Configuring User Accounts and RBAC

This chapter contains the following sections:

Information About User Accounts and RBAC

Cisco Nexus Series switches use role-based access control (RBAC) to define the amount of access that each user has when the user logs into the switch.

With RBAC, you define one or more user roles and then specify which management operations each user role is allowed to perform. When you create a user account for the switch, you associate that account with a user role, which then determines what the individual user is allowed to do on the switch.

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, users who belong to both role1 and role2 can access configuration and debug operations. You can also limit access to specific VSANs, VLANs, and interfaces.

The switch provides the following default user roles:

network-admin (superuser)

Complete read and write access to the entire switch.

network-operator

Complete read access to the switch.

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.

Note Only network-admin user can perform a Checkpoint or Rollback in the RBAC roles. Though other users have these commands as a permit rule in their role, the user access is denied when you try to execute these commands.

Predefined SAN Admin User Role

The SAN admin user role is a noneditable, predefined user role that is designed to provide separation between LAN and SAN administrative tasks. Users that have been assigned the SAN admin user role have read-only access to all Ethernet configuration tasks. Write access for Ethernet features is not granted to SAN admin users unless it is assigned to them through another user role.

The following capabilities are permitted to SAN admin users:

- Interface configuration
- Attribute configuration for Fibre Channel Unified Ports, except creation and deletion
- VSAN configuration, including database and membership
- Mapping of preconfigured VLANs for FCoE to VSANs
- Zoning configuration
- Configuration of SNMP-related parameters, except SNMP community and SNMP users
- Read-only access to all other configurations
- Configuration and management of SAN features such as the following:
  - FC-SP
  - FC-PORT-SECURITY
  - FCoE
  - FCoE-NPV
  - FPORT-CHANNEL-TRUNK
  - PORT-TRACK
  - FABRIC-BINDING

- Configuration and management for the following of EXEC mode commands:
  - DEBUG
  - FCDOMAIN
  - FCPING
  - SAN-PORT-CHANNEL
  - SHOW
  - ZONE
  - ZONESET

Note The SAN Admin role permits configuration on all interface types, not just Fibre Channel interfaces. The predefined SAN Admin user role was designed to allow access to all interfaces—including Ethernet interfaces—so it would not interfere with SNMP operations.

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 Cisco Nexus device. Enter the **show role feature** command to display the feature names available for this parameter.

Feature group

Default or user-defined group of features. Enter the **show role feature-group** command to display the default feature groups available for this parameter.

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.

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.

SAN Admin Role-Feature Rule Mapping

The SAN admin role is not editable. The following role-features are part of preconfigured role. The preconfigured role comes complete read access and the following rules:

Table 1: Role-Feature Rules for SAN Admin User Role

Feature	Permissions
copy	Read and write permissions for copy-related commands
fabric-binding	Read and write permissions for fabric binding-related commands
fcdomain	Read and write permissions for Fibre Channel domain-related commands
fcfe	Read and write permissions for Fibre Channel FE-related commands
fcmgmt	Read and write permissions for Fibre Channel management-related commands
fcns	Read and write permissions for Fibre Channel-related service FCNS commands
fcoe	Read and write permissions for Fibre Channel over Ethernet-related commands
fcsp	Read and write permissions for Fibre Channel Security Protocol (FCSP)-related commands
fdmi	Read and write permissions for Fabric Device Management Interface (FDMI)-related commands
fspf	Read and write permissions for Fabric Shortest Path First (FSPF)-related commands
interface	Read and write permissions for interface-related commands, which includes all interfaces, not just Fibre Channel interfaces.
port-track	Read and write permissions for port track-related commands
port-security	Read and write permissions for port security-related commands
rdl	Read and write permissions for Remote Domain Loopback (RDL)-related commands
rmon	Read and write permissions for RMON-related commands

Feature	Permissions
rscn	Read and write permissions for Registered State Change Notification (RSCN)-related commands
snmp	Read and write permissions for SNMP-related commands
snmpTargetAddrEntry	Read and write permissions for SNMP trap target-related commands
snmpTargetParamsEntry	Read and write permissions for SNMP trap target parameter-related commands
span	Read and write permissions for SPAN-related commands
trapRegEntry	Read and write permissions for SNMP trap registry-related commands
trunk	Read and write permissions for Fibre Channel port channel trunk-related commands
vsan	Read and write permissions for VSAN-related commands
vsanIfvsan	Read and write permissions for FCoE VLAN-VSAN mapping command-related commands
wwnm	Read and write permissions for World Wide Name (WWN)-related commands
zone	Read and write permissions for zoning commands

User Role Policies

You can define user role policies to limit the switch resources that the user can access, or to limit access to interfaces, VLANs, and VSANs.

