Configuring RBAC

This section contains the following topics:

RBAC

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 the locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and locales.

A user is granted write access to desired 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 could update server configurations in the Engineering organization but could not update server configurations in the Finance organization unless the locales assigned to the user include the Finance organization.

User Accounts

User accounts are used to access the system. Up to 128 local user accounts can be configured in each Prime Network Services Controller instance. Each user account must have a unique username.

A local user can be authenticated using a password or an SSH public key. The public key can be set in either of the two formats: OpenSSH and SECSH.

Default User Account

Each Prime Network Services Controller instance has a default user account, admin, which cannot be modified or deleted. 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.

Expiration of User Accounts

User accounts can be configured to expire at a predefined time. When the expiration time is reached, the user account is disabled.

By default, user accounts do not expire.

Username Guidelines

The username is also used as the login ID for Prime Network Services Controller. When you assign usernames to Prime Network Services Controller user accounts, consider the following guidelines and restrictions:

- The login ID can contain from 1 to 32 characters, including the following:
  - Any alphanumeric character
  - Period (.)
  - Underscore (_)
  - Dash (-)
  - At symbol (@)
- Neither the unique username nor a local user's username can consist solely of numbers.
- The unique username cannot start with a number.
- If an all-numeric username exists on a AAA server (LDAP) and is entered during login, Prime Network Services Controller cannot log in the user.

After you create a user account, you cannot change the username. You must delete the user account and create a new one.

Note You can create up to 128 user accounts in a Prime Network Services Controller instance.

Password Guidelines

For authentication purposes, a password is required for each user account. To prevent users from choosing insecure passwords, each password must be strong. If the Password Strength Check option is enabled, Prime Network Services Controller rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters.

- Must contain at least three of the following:
  - Lowercase letters
  - Uppercase letters
  - Digits
  - Special characters
- Must not contain a character that is repeated more than three times consecutively, such as aaabbb.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: dollar sign ($), question mark (?), or equals sign (=).
- Should not be blank for local user and admin accounts.

Note The Password Strength Check option is enabled by default. You can disable it from the Locally Authenticated Users pane (Administration > Access Control > Locally Authenticated Users).

Note If Prime Network Services Controller is configured to use remote authentication with LDAP, passwords for those remote accounts can be blank. With this configuration, the remote credentials store is used for authentication only, not authorization. The definition of the local user role definition applies to the remotely authenticated user.

User Roles

User roles contain one or more privileges that define the operations allowed for the user who is assigned the role. A user can be assigned one or more roles. A user assigned multiple roles has the combined privileges of all assigned roles. For example, if Role1 has policy-related privileges, and Role2 has tenant-related privileges, users who are assigned to both Role1 and Role2 have policy- and tenant-related privileges.

All roles include read access to all configuration settings in the Prime Network Services Controller instance. The difference between the read-only role and other roles is that a user who is assigned only the read-only role cannot modify the system state. A user assigned another role can modify the system state in that user's assigned area or areas.

The system contains the following default user roles:

aaa

Users have read and write access to users, roles, and AAA configuration, and read access to the rest of the system.

admin

Users have read and write access to the entire system and has most privileges. However, users cannot create or delete files, or perform system upgrades. These functions can be done only through the default admin account. The default admin account is assigned this role by default, and it cannot be changed.

intercloud-infra

Users have read and write access for InterCloud operations, including creating InterCloud links, creating provider accounts, managing InterCloud Extender and Switch images, and importing InterCloud Agent images. Users with this role are limited to InterCloud functionality.

intercloud-server

Users have read and write access for cloud VMs. User can create or move VMs from the enterprise to the cloud. Users can monitor cloud VMs for multiple tenants. Users with this role are limited to InterCloud functionality.

network

Users can create organizations, security policies, and device profiles.

operations

Users can acknowledge faults and perform some basic operations, such as logging configuration.

read-only

Users have read-only access to system configuration and operational status with no privileges to perform any operations.

tenant-admin

Users can configure tenant-related policies and resources for their associated tenants. However, users can view only those objects related to their associated tenants as defined by their assigned locales and organizations. They cannot see information about tenants that do not belong to their assigned locales and organizations.

Roles can be created, modified to add new or remove existing privileges, or deleted. When a role is modified, the new privileges are applied to all users assigned to that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you can use a custom set of privileges to create a unique role. For example, the default Network and Operations roles have different sets of privileges, but a new Network and Operations role can be created that combines the privileges of both roles.

If a role is deleted after it has been assigned to users, it is also deleted from those user accounts.

The role and locale assignment for a local user can be changed on Prime Network Services Controller. The role and locale assignment for a remote user can be changed on LDAP. If any of the following information assigned to a user is modified, the administrator must delete all the existing sessions of that user so that the new privileges take effect:

- Role
- Privilege for a role
- Locale
- Organization in a locale

Privileges

User 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 its description.

