules

You can configure up to 64 user roles in a VDC. Each user role can have up to 256 rules. You can assign a user role to more that one user account.

The rule number that you specify determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

BEFORE YOU BEGIN

Ensure that you are in the desired VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **role name** *role-name*
3. **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*
4. **description** *text*
5. **exit**
6. **show role**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**role name** *role-name*
	
	Example:
	`switch(config)# role name UserA`
	`switch(config-role)#`
		Specifies a user role and enters role configuration mode. The *role-name* argument is a case-sensitive, alphanumeric character string with a maximum length of 16 characters.

Step 3	**rule** *number* {**deny** | **permit**} **command** *command-string* **Example:** `switch(config-role)# rule 1 deny command clear users`	Configures a command rule. The *command-string* argument can contain spaces and regular expressions. For example, "interface ethernet *" includes all Ethernet interfaces. Repeat this command for as many rules as needed.
	rule *number* {**deny** | **permit**} {**read** | **read-write**} **Example:** `switch(config-role)# rule 2 deny read-write`	Configures a read-only or read-and-write rule for all operations.
	rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name* **Example:** `switch(config-role)# rule 3 permit read feature router-bgp`	Configures a read-only or read-and-write rule for a feature. Use the **show role feature** command to display a list of features. Repeat this command for as many rules as needed.
	rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name* **Example:** `switch(config-role)# rule 4 deny read-write L3`	Configures a read-only or read-and-write rule for a feature group. Use the **show role feature-group** command to display a list of feature groups. Repeat this command for as many rules as needed.
Step 4	**description** *text* **Example:** `switch(config-role)# description This role does not allow users to use clear commands`	(Optional) Configures the role description. You can include spaces in the description.

Step 5	**exit**
	
	Example:
	`switch(config-role)# exit`
	`switch(config)#`
		Exits role configuration mode.

	Command	Purpose
Step 6	**show role** **Example:** `switch(config)# show role`	(Optional) Displays the user role configuration.
Step 7	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Creating Feature Groups

You can create custom feature groups to add to the default list of features provided by the Cisco NX-OS software. These groups contain one or more of the features. You can create up to 64 feature groups in a VDC.

Note You cannot change the default feature group L3.

BEFORE YOU BEGIN

Ensure that you are in the desired VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **role feature-group** *group-name*
3. **feature** *feature-name*
4. **exit**
5. **show role feature-group**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**role feature-group** *group-name*
	
	Example:
	`switch(config)# role feature GroupA`
	`switch(config-role-featuregrp)#`
		Specifies a user role feature group and enters role feature group configuration mode.
		
		The *group-name* argument is a case-sensitive, alphanumeric character string with a maximum length of 32 characters.

	Command	Purpose
Step 3	**feature** *feature-name* **Example:** `switch(config-role-featuregrp)# feature vdc`	Specifies a feature for the feature group. Repeat this command for as many features as needed. **Note** Use the **show role component** command to display a list of features.

Step 4	**exit**
	
	Example:
	`switch(config-role-featuregrp)# exit`
	`switch(config)#`
		Exits role feature group configuration mode.

Step 5	**show role feature-group** **Example:** `switch(config)# show role feature-group`	(Optional) Displays the role feature group configuration.
Step 6	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Changing User Role Interface Policies

You can change a user role interface policy to limit the interfaces that the user can access. By default, a user role allows access to all interfaces in the VDC.

BEFORE YOU BEGIN

Ensure that you are in the desired VDC (or use the **switchto vdc** command).

Create one or more user roles (see the "Creating User Roles and Rules" section on page 6-8).

SUMMARY STEPS

1. **config t**
2. **role name** *role-name*
3. **interface policy deny**
4. **permit interface** *interface-list*
5. **exit**
6. **show role**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**role name** *role-name* **Example:** switch(config)# role name UserA switch(config-role)#	Specifies a user role and enters role configuration mode.
Step 3	**interface policy deny** **Example:** switch(config-role)# interface policy deny switch(config-role-interface)#	Enters role interface policy configuration mode.
Step 4	**permit interface** *interface-list* **Example:** switch(config-role-interface)# permit interface ethernet 2/1-4	Specifies a list of interfaces that the role can access. Repeat this command for as many interfaces as needed.
Step 5	**exit** **Example:** switch(config-role-interface)# exit switch(config-role)#	Exits role interface policy configuration mode.
Step 6	**show role** **Example:** switch(config-role)# show role	(Optional) Displays the role configuration.
Step 7	**copy running-config startup-config** **Example:** switch(config-role)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Changing User Role VLAN Policies

You can change a user role VLAN policy to limit the VLANs that the user can access. By default, a user role allows access to all VLANs in the VDC.

