Role-Based Access Controls

• Configuring User Roles, on page 1

Configuring User Roles

Role-Based Access Control Overview

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and locales. A role defines the privileges of a user in the system and a locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, you can manage individual user privileges by assigning the appropriate roles and locales.

A user is granted write access to the required system resources only if the assigned role grants the access privileges and the assigned locale allows access. For example, a user with the Server Administrator role in the engineering organization can update server configurations in the Engineering organization. They cannot, however, update server configurations in the Finance organization, unless the locales assigned to the user include the Finance organization.

User Roles

User roles contain one or more privileges that define the operations that are allowed for a user. You can assign one or more roles to each user. Users with multiple roles have the combined privileges of all assigned roles. For example, if Role1 has storage-related privileges, and Role 2 has server-related privileges, users with Role1 and Role 2 have both storage-related and server-related privileges.

A Cisco UCS domain can contain up to 48 user roles, including the default user roles. Any user roles configured after the first 48 are accepted, but they are inactive with faults raised.

All roles include read access to all configuration settings in the Cisco UCS domain. Users with read-only roles cannot modify the system state.

You can create, modify or remove existing privileges, and delete roles. When you modify a role, the new privileges apply to all users with that role. Privilege assignment is not restricted to the privileges defined for the default roles. Meaning, you can use a custom set of privileges to create a unique role. For example, the default Server Administrator and Storage Administrator roles have a different set of privileges. However, you can create a Server and Storage Administrator role that combines the privileges of both roles.

Note If you delete a role after it was assigned to users, it is also deleted from those user accounts.

Modify the user profiles on AAA servers (RADIUS or TACACS+) to add the roles corresponding to the privileges granted to that user. The attribute stores the role information. The AAA servers return this attribute with the request and parse it to obtain the roles. LDAP servers return the roles in the user profile attributes.

Default User Roles

The system contains the following default user roles:

AAA Administrator

Read-and-write access to users, roles, and AAA configuration. Read access to the remaining system.

Administrator

Complete read-and-write access to the entire system. Assigns this role to the default administrator account by default. You cannot change it.

Facility Manager

Read-and-write access to power management operations through the power management privilege. Read access to the remaining system.

Network Administrator

Read-and-write access to fabric interconnect infrastructure and network security operations. Read access to the remaining system.

Operations

Read-and-write access to systems logs, including the syslog servers, and faults. Read access to the remaining system.

Read-Only

Read-only access to system configuration with no privileges to modify the system state.

Server Compute

Read and write access to most aspects of service profiles. However, the user cannot create, modify or delete vNICs or vHBAs.

Server Equipment Administrator

Read-and-write access to physical server-related operations. Read access to the remaining system.

Server Profile Administrator

Read-and-write access to logical server-related operations. Read access to the remaining system.

Server Security Administrator

Read-and-write access to server security-related operations. Read access to the remaining system.

Storage Administrator

Read-and-write access to storage operations. Read access to the remaining system.

Reserved Words: User Roles

You cannot use the following words when creating custom roles in Cisco UCS.

- network-admin
- network-operator
- vdc-admin
- vdc-operator
- server-admin

Privileges

Privileges give users, assigned to user roles, access to specific system resources and permission to perform specific tasks. The following table lists each privilege and the user role given that privilege by default.

Tip Detailed information about these privileges and the tasks that they enable users to perform is available in *Privileges in Cisco UCS* available at the following URL: http://www.cisco.com/en/US/products/ps10281/prod_technical_reference_list.html.

Table 1: System Defined Roles

Role	Privileges	Role to Configure in LDAP/RADIUS/TACACS Server
AAA Administrator	aaa	aaa
Administrator	admin	admin
KVM Administrator	kvm	kvm
Network	pod-qos, pod-config, pod-policy, ext-lan-qos, pod-security, [illegible]	network
Operations	fault, operations	fault, operations
Read-Only	read-only	read-only
Server-Compute Administrator	service-profile-compute, service-profile-server-oper, service-profile-server-policy	server-compute
Server-Equipment Administrator	server-policy, server-equipment, server-maintenance	server-equipment
Server Profile Administrator	[illegible]	server-profile
Server Security Administrator	server-security, service-profile-security, service-profile-security-policy	server-security
Statistics Administrator	stats	stats-management
Storage Administrator	[illegible]	storage

Table 2: User Privileges

Privilege	Description	Default Role Assignment
aaa	System security and AAA	AAA Administrator
admin	System administration	Administrator
ext-lan-config	External LAN configuration	Network Administrator
ext-lan-policy	External LAN policy	Network Administrator
ext-lan-qos	External LAN QoS	Network Administrator
ext-lan-security	External LAN security	Network Administrator
ext-san-config	External SAN configuration	Storage Administrator
ext-san-policy	External SAN policy	Storage Administrator
ext-san-qos	External SAN QoS	Storage Administrator
ext-san-security	External SAN security	Storage Administrator
fault	Alarms and alarm policies	Operations
kvm	Launch KVM	Operations
operations	Logs and Smart Call Home	Operations
org-management	Organization management	Operations
pod-config	Pod configuration	Network Administrator
pod-policy	Pod policy	Network Administrator
pod-qos	Pod QoS	Network Administrator
pod-security	Pod security	Network Administrator
power-mgmt	Read-and-write access to power management operations	Facility Manager
read-only	Read-only access Read-only cannot be selected as a privilege; it is assigned to every user role.	Read-Only
server-equipment	Server hardware management	Server Equipment Administrator
server-maintenance	Server maintenance	Server Equipment Administrator
server-policy	Server policy	Server Equipment Administrator
server-security	Server security	Server Security Administrator