Privilege Name	Description
AAA	System security and AAA.
Admin	System administration.
InterCloud-Infrastructure	InterCloud infrastructure management.
InterCloud-Server	InterCloud VM management.
read-only	Read-only access. Read-only cannot be selected as a privilege; it is assigned to every user role.
Resource Configuration	Edge and compute firewall configuration.
Policy Management	Edge and compute firewall policies.
Fault Management	Alarms and alarm policies.
Operations	Logs, core file management, and **show tech-support** command.
Tenant Management	Create, delete, and modify tenants and organization containers.

Privileges and Role Assignments

The following table lists the out-of-box roles and the associated privileges.

Role	Associated Privileges
aaa	aaa
admin	admin
intercloud-infra	InterCloud-Infrastructure
intercloud-server	InterCloud-Server
network	policy, res-config, tenant

Role	Associated Privileges
operations	fault, operations
read-only	read-only
tenant-admin	policy, res-config[1], tenant

[1] Users with the tenant-admin role cannot create or delete firewalls under a tenant.

User Locales

A user can be assigned one or more locales. Each locale defines one or more organizations or domains (collectively referred to as *resources*) to which the user is allowed access. In addition, the user has read-only access privileges outside their assigned locale and going up the organization tree. This enables the user to use these resources when creating policies. One exception to this rule is a locale without any organizations, which gives unrestricted access to system resources in all organizations. Only the objects under organizations are controlled by locales. Access to other objects such as users, roles, and resources that are not present in the organization tree are not affected by locales.

At least one locale is required when adding a user account with either the network or tenant-admin role. If all the locales associated with a tenant-admin or network user are deleted, the tenant-admin or network user will not have access to the system. A user with the admin role needs to manually delete the user.

Note Users not assigned to a locale have access to all resources in all organizations. For users assigned to a locale, access is restricted to the objects that reside under the organizations that belong to that locale.

Users with AAA privileges (AAA role) 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, then a user assigned that locale can assign only the Engineering organization to other users.

Note AAA privileges must be carefully assigned because they allow a user to manage other users' privileges and role assignments.

You can hierarchically manage organizations. A user who is assigned to a top-level organization has automatic access to all organizations under 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.

The role and locale assignment for a local user can be changed on Prime Network Services Controller. The role and locale assignment for a remote user can be changed on LDAP. If any of the following information assigned to a user is modified, the administrator must delete all the existing sessions of that user so that the new privileges take effect:

- Role
- Privilege for a role
- Locale
- Organization in a locale

Configuring User Roles

Creating a User Role

Procedure

Step 1 Choose **Administration > Access Control > Roles**.

Step 2 Click **Create Role**.

Step 3 In the Create Role dialog box, complete the following fields, then click **OK**:

Field	Description
Name	User role name.
Privileges	Available privileges. To assign a privilege to the selected role, check one or more of the following check boxes: • Admin • AAA • Fault Management • InterCloud-Infrastructure • InterCloud-Server • Operations • Policy Management • Resource Configuration • Tenant Management **Note** You can assign the admin privilege, which includes all privileges, or you can assign privileges individually.

Editing a User Role

Procedure

Step 1 Choose **Administration > Access Control > Roles**.

Step 2 Select the role you want to edit, then click **Edit**.

Step 3 In the Edit dialog box, check or uncheck the boxes for the privileges you want to add to or remove from the role, then click **OK**.

Deleting a User Role

Except for the admin and read-only roles, you can delete user roles that are not appropriate for your environment.

Procedure

Step 1 Choose **Administration > Access Control > Roles**.

Step 2 Select the user role you want to delete, then click **Delete**.

Note You cannot delete the admin or read-only role.

Step 3 In the Confirm dialog box, click **Yes**.

Configuring User Locales

Creating a Locale

Before You Begin

Verify that one or more organizations (tenants) exist; if none exist, create one. For information on creating tenants, see Creating a Tenant.

Procedure

Step 1 Choose **Administration > Access Control > Locales**.

Step 2 Click **Create Locale**.

Step 3 In the Create Locale dialog box, complete the following fields, then click **OK**:

Field	Description
Name	Locale name, containing 2 to 255 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change this name after it is saved.
Description	Brief locale description, containing 1 to 256 characters. The description can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:).
Assigned Organizations	
Assign Organization	Click to assign organizations to locales.
Assigned Organization	List of organizations assigned to the locale.

What to Do Next

Add the locale to one or more user accounts. For more information, see Changing the Locales or Roles Assigned to a Locally Authenticated User, on page 15.

Editing a Locale

Procedure

Step 1 Choose **Administration > Access Control > Locales**.

Step 2 In the list of locales, select the locale you want to edit, then click **Edit**.

Step 3 In the Description field, change the description as appropriate.

Step 4 Click **Assign Organization**.

Step 5 In the Assign Organization dialog box:

a) Expand the root node to view the available organizations.

b) Check the check boxes of the organizations to assign to the locale.

Step 6 Click **OK** in the open dialog boxes to save your changes.

Deleting a Locale

Before You Begin

Caution If the locale you want to delete is assigned to any user/s, remove the locale from the user list of locales.

