1.

Q : What is Sharing and Security in Salesforce?

A :

- Data Security is important because you need to control what a user or group of user can see in the org or app.
- Salesforce provides layered sharing model.
- You can easily assign different data sets to different group of users.
- You can control access to your whole org, any specific object, fields, and records.

2.

Q : Sharing & Security Model

A :

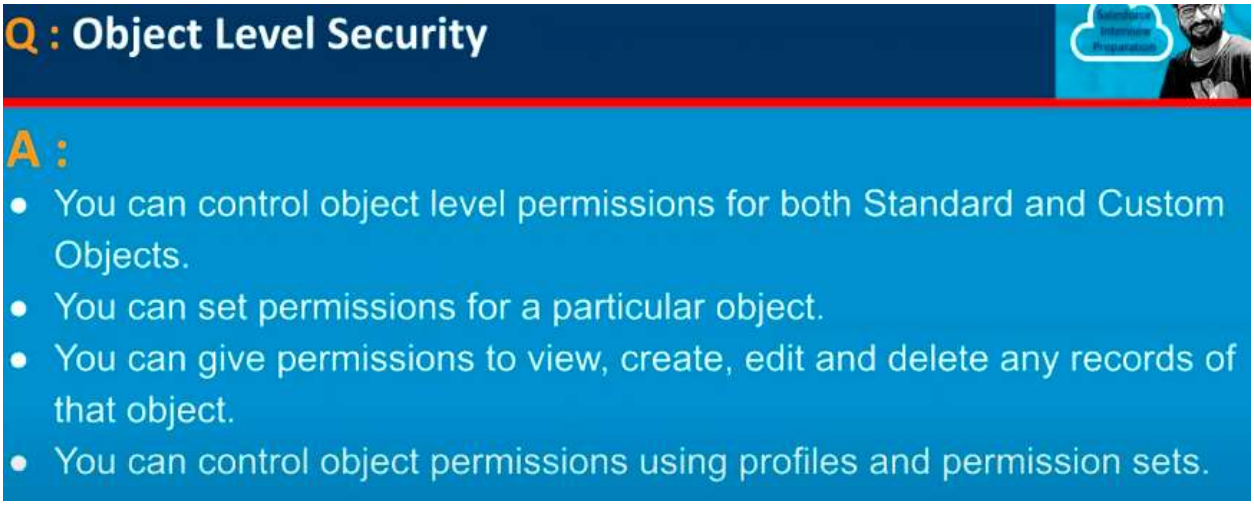
- Organization Level Security
- Object Level Security
- Field Level Security
- Record Level Security


Security
App
Data
Org
1. Profile
2. PermissionSets
1. OWD
2. Sharing Rules
3. Role Heirarchy
4. Manual Sharing
1. Password policies
2. Trusted IP

3.


Q : Organization Level Security
A :
Maintain a list of authorized users
Set password policies
Limit login to certain hours and locations
Limit IP Addresses from which users can log in
Limit the times at which users can log in

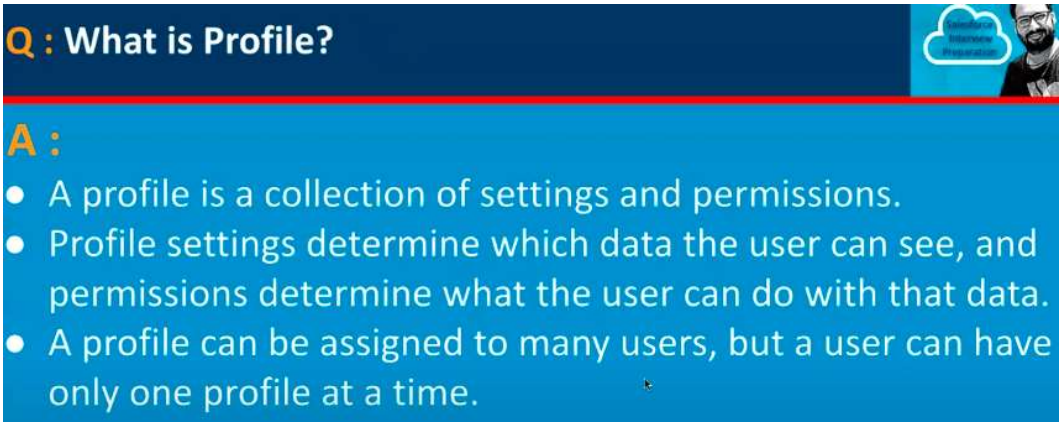
4.


