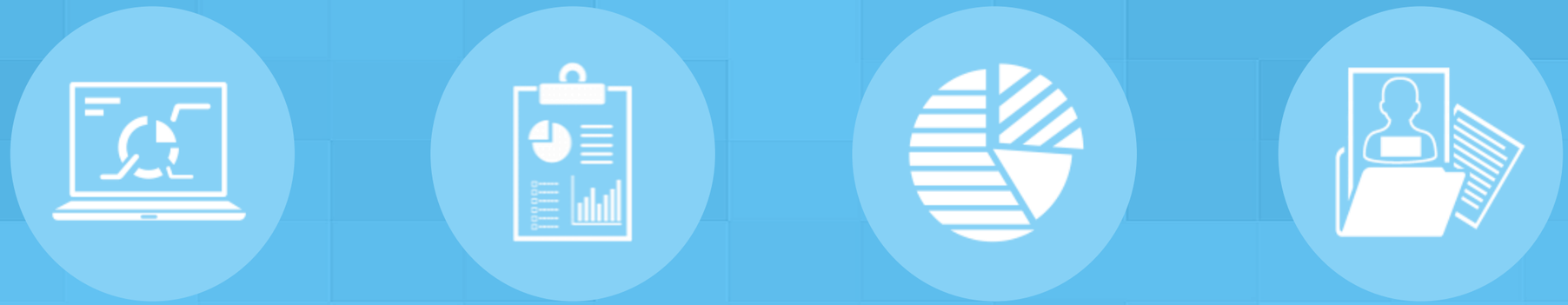
Salesforce Certified Admin and App Builder

Lesson 7—Role Hierarchy



What You'll Learn

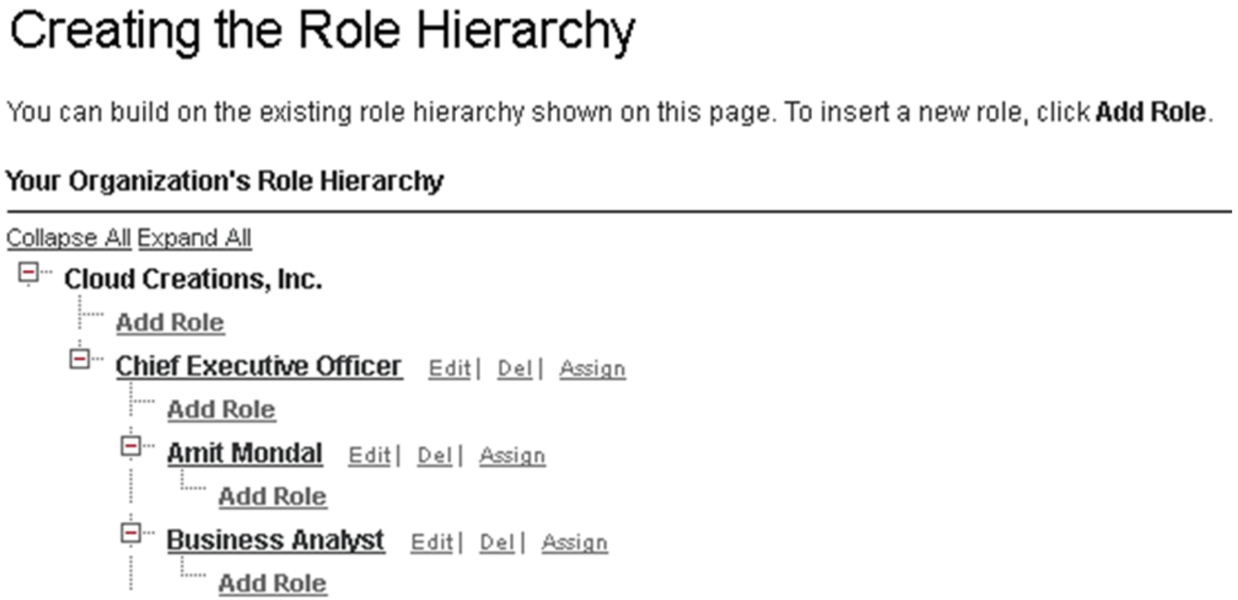
- Viewing the Role Hierarchy and creating Roles
- Enabling Field History
- Creating Groups and Permission Sets
- Creating Permission Sets
- Assigning Roles to Users

Viewing Role Hierarchy

Viewing Role Hierarchy

Important considerations of the Role Hierarchy are the following:

- Role Hierarchy works like your company's organizational chart.
- Roles and sharing settings control the access level to organizational data.
- Users at any level can view, edit, and report on all data owned or shared with users below them in the hierarchy unless the sharing model for an object is set otherwise.
- To view the Role Hierarchy click on Manage users.
- Click on Roles.