BEFORE YOU BEGIN

Ensure that you are in the desired VDC (or use the **switchto vdc** command).

Create one or more user roles (see the "Creating User Roles and Rules" section on page 6-8).

SUMMARY STEPS

1. **config t**
2. **role name** *role-name*

3. **vlan policy deny**
4. **permit vlan** *vlan-range*
5. **exit**
6. **show role**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**role name** *role-name* **Example:** switch(config)# role name UserA switch(config-role)#	Specifies a user role and enters role configuration mode.
Step 3	**vlan policy deny** **Example:** switch(config-role)# vlan policy deny switch(config-role-vlan)#	Enters role VLAN policy configuration mode.
Step 4	**permit vlan** *vlan-list* **Example:** switch(config-role-vlan)# permit vlan 1-4	Specifies a range of VLANs that the role can access. Repeat this command for as many VLANs as needed.
Step 5	**exit** **Example:** switch(config-role-vlan)# exit switch(config-role)#	Exits role VLAN policy configuration mode.
Step 6	**show role** **Example:** switch(config-role)# show role	(Optional) Displays the role configuration.
Step 7	**copy running-config startup-config** **Example:** switch(config-role)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Changing User Role VRF Policies

You can change a user role VRF policy to limit the VRFs that the user can access. By default, a user role allows access to all VRFs in the VDC.

BEFORE YOU BEGIN

Ensure that you are in the desired VDC (or use the **switchto vdc** command).

Create one or more user roles (see the "Creating User Roles and Rules" section on page 6-8).

SUMMARY STEPS

1. **config t**
2. **role name** *role-name*
3. **vrf policy deny**
4. **permit vrf** *vrf-name*
5. **exit**
6. **show role**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**role name** *role-name*
	
	Example:
	`switch(config)# role name UserA`
	`switch(config-role)#`
		Specifies a user role and enters role configuration mode.

Step 3	**vrf policy deny**
	
	Example:
	`switch(config-role)# vrf policy deny`
	`switch(config-role-vrf)#`
		Enters role VRF policy configuration mode.

Step 4	**permit vrf** *vrf-name* **Example:** `switch(config-role-vrf)# permit vrf vrf1`	Specifies the VRF that the role can access. Repeat this command for as many VRFs as needed.

Step 5	**exit**
	
	Example:
	`switch(config-role-vrf)# exit`
	`switch(config-role)#`
		Exits role VRF policy configuration mode.

Step 6	**show role** **Example:** `switch(config-role)# show role`	(Optional) Displays the role configuration.
Step 7	**copy running-config startup-config** **Example:** `switch(config-role)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Verifying User Accounts and RBAC Configuration

To display user account and RBAC configuration information, perform one of the following tasks:

Command	Purpose
show role	Displays the user role configuration.
show role feature	Displays the feature list.
show role feature-group	Displays the feature group configuration.
show startup-config security	Displays the user account configuration in the startup configuration.
show running-config security [**all**]	Displays the user account configuration in the running configuration. The **all** keyword displays the default values for the user accounts.
show user-account	Displays user account information.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.

Example User Accounts and RBAC Configuration

The following example shows how to configure a user role:

```
role name UserA
  rule 3 permit read feature l2nac
  rule 2 permit read feature dot1x
  rule 1 deny command clear *
```

The following example shows how to configure a user role feature group:

```
role feature-group name Security-features
  feature radius
  feature tacacs
  feature dot1x
  feature aaa
  feature l2nac
  feature acl
  feature access-list
```

Default Settings

Table 6-1 lists the default settings for user accounts and RBAC parameters.

Table 6-1 Default User Accounts and RBAC Parameters

Parameters	Default
User account password	Undefined.
User account expiry date.	None.

Table 6-1 Default User Accounts and RBAC Parameters (continued)

Parameters	Default
User account role in the default VDC	Network-operator if the creating user has the network-admin role, or vdc-operator if the creating user has the vdc-admin role.
User account role in the non-VDCs	Vdc-operator if the creating user has the vdc-admin role.
Default user roles in the default VDC	Network-admin, network-operator, vdc-admin, and vdc-operator.
Default user roles in the non-default VDCs	Vdc-admin and vdc-operator.
Interface policy	All interfaces are accessible.
VLAN policy	All VLANs are accessible.
VRF policy	All VRFs are accessible.
Feature group	L3.

Additional References

For additional information related to implementing RBAC, see the following sections:

- Related Documents, page 6-16
- Standards, page 6-16
- MIBs, page 6-17

Related Documents

Related Topic	Document Title
NX-OS Licensing	*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*
VRF configuration	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
• CISCO-COMMON-MGMT-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml