Contents

1 Configuring RBAC

1.1 Introduction

1.1.1 Overview

Role-based access control (RBAC) associates roles with permissions. Users are assigned with appropriate roles with -permissions. The authorization structure of user-role-permission is formed to simplify permission management. Roles are defined to complete various tasks, and a device administrator can predefine all the roles and their permissions. To change a user's permission, use RBAC to change only the permission of his role. This process reduces the authorization workload and device management overhead.

1.1.2 Basic Concepts

- Feature

  Features vary with CLI commands. CLI commands with the same features constitute one feature.

- Feature group

  A feature group is composed of features. Different features are classified as needed to form one feature group. In short, a feature group is composed of several types of CLI commands.

- User

  By default, a user does not have any permissions to operate a device. Only after you specify a proper role to a user, the user has the permission of this role. There are local users and remote AAA server users. Local users are used for local authentication while remote AAA server users are used for remote AAA authentication.

- Role

  There are predefined system roles and user-defined roles. The system predefines 18 roles, including **network-admin**, **network-operator**, and **priv-*n*** (0–15). Each role is granted with specific operation permissions. Table 1-1 lists these roles and their permissions.

Table 1-1Roles and Permissions

Role	Default Permission
network-admin	Administrator role, with all operation permissions.
network-operator	Operator role, with the following permissions: ● Permission control: ○ CLI commands: allowed to run the **ping**, **show**, **ssh**, **telnet**, **traceroute**, **ssh-session**, and **terminal** commands and the command to change the current local user password. The **show** command displays all information. ● Resource control: ○ Interfaces: allowed to operate all interfaces. ○ Virtual local area networks (VLANs): allowed to operate all VLANs.

	○ VPN routing and forwarding (VRF): allowed to operate all VRF instances.
priv-0	Level-0 role, assigned with the following permissions: ● Permission control: ○ CLI commands: allowed to run the **ping**, **ssh**, **telnet**, **traceroute**, **ssh-session**, and **enable** commands. ● Resource control: ○ Interfaces: allowed to operate all interfaces. ○ VLANs: allowed to operate all VLANs. ○ VRF: allowed to operate all VRF instances.
priv-n (1-13)	Level-1 to level-13 roles, without any permission
priv-14	Level-14 role, with the following permissions: ● Permission control: ○ CLI commands: allowed to run CLI commands other than the **more**, **upgrade**, and **debug** commands that are executable only by an administrator. ● Resource control: ○ Interfaces: allowed to operate all interfaces. ○ VLANs: allowed to operate all VLANs. ○ VRF: allowed to operate all VRF instances.
priv-15	Level-15 role, with the same all operation permissions as the role **network-admin**.

- Permission

  Permissions fall into three modes - read, write, and execute - or into two types - rule permissions and resource permissions. Rule permissions include those of command-based rules, those of feature-based rules, and those of feature group-based rules. Resource permissions include those of interface resources, those of VLAN resources, and those of VRF resources.

  Rule permissions configured for user roles are divided into the following categories:

  - Prohibit a role from running or allow a role to execute a specific command line.
  - Prohibit a role from running or allows a role to run one or several types of commands for specified or all features.
  - Prohibit a role from running or allows a role to run one or several types of commands for all features in a feature group.

  Resources permissions configured for user roles are divided into the following categories:

  - Prohibit a role from operating or allow a role to operate all or some interfaces.
  - Prohibit a role from operating or allow a role to operate all or some VLANs.
  - Prohibit a role from operating or allow a role to operate all or some VRF instances.

1.2 Configuration Task Summary

RBAC configuration includes the following tasks:

(1) (Optional) Configuring a Feature Group

(2) Configuring Role Permissions

a Enabling the RBAC Function

b Configuring Roles

c Configuring Rule Permissions for a Role

d (Optional) Configuring Description of a Role

e (Optional) Prohibiting a Role from Operating All Interface Resources

f (Optional) Allowing a Role to Operate a Specific Interface Resource

g (Optional) Prohibiting a Role from Operating All VLAN Resources

h (Optional) Allowing a Role to Operate a Specific VLAN Resource

i (Optional) Prohibiting a Role from Operating All VRF Resources

j (Optional) Allowing a Role to Operate a Specific VRF Resource

1.3 Configuring a Feature Group

1.3.1 Overview

This section describes how to create a feature group and add features to the feature group.

1.3.2 Restrictions and Guidelines

- Feature groups predefined in the system cannot be deleted or modified.
- Up to 64 feature groups can be customized.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a feature group and enter the feature group configuration mode.

role feature-group name *group-name*

The system predefines feature groups **L2** and **L3** by default. Feature group **L2** contains all commands for functions related to L2 protocols. Feature group **L3** contains all commands for functions related to L3 protocols.

(4) Add features to the feature group.

feature *feature-name*

By default, a system predefined feature group contains default features while a user-defined feature group contains no feature.

1.4 Configuring Role Permissions

1.4.1 Overview

This section describes how to create a user role and configure its operation permissions. After a user is authenticated to get a proper role, he has operation permissions.

1.4.2 Configuration Tasks

User role permission configuration includes the following tasks:

(1) Enabling the RBAC Function

(2) Configuring Roles

(3) Configuring Rule Permissions for a Role

(4) (Optional) Configuring Description of a Role

(5) (Optional) Prohibiting a Role from Operating All Interface Resources

(6) (Optional) Allowing a Role to Operate a Specific Interface Resource

(7) (Optional) Prohibiting a Role from Operating All VLAN Resources

(8) (Optional) Allowing a Role to Operate a Specific VLAN Resource

(9) (Optional) Prohibiting a Role from Operating All VRF Resources

(10) (Optional) Allowing a Role to Operate a Specific VRF Resource

1.4.3 Enabling the RBAC Function

1. Overview

This section describes how to enable the RBAC function.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the RBAC function.

role enable

The RBAC function is disabled by default.

1.4.4 Configuring Roles

1. Overview

This section describes how to customize a role.

2. Restrictions and Guidelines

- System predefined roles cannot be deleted by running the **no** command. The default permission of only the **priv-***n* (0–13) role can be restored by running the **default** command.

- Permissions can be added to the **priv-***n* (0–13) role only.
- Users can customize up to 64 roles and configure permissions for the roles. .

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a role and enter the role configuration mode.

role name *role-name*

By default, the system predefines 18 roles, including **network-admin**, **network-operator**, and **priv-***n* (0–15). Each role is granted with specific operation permissions.

1.4.5 Configuring Rule Permissions for a Role

1. Overview

This section describes how to configure the rule permissions for a role.

2. Restrictions and Guidelines

- By default, system predefined roles have predefined rule permissions while user-defined roles have no rule permission.
- During rule configuration, if the specified rule number does not exist, create a rule; otherwise, modify the rule corresponding to the specified rule number. The modified rule supports newly authenticated users only.
- A user role is allowed to create multiple rules, and permissions executable by this role is a union set of these rules. If permissions defined by these rules conflict with each other, rules with larger serial numbers prevail. For example, if command A is prohibited by rule 1, and command B is prohibited by rule 2, but command A is allowed by rule 3, rule 2 and rule 3 finally take effect. Specifically, command A is allowed and command B is prohibited.
- Predefined rules for predefined roles in the system cannot be deleted or modified. If there is a conflict between system predefined rules and user-defined rules, user-defined rules prevail.
- Up to 256 rules can be configured for each role. A maximum of 1024 rules can be configured for all roles on the device.
- To configure command-based rules, follow the rules below:
  - Division of segments. To describe a multi-level mode command, divide the command character string into multiple segments by a semicolon (;). Each segment represents one or a series of commands. The command in the latter segment is used to execute the mode of a command in the preceding segment. A segment must contain at least one printable character.
  - Use of semicolons. To describe a multi-level mode command, separate the command segments with a semicolon. For example, the character string **config ; logging on** is used to grant a permission over the **logging on** command in configuration mode. The semicolon in the last command segment indicates that the permission is granted over the current mode command. For example, the character string **config ; interface *** is used to grant a permission over only the command to enter the interface configuration mode.

