Users and 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.

Cisco UCS Central User Accounts

Access the system with user accounts. You can configure up to 128 user accounts in each Cisco UCS Central domain. Each user account must have a unique username and password.

You can setup a user account with an SSH public key, in either of the two formats: OpenSSH or SECSH.

Admin Account

The Cisco UCS Central admin account is the default user account. You cannot modify or delete it. This account is the system administrator, or superuser account, and has full privileges. There is no default password assigned to the admin account. You must choose the password during the initial system setup.

The admin account is always active and does not expire. You cannot configure the admin account as inactive.

The local admin user can login for fail over, even when authentication is set to remote.

Locally Authenticated User Accounts

A locally authenticated user account is authenticated through the Cisco UCS Central user database. Anyone with admin or aaa privileges can enable or disable it. Once you disable a local user account, the user cannot log in.

Note Cisco UCS Central does not delete configuration details for disabled local user accounts from the database. If you re-enable a disabled local user account, the account becomes active again with the existing configuration, including username and password.

Remotely Authenticated User Accounts

A remotely authenticated user account is any Cisco UCS Central user account that is authenticated through LDAP. Cisco UCS domains support LDAP, RADIUS and TACACS+.

If a user maintains a local user account and a remote user account simultaneously, the roles defined in the local user account override those maintained in the remote user account.

Expiration of User Accounts

You can configure user accounts to expire at a predefined time. When the user account reaches the expiration time, the account disables.

By default, user accounts do not expire.

Note After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. You can, however, configure the account to expire with the farthest expiration date available.

Guidelines for Creating Usernames

The username is also used as the login ID for Cisco UCS Central. When you assign login IDs to Cisco UCS Central user accounts, consider the following guidelines and restrictions:

- The login ID can contain between 1 and 32 characters, including the following:
  - Any alphabetic character
  - Any digit
  - _ (underscore)
  - - (dash)
  - . (dot)
- The login ID must be unique within Cisco UCS Central.

- The login ID must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.
- The login ID is case-sensitive.
- You cannot create an all-numeric login ID.
- After you create a user account, you cannot change the login ID. You must delete the user account and create a new one.

Reserved Words: Locally Authenticated User Accounts

You cannot use the following words when creating a local user account in Cisco UCS.

- root
- bin
- daemon
- adm
- lp
- sync
- shutdown
- halt
- news
- uucp
- operator
- games
- gopher
- nobody
- nscd
- mailnull
- mail
- rpcuser
- rpc
- mtsuser
- ftpuser
- ftp
- man

- sys
- samdme
- debug

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. Each domain group in Cisco UCS Central can also contain 48 user roles, including the user roles that are inherited from the parent domain group. When user roles are pushed to Cisco UCS Manager from Cisco UCS Central, only the first 48 roles are active. Any user roles after the first 48 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
Facility Manager	facility-manager	power-mgmt
KVM Administrator	kvm	kvm
Network	pod-qos,pod-config,pod-policy,ext-lan-qos,pod-security,	network
Operations	fault, operations	fault, operations
Read-Only	read-only	read-only
Server-Compute Administrator		server-compute
Server-Equipment Administrator	server-policy,server-equipment,server-maintenance	server-equipment
Server Profile Administrator		server-profile
Server Security Administrator	server-security,service-profile-security,service-profile-security-policy	server-security
Statistics Administrator	stats	stats-management
Storage Administrator		storage

Table 2: User Privileges

Privilege	Description	Default Role Assignment
aaa	System security and AAA	AAA Administrator
admin	System administration	Administrator
domain-group-management	Domain Group Management	Domain Group 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

Privilege	Description	Default Role Assignment
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
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

Privilege	Description	Default Role Assignment
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
stats	Statistics Management	Statistics Administrator

Managing UCS Central Roles

Procedure

Step 1 In the Actions bar, type **Manage UCS Central Roles** and press **Enter**.

This launches the **UCS Central Roles Manage** dialog box.

Step 2 In **Roles**, click **Add** to create a new role, or select an existing role.

Step 3 In the **Network** tab, click **Add** to update and add privileges.

Step 4 Select relevant privileges for the role.

Step 5 Click **Apply** to apply the new privileges.

Step 6 Update the **Storage**, **Server**, and **Operations** privileges for the role, in the same manner.

Step 7 Click **Save**.