Privilege	Description	Default Role Assignment
service-profile-compute	Service profile compute	Server Compute Administrator
service-profile-config	Service profile configuration	Server Profile Administrator
service-profile-config-policy	Service profile configuration policy	Server Profile Administrator
service-profile-ext-access	Service profile endpoint access	Server Profile Administrator
service-profile-network	Service profile network	Network Administrator
service-profile-network-policy	Service profile network policy	Network Administrator
service-profile-qos	Service profile QoS	Network Administrator
service-profile-qos-policy	Service profile QoS policy	Network Administrator
service-profile-security	Service profile security	Server Security Administrator
service-profile-security-policy	Service profile security policy	Server Security Administrator
service-profile-server	Service profile server management	Server Profile Administrator
service-profile-server-oper	Service profile consumer	Server Profile Administrator
service-profile-server-policy	Service profile pool policy	Server Security Administrator
service-profile-storage	Service profile storage	Storage Administrator
service-profile-storage-policy	Service profile storage policy	Storage Administrator

Creating a User Role

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **create role** *name*	Creates the user role and enters role security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/role* # **add privilege** *privilege-name*	Adds one or more privileges to the role.

	Command or Action	Purpose
		Note You can specify more than one *privilege-name* on the same command line to add multiple privileges to the role. You can also add privileges to the same role using multiple **add** commands.
Step 7	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Creates the service-profile-security-admin role
- Adds the service profile security to the role
- Adds the service profile security policy privileges to the role
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # create role ls-security-admin
UCSC(policy-mgr) /org/device-profile/security/role* # add privilege service-profile-security

service-profile-security-policy
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/role #
```

Deleting a User Role

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **delete role** *name*	Deletes the user role.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the service-profile-security-admin role
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # delete role service-profile-security-admin
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/role #
```

Adding Privileges to a User Role

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope role** *name*	Enters role security mode for the specified role.
Step 6	UCSC(policy-mgr) /org/device-profile/security/role # **add privilege** *privilege-name*	Adds one or more privileges to the existing privileges of the user role. **Note** You can specify more than one *privilege-name* on the same command line to add multiple privileges to the role. You can also add privileges to the same role using multiple **add privilege** commands.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Adds the server security to the service-profile-security-admin role
- Adds the server policy privileges to the service-profile-security-admin role
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope role
UCSC(policy-mgr) /org/device-profile/security/role # scope role service-profile-security-admin
UCSC(policy-mgr) /org/device-profile/security/role* # add privilege server-security
server-policy
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/role #
```

Replacing Privileges for a User Role

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope role** *name*	Enters role security mode for the specified role.
Step 6	UCSC(policy-mgr) /org/device-profile/security/role # **set privilege** *privilege-name*	Replaces the existing privileges of the user role.

	Command or Action	Purpose
		Note You can specify more than one *privilege-name* on the same command line to replace the existing privilege with multiple privileges. After replacing the privileges, you can add privileges to the same role using the **add privilege** command.
Step 7	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Replaces the existing privileges for the service-profile-security-admin role with server security
- Replaces the existing privileges for the service-profile-security-admin role with server policy privileges
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope role
UCSC(policy-mgr) /org/device-profile/security/role # scope role service-profile-security-admin
UCSC(policy-mgr) /org/device-profile/security/role* # set privilege server-security
server-policy
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/role #
```

Removing Privileges from a User Role

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope security**	Enters security mode.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope role** *name*	Enters role security mode for the specified role.
Step 6	UCSC(policy-mgr) /org/device-profile/security/role # **remove privilege** *privilege-name*	Removes one or more privileges from the existing user role privileges. **Note** You can specify more than one *privilege-name* on the same command line to remove multiple privileges from the role. You can also remove privileges from the same role using multiple **remove privilege** commands.
Step 7	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Removes the server security from the service-profile-security-admin role
- Removes the server policy privileges from the service-profile-security-admin role
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope role
UCSC(policy-mgr) /org/device-profile/security/role # remove privilege server-security
server-policy
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/role #
```

Assigning a Role to a User Account

Changes in user roles and privileges do not take effect until the next time the user logs in. If a user is logged in when you assign a new role to or remove an existing role from a user account, the active session continues with the previous roles and privileges.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the organization root.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope local-user** *local-user-name*	Enters local user security mode for the specified local user account.
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **create role** *role-name*	Assigns the specified role to the user account. **Note** You can enter the **create role** command multiple times to assign more than one role to a user account.
Step 7	UCSC(policy-mgr) /org/device-profile/security/local-user* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Assigns the operations role to the kikipopo local user account
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope local-user kikipopo
UCSC(policy-mgr) /org/device-profile/security/local-user # create role operations
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/local-user #
```

Removing a Role from a User Account

Changes in user roles and privileges do not take effect until the next time the user logs in. If a user is logged in when you assign a new role to or remove an existing role from a user account, the active session continues with the previous roles and privileges.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the organization root.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope local-user** *local-user-name*	Enters local user security mode for the specified local user account.
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **delete role** *role-name*	Removes the specified role from the user account. **Note** You can enter the **delete role** command multiple times to remove more than one role from a user account.
Step 7	UCSC(policy-mgr) /org/device-profile/security/local-user* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Removes the operations role from the kikipopo local user account
- Commits the transaction

```
CSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope local-user kikipopo
UCSC(policy-mgr) /org/device-profile/security/local-user # delete role operations
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/local-user #
```