Creating Roles

Creating Roles

Considerations when creating Roles:

- Assign the role and title just as you would for your organization.
- Designing the hierarchy is very important as it directly effects communication, efficiency, and security.
- At each role level you have the option to edit the role, delete it or assign it.

Enabling Field History

Enabling Field History

Keep in mind the following when enabling field history:

- History tracking allows you to track changes made to contacts, accounts, and so on.
- To enable history tracking click on customize, accounts (or other object), fields.
- At the top of the page click the Set History Tracking button.
- Click the check box to enable the tracking.
- Click Save.

Creating Groups

Creating Groups

Important considerations when creating Groups:

- A group is a set of users.
- People in a role, other groups, territories, and department can make up a group.
- You can use groups to share records with other users.
- A group can be a personal group or a public group.
- Only admins can create and edit a public group.

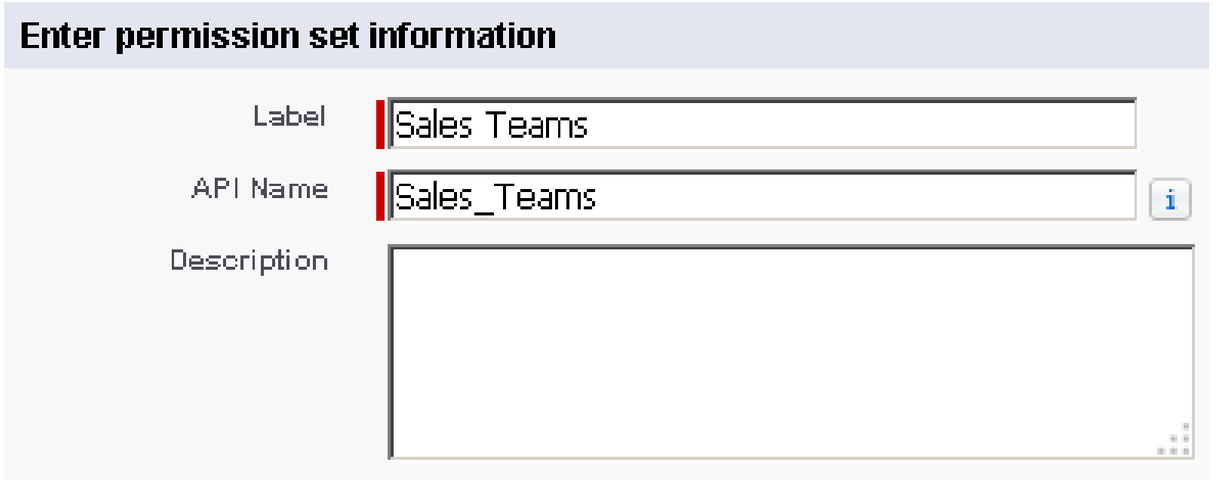
Action	Label ↑	Group Name
Edit | Del	Executive	Executive
Edit | Del	External	External
Edit | Del	Internal	Internal
Edit | Del	Management	Management
Edit | Del	Staff	Staff

Creating Permission Sets

Creating Permission Sets

Here are some important facts regarding permission sets:

- Permission sets can extend a users access without changing the profile.
- To create permission sets click on Manage Users.
- Click permission sets.
- Click new.
- Enter a name and description.
- Select a user license option.
- Click Save.