The absence of a semicolon in the last command segment indicates that permissions are granted over the current command mode and all commands in this mode. For example, the character string **config ; interface *** is used to grant permissions over all commands in interface mode.

- Use of asterisks. Each command segment contains at least one asterisk (*). An asterisk resides either in the middle or at both ends of a command segment. Each asterisk serves to fuzzily match a command. For example, the character string **config ; *** is used to grant permissions over all the commands in configuration mode. The character string **config ; logging * flush** is used to grant a permission over a command starting with **logging** and ending with **flush** in configuration mode. The character string **config ; logging *** is used to grant permissions over all commands starting with **logging on** in configuration mode. When an asterisk resides in the middle of a command segment and the asterisk is used to match the command, the command is matched up to only the first asterisk in the middle, and the subsequent command segments are all considered matched. An execution command must be fully matched.
- Matching of keyword prefixes. A prefix matching algorithm is used for the matching between the command keyword and the command character string. That is, if the first several consecutive characters or all characters of a keyword in the command line match the keyword defined in a rule, the command line matches this rule. Therefore, a command character string may include a partial or complete command keyword. For example, if the rule **rule 1 deny command show ssh** is effective, the **show ssh** command and the **show ssh-session** command are disabled.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the role configuration mode.

role name *role-name*

(4) Configure rule permissions for a role.

rule *rule-number* { **permit** | **deny** } { **command** *command-string* | { **read** | **write** | **execute** }* { **feature** [*feature-name*] | **feature-group** *feature-group-name* } }

By default, predefined roles have predefined rule permissions while user-defined roles have no rule permission.

1.4.6 Configuring Description of a Role

1. Overview

This section describes how to configure the description for a role.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the role configuration mode.

role name *role-name*

(4) Configure the description for a role.

description *description*

By default, a predefined role is provided with a default description with the user-defined role is provided with no description.

1.4.7 Prohibiting a Role from Operating All Interface Resources

1. Overview

This section describes how to prohibit a role from -creating, deleting or applying all interface resources.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the role configuration mode.

role name *role-name*

(4) Prohibit a role from operating all interface resources and enter the role interface configuration mode.

interface policy deny

By default, a role has the permission to operate all interface resources.

1.4.8 Allowing a Role to Operate a Specific Interface Resource

1. Overview

This section describes how to allow a role to create, delete or apply a specific interface resource.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the role configuration mode.

role name *role-name*

(4) Prohibit a role from operating all interface resources and enter the role interface configuration mode.

interface policy deny

(5) Enable the role to operate a specific interface resource.

permit interface *interface-type interface-number-list*

By default, a role is prohibited from operating all interface resources.

1.4.9 Prohibiting a Role from Operating All VLAN Resources

1. Overview

This section describes how to prohibit a role from creating, deleting or applying all VLAN resources.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the role configuration mode.

role name *role-name*

(4) Prohibit a role from operating all VLAN resources and enter the role VLAN configuration mode.

vlan policy deny

By default, a role has the permission to operate all VLAN resources.

1.4.10 Allowing a Role to Operate a Specific VLAN Resource

1. Overview

This section describes how to allow a role to create, delete, and apply a specific VLAN resource.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the role configuration mode.

role name *role-name*

(4) Prohibit a role from operating all VLAN resources and enter the role VLAN configuration mode.

vlan policy deny

(5) Allow a role to operate a specific VLAN resource.

permit vlan *vlan-list*

By default, a role is prohibited from operating all VLAN resources.

1.4.11 Prohibiting a Role from Operating All VRF Resources

1. Overview

This section describes how to prohibit a role from creating, deleting or applying all VRF resources.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the role configuration mode.

role name *role-name*

(4) Prohibit a role from operating all VRF resources and enter the role VRF configuration mode.

vrf policy deny

By default, a role has the permission to operate all VRF resources.