User role policies are constrained by the rules defined for the role. For example, if you define an interface policy to permit access to specific interfaces, the user does not have access to the interfaces unless you configure a command rule for the role to permit the **interface** command.

If a command rule permits access to specific resources (interfaces, VLANs, or VSANs), the user is permitted to access these resources, even if the user is not listed in the user role policies associated with that user.

User Account Configuration Restrictions

The following words are reserved and cannot be used to configure users:

- adm
- bin
- daemon
- ftp
- ftpuser
- games
- gdm
- gopher
- halt
- lp
- mail
- mailnull
- man
- mtsuser
- news
- nobody
- san-admin
- shutdown
- sync
- sys
- uucp
- xfs

Caution The Cisco Nexus 5000 Series switch does not support all numeric usernames, even if those usernames were created in TACACS+ or RADIUS. If an all numeric username exists on an AAA server and is entered during login, the switch rejects the login request.

Usernames must begin with an alphanumeric character and can contain only these special characters: (+ = . _ \ -). The # and ! symbols are not supported. If the username contains characters that are not allowed, the specified user is unable to log in. **This caution is applicable only for the Cisco Nexus 5000 and 5500 Series Switches for all 6.x and earlier releases.**

User Password Requirements

Cisco Nexus device passwords are case sensitive and can contain alphanumeric characters only. Special characters, such as the dollar sign ($) or the percent sign (%), are not allowed.

If a password is trivial (such as a short, easy-to-decipher password), the Cisco Nexus device rejects the password. Be sure to configure a strong password for each user account. 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
- 2009AsdfLkj30
- Cb1955S21

Note For security reasons, user passwords do not display in the configuration files.

Guidelines and Limitations for User Accounts

User accounts have the following guidelines and limitations when configuring user accounts and RBAC:

- Up to 256 rules can be added to a user role.
- A maximum of 64 user roles can be assigned to a user account.
- You can assign a user role to more that one user account.
- Predefined roles such as network-admin, network-operator, and san-admin are not editable.
- Add, delete, and editing of rules is not supported for the SAN admin user role.
- The interface, VLAN, and/or VSAN scope cannot be changed for the SAN admin user role.

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

Configuring User Accounts

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **show role**	(Optional) Displays the user roles available. You can configure other user roles, if necessary.
Step 3	switch(config) # **username** *user-id* [**password** *password*] [**expire** *date*] [**role** *role-name*]	Configures a user account. The *user-id* is a case-sensitive, alphanumeric character string with a maximum of 28 characters. The default *password* is undefined. **Note** If you do not specify a password, the user might not be able to log into the switch. The **expire** *date* option format is YYYY-MM-DD. The default is no expiry date.
Step 4	switch(config) # **exit**	Exists global configuration mode.
Step 5	switch# **show user-account**	(Optional) Displays the role configuration.
Step 6	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure a user account:

```
switch# configure terminal
switch(config)# username NewUser password 4Ty18Rnt
switch(config)# exit
switch# show user-account
```

Configuring SAN Admin Users

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **username** *user-id* **role san-admin password** *password*	Configures SAN admin user role access for the specified user.
Step 3	switch(config) # **show user-account**	(Optional) Displays the role configuration.
Step 4	switch(config) # **show snmp-user**	(Optional) Displays the SNMP user configuration.
Step 5	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to configure a SAN admin user and display the user account and SNMP user configuration:

```
switch# configure terminal
switch(config)# username user1 role san-admin password xyz123
switch(config)# show user-account
user:admin
     this user account has no expiry date
     roles:network-admin
user:user1
     this user account has no expiry date
     roles:san-admin
switch(config) # show snmp user
_____________________________________________________________________________
     SNMP USERS
_____________________________________________________________________________

User     Auth  Priv(enforce)  Groups
____     ____  _____________  ______
admin    md5   des(no)        network-admin
user1    md5   des(no)        san-admin

_____________________________________________________________________________
NOTIFICATION TARGET USES (configured for sending V3 Inform)
_____________________________________________________________________________

User     Auth   Priv
____     ____   ____

switch(config) #
```

