Nexus N5500, 5600 and N6000 Role Base Access Control (RBAC)

Contents

Introduction

This document describes how to limit a user to access Nexus 5500, Nexus 5600 and Nexus 6000 switches using Role Base Access Control (RBAC).

RBAC allows you to define the rules for an assigned user role to restrict the authorization of a user that has access to the switch management operations.

You can create and manage a user account and assign roles that limit access to Nexus 5500, Nexus 5600 and Nexus 6000 switches.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Nexus 5500, Nexus 5600, Nexus 6000 switches CLI configuration commands
- Cisco Fabric Services (CFS).

Components Used

The information in this document is based on Nexus 5500, Nexus 5600 and Nexus 6000 switches running NXOS 5.2(1)N1(9) 7.3(1)N1(1).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

User Requirements

These are some user requirements which are need to be fulfilled:

- Only users with network-admin role can create roles.
- Only users with network-admin role can view the output of **show role**.
- Even if users are permitted to perform all show commands, they are not allowed to view **show role** output, unless these users are assigned a network-admin role.
- A user account must have at least one user role.

User Roles

Each role can be assigned to multiple users and each user can be part of multiple roles.

For example, role A users are allowed to issue show commands and role B users are allowed to make configuration changes.

If a user is assigned to both role A and Role B, this user can issue show command and make changes to configuration.

Permit access command takes priority over deny access command.

For example, if you belong to a role which denies access to configuration commands.

However, if you also belong to a role that has access to configuration commands, you then have the access to configuration commands.

There are five default user roles:

- network-admin - Complete read-and-write access to the entire switch.
- network-operator - Complete read access to the entire switch.
- vdc-admin - Read-and-write access limited to a VDC
- vdc-operator - Read access limited to a VDC
- san-admin - Complete read-and-write access to SAN administrators.

> **Note**:You cannot modify/delete default user roles.

> **Note**: **show role** command will display the role available on the switch

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 these 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 rules.

The user-specified rule number determines the order in which rules are applied.

The rules are applied in descending order.

For example, rule 1 is applied before rule 2, which is applied before rule 3, and so on.

The rule command specifies operations that can be performed by a specific role. Each rule consists of a rule number, a rule type (permit or deny),

a command type (for example, configuration, show, exec, debug), and an optional feature name (for example, FCOE, HSRP, VTP, interface).

User Role Distribution

Role-based configurations use the Cisco Fabric Services (CFS) infrastructure to enable efficient database management and to provide a single point of configuration in the network.

When you enable CFS distribution for a feature on your device, the device belongs to a CFS region containing other devices in the network that you have also enabled for CFS distribution for the feature. CFS distribution for the user role feature is disabled by default.

You must enable CFS for user roles on each device to which you want to distribute configuration changes.

After you enable CFS distribution for user roles on the switch, the first user role configuration command that you enter causes the switch NX-OS software to take these actions:

1. Creates a CFS session on the switch.
2. Locks the user role configuration on all switches in the CFS region with CFS enabled for the user role feature.
3. Saves the user role configuration changes in a temporary buffer on the switch.

The changes stay in the temporary buffer on the switch until you explicitly commit them to be distributed to the devices in the CFS region.

When you commit the changes, the NX-OS software takes these actions:

1. Applies the changes to the running configuration on the switch.
2. Distributes the updated user role configuration to the other switches in the CFS region.
3. Unlocks the user role configuration in the devices in the CFS region.
4. Terminates the CFS session.

These configurations are distributed:

- Role names and descriptions
- List of rules for the roles

Configuration and Show Commands

	Command	**Purpose**
Step 1.	**configure terminal** Example: switch# **configure terminal** 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-*id* Example: switch(config-role-vlan)# **permit vlan 1**	Specifies the vlan 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.	**show role** {**pending | pending-diff**} Example: switch(config-role)# **show role pending**	(Optional) Displays the user role configuration pending for distribution
Step 8.	**role commit** Example: switch(config-role)# **role commit**	(Optional) Applies the user role configuration changes in the temporary database to the running configuration and distributes user role configuration to other swithces if you have enabled CFS configuration distribution for the user role feature.

Step 9.	**copy running-config startup-config** Example: switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

These steps enable the role configuration distribution:

	Command	Purpose
Step 1.	switch# **config t** switch(config)#	Enters configuration mode.
Step 2.	switch(config)# **role distribute** switch(config)#**no role distribute**	Enables role configuration distribution. Disables role configuration distribution (default).

These steps commit role configuration changes:

	Command	Purpose
Step 1	Nexus# **config t** Nexus(config)#	Enters configuration mode.
Step 2	Nexus(config)# **role commit**	Commits the role configuration changes.

These steps discard role configuration changes:

	Command	Purpose
Step 1	Nexus# **config t** Nexus(config)#	Enters configuration mode.
Step 2	Nexus(config)# **role abort**	Discards the role configuration changes and clears the pending configurat database.

To display user account and RBAC configuration information, perform one of these 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.

Clear the User Role Distribution Session

You can clear the ongoing Cisco Fabric Services distribution session (if any) and unlock the fabric for the user role feature.

Caution: Any changes in the pending database will be lost when you issue this command.

	Command	Purpose
Step 1	switch# **clear role session** **Example:** switch# clear role session	Clears the session and unlocks the fabric.
Step 2	**show role session status** **Example:** switch# show role session status	(Optional) Displays the user role CFS session status.

Configuration Example

In this example, we are going to create a user account TAC with these access permission:

- Access to clear command
- Access to configuration command
- Access to debug command
- Access to exec command
- Access to show command
- Access to vlan 1-10 only

```
C5548P-1# config t
Enter configuration commands, one per line.  End with CNTL/Z
C5548P-1(config)# role name Cisco
C5548P-1(config-role)# rule 1 permit command clear
C5548P-1(config-role)# rule 2 permit command config
C5548P-1(config-role)# rule 3 permit command debug
C5548P-1(config-role)# rule 4 permit command exec
C5548P-1(config-role)# rule 5 permit command show
C5548P-1(config-role)# vlan policy deny
C5548P-1(config-role-vlan)# permit vlan 1-10
C5548P-1(config-role-vlan)# end C5548P-1# show role name Cisco

Role: Cisco
  Description: new role
  vsan policy: permit (default)
  Vlan policy: deny
  Permitted vlans: 1-10
  Interface policy: permit (default)
  Vrf policy: permit (default)
  -------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  -------------------------------------------------------------------
  5       permit  command                         show
  4       permit  command                         exec
  3       permit  command                         debug
  2       permit  command                         config
  1       permit  command                         clear


C5548P-1#
C5548P-1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
C5548P-1(config)# username TAC password Cisco123 role Cisco

C5548P-1(config)# show user-account TAC
user:TAC
        this user account has no expiry date
        roles:Cisco
```

Licensing Requirements

Product	License Requirement
NX-OS	User accounts and RBAC require no license.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.