1.4.12 Allowing a Role to Operate a Specific VRF Resource

1. Overview

This section describes how to allow a role to create, delete or apply a specific VRF resource.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the role configuration mode.

role name *role-name*

(4) Prohibit a role from operating all VRF resources and enter the role VRF configuration mode.

vrf policy deny

(5) Enable a role to operate a specific VRF resource.

permit vrf *vrf-name*

By default, a role is prohibited from operating all VRF resources.

1.5 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** command to clear information.

Caution

Running the **clear** commands may lose vital information and thus interrupt services.

Run the **debug** command to output various debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1RBAC Monitoring

Command	Purpose
show role [**name** *role-name*]	Displays the information about a specific role or all roles.
show role feature [**detail** | **name** *feature-name*]	Displays the basic information or details about a specific feature or all features.
show role feature-group [**detail** | **name** *group-name* [**detail**]]	Displays the basic information or details about a specific feature group or all feature groups.
debug rbac	Debugs the RBAC module.

1.6 Configuration Examples

1.6.1 Configuring Role Permissions

1. Requirements

(1) Create the role **test**, set the description to "test role", and configure permissions to:

- Check all device information.
- Execute all commands of features snmpd and syslogd.
- Execute commands to create and delete interfaces, VLANs and VRF instances.
- Prohibit the role from operating all interface resources, but allow the role to operate interface VLAN 1.
- Prohibit the role from operating all VLAN resources, but allow the role to operate VLAN 1.
- Prohibit the role from operating all VRF resources, but allow the role to operate the VRF instance **test**.

(2) Create a user with username **user**, password **user123**, and role **test**.

(3) Configure username and password-based authentication for telnet login.

(4) Let a user log in to a device from a PC in telnet mode, and perform authentication with username **user** and password **user123**. Upon login, the user is assigned with role **test** and has permissions of role **test**.

2. Topology

Figure 1-1Configuring Role Permissions

3. Notes

- Enable the RBAC function.
- Create a role and configure its description.
- Configure role permissions to:

- Operate all **show** commands.
- Operate all read, write, and execution commands of features snmpd and syslogd.
- Execute interface, VLAN and VRF commands, as well as all commands in corresponding modes.
- Prohibit the role from operating all interface resources, but allow it to operate interface vlan 1.
- Prohibit the role from operating all VLAN resources, but allow it to operate VLAN 1.
- Prohibit the role from operating all VRF resources, but allow it to operate VRF instance **test**.
- Create a user with username **user** and password **user123**, and assign the user with the role **test**.
- Configure username and password-based authentication for Telnet login.

4. Procedure

(1) Enable the RBAC function.

Enable the RBAC function for device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# role enable
```

(2) Create a role and configure its description.

Create the role **test** for device A and set the description for the role.

```
DeviceA(config)# role name test
DeviceA(config-role)# description test role
```

(3) Configure the role permissions.

Allow the role to run all **show** commands.

```
DeviceA(config-role)# rule 1 permit command show *
```

Allow the role to operate all read, write, and execute commands of features snmpd and syslogd.

```
DeviceA(config-role)# rule 2 permit read write execute feature snmpd
DeviceA(config-role)# rule 3 permit read write execute feature syslogd
```

Allow the role to execute interface, VLAN and VRF commands, as well as all commands in corresponding modes.

```
DeviceA(config-role)# rule 4 permit command config;interface *
DeviceA(config-role)# rule 5 permit command config;vlan *
DeviceA(config-role)# rule 6 permit command config;vrf definition *
```

Prohibit the role from operating all interface resources, but allow it to operate interface vlan 1.

```
DeviceA(config-role)# interface policy deny
DeviceA(config-role-interface)# permit interface vlan 1
DeviceA(config-role-interface)# exit
```

Prohibit the role from operating all VLAN resources, but allow it to operate VLAN 1.

```
DeviceA(config-role)# vlan policy deny
DeviceA(config-role-vlan)# permit vlan 1
DeviceA(config-role-vlan)# exit
```

Prohibit the role from operating all VRF resources, but allow it to operate the VRF instance **test**.