Configuring RBAC

Creating User Roles and Rules

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.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **role name** *role-name*	Specifies a user role and enters role configuration mode. The *role-name* argument is a case-sensitive, alphanumeric character string with a maximum of 16 characters.
Step 3	switch(config-role) # **rule** *number* {**deny** | **permit**} **command** *command-string*	Configures a command rule. The *command-string* can contain spaces and regular expressions. For example, interface ethernet * includes all Ethernet interfaces. Repeat this command for as many rules as needed.
Step 4	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**}	Configures a read-only or read-and-write rule for all operations.
Step 5	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name*	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.
Step 6	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name*	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 7	switch(config-role)# **description** *text*	(Optional) Configures the role description. You can include spaces in the description.
Step 8	switch(config-role)# **end**	Exits role configuration mode.

	Command or Action	Purpose
Step 9	switch# **show role**	(Optional) Displays the user role configuration.
Step 10	switch# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to create user roles and specify rules:

```
switch# configure terminal
switch(config)# role name UserA
switch(config-role)# rule deny command clear users
switch(config-role)# rule deny read-write
switch(config-role)# description This role does not allow users to use clear commands
switch(config-role)# end
switch(config)# show role
```

Creating Feature Groups

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **role feature-group** *group-name*	Specifies a user role feature group and enters role feature group configuration mode. The *group-name* is a case-sensitive, alphanumeric character string with a maximum of 32 characters.
Step 3	switch(config) # **exit**	Exits global configuration mode.
Step 4	switch# **show role feature-group**	(Optional) Displays the role feature group configuration.
Step 5	switch# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to create a feature group:

```
switch# configure terminal
switch(config) # role feature-group group1
switch(config) # exit
switch# show role feature-group
switch# copy running-config startup-config
switch#
```

Changing User Role Interface Policies

You can change a user role interface policy to limit the interfaces that the user can access. Specify a list of interfaces that the role can access. You can specify it for as many interfaces as needed.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **role name** *role-name*	Specifies a user role and enters role configuration mode.
Step 3	switch(config-role) # **interface policy deny**	Enters role interface policy configuration mode.
Step 4	switch(config-role-interface) # **permit interface** *interface-list*	Specifies a list of interfaces that the role can access. Repeat this command for as many interfaces as needed. For this command, you can specify Ethernet or virtual Fibre Channel interfaces.
Step 5	switch(config-role-interface) # **exit**	Exits role interface policy configuration mode.
Step 6	switch(config-role) # **show role**	(Optional) Displays the role configuration.
Step 7	switch(config-role) # **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to change a user role interface policy to limit the interfaces that the user can access:

```
switch# configure terminal
switch(config)# role name UserB
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 2/1
switch(config-role-interface)# permit interface vfc 30/1
```

Changing User Role VLAN Policies

You can change a user role VLAN policy to limit the VLANs that the user can access.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **role name** *role-name*	Specifies a user role and enters role configuration mode.
Step 3	switch(config-role)# **vlan policy deny**	Enters role VLAN policy configuration mode.
Step 4	switch(config-role-vlan # **permit vlan** *vlan-list*	Specifies a range of VLANs that the role can access. Repeat this command for as many VLANs as needed.
Step 5	switch(config-role-vlan) # **exit**	Exits role VLAN policy configuration mode.
Step 6	switch# **show role**	(Optional) Displays the role configuration.
Step 7	switch# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Changing User Role VSAN Policies

You can change a user role VSAN policy to limit the VSANs that the user can access.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config-role) # **role name** *role-name*	Specifies a user role and enters role configuration mode.
Step 3	switch(config-role) # **vsan policy deny**	Enters role VSAN policy configuration mode.
Step 4	switch(config-role-vsan) # **permit vsan** *vsan-list*	Specifies a range of VSANs that the role can access. Repeat this command for as many VSANs as needed.
Step 5	switch(config-role-vsan) # **exit**	Exits role VSAN policy configuration mode.
Step 6	switch# **show role**	(Optional) Displays the role configuration.

	Command or Action	Purpose
Step 7	switch# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Verifying the User Accounts and RBAC Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show role [*role-name*]	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.

Configuring User Accounts Default Settings for the User Accounts and RBAC

The following table lists the default settings for user accounts and RBAC parameters.

Table 2: Default User Accounts and RBAC Parameters

Parameters	Default
User account password	Undefined.
User account expiry date	None.
Interface policy	All interfaces are accessible.

Parameters	Default
VLAN policy	All VLANs are accessible.
VFC policy	All VFCs are accessible.
VETH policy	All VETHs are accessible.