Note If all the locales associated with a tenant-admin or network user are deleted, the tenant-admin or network user will not have access to the system. A user with the admin role needs to manually delete the user.

Procedure

Step 1 In the Navigation pane, click the **Administration** tab.

Step 2 In the Navigation pane, click the **Access Control** subtab.

Step 3 In the **Navigation** pane, click the **Locales** node.

Step 4 In the **Work** pane, click the locale you want to delete.

Step 5 Click **Delete.**

Step 6 In the **Confirm** dialog box, click **Yes**.

Assigning an Organization to a Locale

Procedure

Step 1 Choose **Administration > Access Control > Locales >** *locale*.

Step 2 Click **Assign Organization**.

Step 3 In the Assign Organization dialog box:

a) Expand root to view the available organizations.

b) Check the check boxes for the organizations you want to add to the locale.

Step 4 Click **OK** in the open dialog boxes, then click **Save** to save the locale.

Deleting an Organization from a Locale

Procedure

Step 1 Choose **Administration > Access Control > Locales >** *locale*.

Step 2 In the content pane, click the **General** tab.

Step 3 In the Assigned Organizations area, select the organization you want to delete, then click **Delete Organization**.

Step 4 When prompted, confirm the deletion.

Step 5 Click **Save**.

Configuring Locally Authenticated User Accounts

Creating a User Account

When you create a user account, you assign one or more roles to the account. If you assign either the network or tenant-admin role to a user, you must also assign a locale. For information on creating locales, see Creating a Locale, on page 8.

Procedure

Step 1 Choose **Administration > Access Control > Locally Authenticated Users**.

Step 2 Click **Create Locally Authenticated Users**.

Step 3 In the Properties area, complete the following fields:

Field	Description
Login ID	Login name. This name must be unique and meet the following guidelines and restrictions for Prime Network Services Controller user accounts: • The login ID can be between 1 and 32 characters, including the following: ◦ Any alphanumeric character ◦ Underscore (_) ◦ Dash (-) ◦ At symbol (@) • The user name for each user account cannot be all-numeric. • The user name cannot start with a number. After you save the user name, it cannot be changed. You must delete the user account and create a new one.
Description	User description.
First Name	User first name. This field can contain up to 32 characters.
Last Name	User last name. This field can contain up to 32 characters.
Email	User email address.
Phone	User telephone number.

Field	Description
Password	Password associated with this account. For maximum security, each password must be strong. If the Password Strength Check check box is checked, the system rejects any password that does not meet the following requirements: • Contains a minimum of eight characters • Contains at least three of the following: ◦ Lowercase letters ◦ Uppercase letters ◦ Digits ◦ Special characters • Does not contain a character that is repeated more than three times consecutively, such as aaabbb. • Is not the user name or the reverse of the user name. • Passes a password dictionary check. For example, the password must not be based on a standard dictionary word. • Does not contain the following symbols: dollar sign ($), question mark (?), equals sign (=). • The password must not be blank for local user and admin accounts. **Note** The password strength check box on the Locally Authenticated Users pane can be unchecked, indicating that the password is not required to be strong. It must, however, contain a minimum of eight characters. The password field is a required field, and a user cannot be created without providing a password.
Confirm Password	Reenter the password for confirmation purposes.
Password Expires	Indicates whether or not password expiration is enabled. Check the check box to enable password expiration.
Expiration Date	Available if password expiration is enabled. Date that the password expires.

Step 4 In the **Roles/Locales** tab area, complete the following fields:

Field	Description
Assigned Roles	Check the applicable check boxes to assign one or more roles to the user: **Note** You must assign a locale to a user before you can assign the network or tenant-admin role. • aaa • admin • intercloud-infra • intercloud-server • network • operations • read-only • tenant-admin
Assigned Locale	Check the applicable check boxes to assign one or more locales to the user.

Step 5 In the **SSH** tab area, complete the following fields, then click **OK**:

Field	Description
Key	SSH key. If you choose the Key radio button, the SSH Data field is displayed.
Password	SSH password.
SSH Data	Available if Key is selected. Enter the SSH public key.

Changing the Locales or Roles Assigned to a Locally Authenticated User

Procedure

Step 1 Choose **Administration > Access Control > Locally Authenticated Users >** *user*.

Step 2 In the General tab, click the **Roles/Locales** tab.

Step 3 Check or uncheck the appropriate check boxes to assign or remove a locale or role.

Step 4 Click **Save**.

Monitoring User Sessions

You can monitor sessions for both locally and remotely authenticated users.

Procedure

Step 1 Choose **Administration > Access Control**, then choose one of the following:

- **Locally Authenticated Users >** *user*.
- **Remotely Authenticated Users >** *user*.

Step 2 Click the **Sessions** tab to view the user session.

Field	Description
Host	IP address from which the user logged in.
Login Time	Date and time that the user logged in.
UI	User interface for this session: • web—GUI login • shell—CLI login • ep—End point
Terminal Type	Kind of terminal through which the user is logged in.