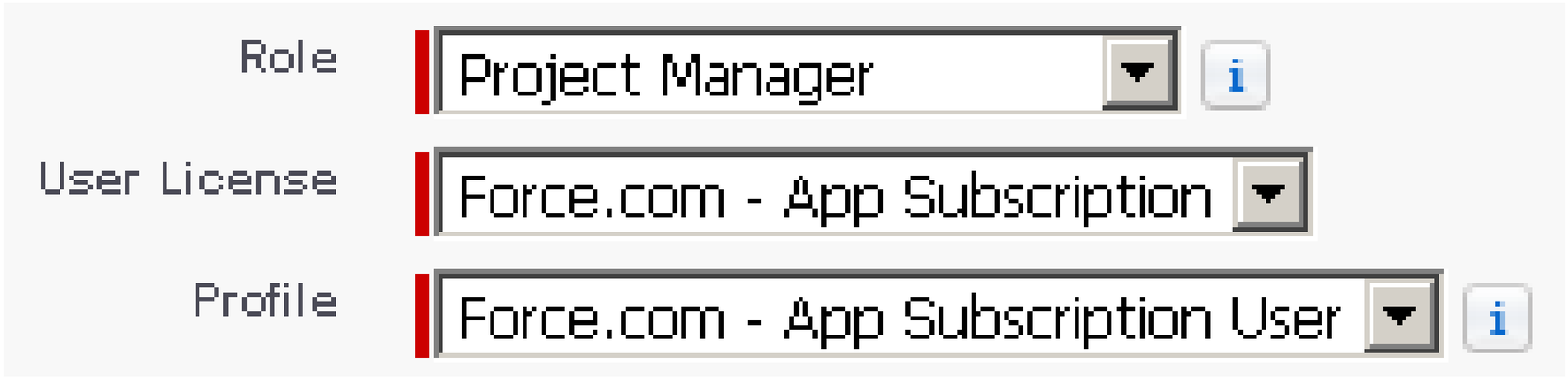


Assigning Roles to Users

Assigning Roles to Users

Keep in mind the following when assigning roles to users:

- After creating your roles you will automatically be taken to the Role Detail Page.
- Click edit to make any changes to your role detail.
- Click assign users and start adding the users for the role.
- Click Save.



Quiz

QUIZ

1

What is the primary purpose of Roles?

a. To restrict access to certain fields on records

b. To enable and restrict access to records

c. To create reports and dashboards

d. To create sandboxes

QUIZ 1

What is the primary purpose of Roles?

a. To restrict access to certain fields on records

b. To enable and restrict access to records

c. To create reports and dashboards

d. To create sandboxes

The correct answer is **b**.

Roles are used to enable and restrict access to records.

QUIZ 2

Field history allows users to:

a. View last modified dates and times of record edits

b. Create new users

c. Restrict access to certain fields

d. View historical changes of field data

QUIZ 2

Field history allows users to:

a. View last modified dates and times of record edits

b. Create new users

c. Restrict access to certain fields

d. View historical changes of field data

The correct answer is **d**.

When field history is enabled, it allows user to view historical changes of field data.

QUIZ 3

What best describes permission sets?

a. Permissions that can be assigned to users without changing profiles

b. System Administrator Profiles

c. A group of profiles

d. A collection of roles and public groups

QUIZ 3

What best describes permission sets?

a. Permissions that can be assigned to users without changing profiles

b. System Administrator Profiles

c. A group of profiles

d. A collection of roles and public groups

The correct answer is **a**.

Permissions sets can be assigned to users without changing profiles.

QUIZ 4

What is true about the role hierarchy and org-wide defaults?

a. Org-wide defaults must be set to private for correct role-based sharing

b. Org-wide defaults must be set to public read or write

c. It doesn't matter how org-wide defaults are set

d. You can't manually share records outside the role hierarchy

QUIZ 4

What is true about the role hierarchy and org-wide defaults?

a. Org-wide defaults must be set to private for correct role-based sharing

b. Org-wide defaults must be set to public read or write

c. It doesn't matter how org-wide defaults are set

d. You can't manually share records outside the role hierarchy

The correct answer is **a**.

Org-wide defaults must be set to private for correct role-based sharing.

QUIZ 5

Which of the following is a true statement of the role hierarchy and sharing rules?

a. The role hierarchy overrides sharing rules

b. Sharing rules override the role hierarchy

c. Org-wide are not affected by sharing rules

d. Profiles are used in sharing rules

QUIZ 5

Which of the following is a true statement of the role hierarchy and sharing rules?

a. The role hierarchy overrides sharing rules

b. Sharing rules override the role hierarchy

c. Org-wide are not affected by sharing rules

d. Profiles are used in sharing rules

The correct answer is **b**.

Sharing rules override the role hierarchy.

Case Study

Case Study

Scenario | Analysis | Solution

United Containers has three sales teams in three territories. They want to restrict user access to their relevant areas. Currently, sales teams can see all sales data across all territories, which is causing problems. Leads are being incorrectly called on by users, causing confusion among prospects and customer alike.

Scenario | Analysis | Solution

United Containers decided to implement the role hierarchy for the following reasons:

1. Roles can be assigned quickly and easily to active users.
2. Using a company org chart allowed an administrator to create correct roles.
3. There is no downtime when the new roles were assigned.
4. Salesforce instantly restricts access when the new role is active.

Scenario | Analysis | Solution

To implement this solution, United Containers performed the following steps:

1. A company org chart was provided to the System Administrator.
2. Roles were created to match the hierarchy of the company org chart.
3. Org-wide defaults were set to private.
4. User records were assigned roles one-by-one.

Key Takeaways

- The role hierarchy is used to restrict access through role-based permissions.
- Org-wide defaults need to be set to private.
- Sharing rules can be created to allow access to records outside the role hierarchy.

This concludes ‘Role Hierarchy.’

The next lesson is ‘Security Controls.’