```
DeviceA(config-role)# vrf policy deny
DeviceA(config-role-vrf)# permit vrf test
DeviceA(config-role-vrf)# exit
DeviceA(config-role)# exit
```

Create a user with username **user** and password **user123**, and assign the user with the role **test**.

```
DeviceA(config)# username user password user123
DeviceA(config)# username user role test
```

Configure local username and password-based authentication for remote telnet login.

```
DeviceA(config)# line vty 0 4
DeviceA(config-line)# login local
```

5. Verification

View the role information.

```
DeviceA# show role name test
Role: test
  Description: test role
  Interface policy: deny
  Permit interfaces:
  VLAN1
  VLAN policy: deny
  Permit VLANs: 1
  Vrf policy: deny
  Permit vrfs: test
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  1       permit       command       show *
  2       permit RWX   feature       snmpd
  3       permit RWX   feature       syslogd
  4       permit       command       config;interface *
  5       permit       command       config;vlan *
  6       permit       command       config;vrf definition *
  R:Read W:Write X:Execute
```

Run any **show** command.

```
DeviceA# show privilege
Current privilege role is test
orion_B26Q# show users
Line              User         Host(s)              Idle       Location
---------------- ------------ -------------------- ---------- ------------------
*  1 vty 0        user         idle                 00:00:00   172.30.31.16
```

Run all read, write, and execution commands of features snmpd and syslogd.

```
DeviceA# show logging
Syslog logging: enabled
  Console logging: level debugging, 46 messages logged
```

```
  Monitor logging: level debugging, 19 messages logged
  Buffer logging: level debugging, 46 messages logged
  Standard format:false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: disable
  Sysname log messages: disable
  Count log messages: disable
  Trap logging: level informational, 46 message lines logged,0 fail
Log Buffer (Total 1048576 Bytes): have written 4462
*Oct 16 07:23:17: %CLI-6-STARTUP: Cli server process startup.
*Oct 16 07:23:17: %LOCALEAP-6-PKIMANAGE: Self-Signed PKI is activated
DeviceA# show snmp
Chassis: 60FF60
0 SNMP packets input
        0 Bad SNMP version errors
        0 Unknown community name
        0 Illegal operation for community name supplied
        0 Encoding errors
        0 Number of requested variables
        0 Number of altered variables
        0 Get-request PDUs
        0 Get-next PDUs
        0 Set-request PDUs
        0 Drop PDUs
        0 UDP parse errors
0 SNMP packets output
        0 Too big errors (Maximum packet size 1472)
        0 No such name errors
        0 Bad values errors
        0 General errors
        0 Response PDUs
        0 Trap PDUs
SNMP global trap: disabled
SNMP logging: disabled
SNMP agent: enabled
SNMP v1: enabled
```

Run the interface access command. Then, a prompt for no permission appears.

```
DeviceA(config)# snmp-server community test rw
DeviceA(config)# logging server 1.1.1.1
DeviceA(config)# interface vlan 1
DeviceA(config-if-VLAN 1)# description test
DeviceA(config-if-VLAN 1)# exit
DeviceA(config)# interface gigabitethernet 0/1
% User doesn't have sufficient privilege to execute this command.
DeviceA(config)# vlan 1
```

```
DeviceA(config-vlan)# name test
DeviceA(config-vlan)# exit
DeviceA(config)# vlan 2
% User doesn't have sufficient privilege to execute this command.
DeviceA(config)# vrf definition test
DeviceA(config-vrf)# description test
DeviceA(config-vrf)# exit
DeviceA(config)# vrf definition test1
% User doesn't have sufficient privilege to execute this command.
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
username user password user123
username user role test
!
role enable
!
role name test
 description test role
 rule 1 permit command show *
 rule 2 permit read write execute feature snmpd
 rule 3 permit read write execute feature syslogd
 rule 4 permit command config;interface *
 rule 5 permit command config;vlan *
 rule 6 permit command config;vrf definition *
 interface policy deny
  permit interface VLAN 1
 vlan policy deny
  permit vlan 1
 vrf policy deny
  permit vrf test
!
line vty 0 4
 login local
```