Managing UCS Central Local Users

Procedure

Step 1 In the Actions bar, type **Manage UCS Central Local Users** and press **Enter**.

This launches the **UCS Central Local Users Manage** dialog box.

Step 2 In **Local Users**, click **Add** to create a new local user, or select an existing one.

Step 3 In the **Basic** tab, complete the necessary information for the user.

Step 4 In the **Roles** tab, add or remove the roles assigned to the user.

a) Click **Add** to display the roles.
b) Select a role or roles.
c) Click **Apply** to apply the new privileges.

Step 5 In the **Locales** tab, add or remove the locales assigned to the user.

a) Click **Add** to display the roles.
b) Select a role or roles.
c) Click **Apply** to apply the new privileges.

Step 6 In the **SSH** tab, select the **Authentication Type**.

Step 7 Click **Save**.

Managing UCS Central Remote Users

Procedure

Step 1 In the Actions bar, type **Manage UCS Central Remote Users** and press **Enter**.

This launches the **UCS Central Remote Users Manage** dialog box.

Step 2 In **Remote Users**, review the remote LDAP users, roles, and locales.

Note This section is read-only.

Step 3 Click **Cancel** to close the window, or **Save** to save any changes made in other sections.

User Locales

You can assign a user to one or more locales. Each locale defines one or more organizations (domains) to which a user can access. Access is usually limited to the organizations specified in the locale. An exception is a locale without any organizations. It provides unrestricted access to system resources in all organizations.

A Cisco UCS domain can contain up to 48 user locales. Any user locales configured after the first 48 are accepted, but are inactive with faults raised. Each domain group in Cisco UCS Central can contain 48 user locales, including the user locales that are inherited from the parent domain group. When user locales are pushed to Cisco UCS Manager from Cisco UCS Central, only the first 48 locales are active. Any user locales after the first 48 are inactive with faults raised.

Users with admin or aaaadmin, aaa, or domain-group-management privileges can assign organizations to the locale of other users. The assignment of organizations is restricted to only those in the locale of the user assigning the organizations. For example, if a locale contains only the Engineering organization, a user assigned to that locale can only assign the Engineering organization to other users.

Note You cannot assign a locale to users with the admin privilege.

Note You cannot assign a locale to users with one or more of the following privileges:

- aaa
- admin
- fault
- operations

You can hierarchically manage organizations. A user who is assigned to a top-level organization has automatic access to all organizations below it. For example, an Engineering organization can contain a Software Engineering organization and a Hardware Engineering organization. A locale containing only the Software Engineering organization has access to system resources only within that organization. However, a locale that contains the Engineering organization has access to the resources for both the Software Engineering and Hardware Engineering organizations.

User Organizations

A user can create one or more organizations. Each organization defines sub-organizations, faults, events, UUID suffix pools and blocks of UUIDs.

Cisco UCS organizations are hierarchically managed by users. A user that is assigned at the root level organization has automatic access to all organizations and domain groups under it.

Managing UCS Central Locales

Procedure

Step 1 In the Actions bar, type **Manage UCS Central Locales** and press **Enter**.

This launches the **UCS Central Locales Manage** dialog box.

Step 2 In **Locales**, click **Add** to add a new locale, or select an existing one.

Step 3 Assign **Organizations** and **Domain Groups** to the locale.

a) Click **Add** to display the organizations or domain groups.
b) Select the organizations or domain groups.
c) Click **Apply** to apply the new privileges.

Step 4 Click **Save**.

Managing Domain Group Users

Procedure

Step 1 Click the **Domain Group** icon and choose **root**.

Step 2 Click the **Settings** icon and choose **Users**.

Step 3 In **Roles**, select roles to associate them with the domain group. Uncheck roles to disassociate them from the domain group.

Step 4 In the **Network** tab, click **Add** to update and add privileges.

a) Click **Add** to display the organizations.
b) Select relevant privileges for the role.
c) Click **Apply** to apply the new privileges.

Step 5 Update the **Storage**, **Server**, and **Operations** privileges for the role, in the same manner.

Step 6 In **Locales**, select locales to associate them with the domain group. Uncheck roles to disassociate them from the domain group.

Step 7 Assign **Organizations** to the locale.

a) Click **Add** to display the organizations.
b) Select the organizations or domain groups.
c) Click **Apply** to apply the new privileges.

Step 8 Click **Save**.