Q : Object Level Security
A :
• You can control object level permissions for both Standard and Custom Objects.
• You can set permissions for a particular object.
• You can give permissions to view, create, edit and delete any records of that object.
• You can control object permissions using profiles and permission sets.

5.


Q : Field Level Security
A :
• You can restrict access to certain fields in Salesforce, even if user has object level access.
• You can make a field visible to a particular user and can hide that from another user.
• You can give Read or Edit permission to a field, if you don't give both then that field will not be visible.
• Field Level Security can be controlled using Profiles and Permission Sets.

6.


Q : What is Profile?
A :
• A profile is a collection of settings and permissions.
• Profile settings determine which data the user can see, and permissions determine what the user can do with that data.
• A profile can be assigned to many users, but a user can have only one profile at a time.

6.

Q : What can be controlled through a Profile?

A :

- Assigned App & Assigned Connected Apps
- Object Settings
- App Permissions
- Apex Class & VF Page Access
- External Data Source Access
- Named Credential Access
- Flow Access
- Custom Permissions & Custom Metadata Type
- Custom Setting Definitions
- System Permissions

7.

Q : Enhanced Profile User Interface?

A :

- You can switch to Enhanced Profile User Interface through Setup > User Management Settings.
- If enabled then you can Browse, search and modify settings and permissions in a profile through a streamlined user interface.

8.

Q : What is Permission Set?

A :

- A permission set is a collection of settings and permissions that give user access to various tools and functions.
- Permission sets extend users functional access without changing their profile.
- Through Permission sets permission can be granted and any time it can be taken away as well.
- Users can have only one profile, but they can have multiple permission sets assigned.

9.

Q : What can be addon through a Permission Set?

A :

- Assigned App & Assigned Connected Apps
- Object Settings
- App Permissions
- Apex Class & VF Page Access
- External Data Source Access
- Named Credential Access
- Flow Access
- Custom Permissions & Custom Metadata Type
- Custom Setting Definitions
- System Permissions

10.

Q : What is Permission Set Group?

A :

- Permission Set group bundles different permission sets together based on a persona.
- A permission set group includes all the permissions available in the permission sets.
- One permission set can be included in more than one permission set groups.
- A user can be assigned one or more Permission Set Groups.
- Also we can assign Permission Set and Permission Set Groups together to users.

11.

Q : What is MUTE in Permission Set Group?

A :

- One can mute some permissions in Permission Set Groups so that they won't be given to the user.
- If you mute particular permission in Permission Set Group then it won't impact individual Permission Set, they remain intact.
- You can anytime unmute the permissions in permission set group.

12.

Q : How many Profiles can be assigned to a user?

A :

- **One**

13.


Q : How many Permission Sets can be assigned to a user?
A :
• Zero or Any number of Permission Sets

14.


Q : Record Level Security
A :
• You can restrict access to records for users, even if user has object level permissions.
• For example, a user can view his own records but not others.
• You can manage Record Level Access in following ways:
○ Organization-wide defaults
○ Role hierarchies
○ Sharing rules
○ Manual sharing

15.


Q : What is OWD?
A :
• It specifies the default level of access of records.
• Org-wide sharing setting lock down the data to the most restrictive level.
• Here you have three access level:
○ Private
○ Public Read-Only
○ Public Read/Write
• You can use other Record Level security and sharing tools to open up the sharing of records.

16.


Q : What is Role Hierarchy?
A :
• Role Hierarchy gives access for users higher in the hierarchy.
• That user can access all records owned by the users below them in the hierarchy.
• Each role in the hierarchy should represent a level of data access that a user or group of user needs.
• You can assign users to role through Role Hierarchy or User detail page.

17.


Q : What is Grant Access Using Hierarchies?
A :
• This feature controls whether the user who is above in the role hierarchy can access the records of subordinates or not.
• It is checked by default for all standard object.
• We can control it for custom objects.

18.


Q : What is Sharing Rule?
A :
• Sharing Rules are exceptions to Org-Wide defaults.
• Through sharing rules you can share records to a group of users or to roles, roles & subordinates.
• So that, they can get access to the records they don't own or can't manually see.

19.

Q : Two ways to create Sharing Rule?

A :

- Owner Based Sharing
- Criteria Based Sharing

20.

Q : What is Manual Sharing?

A :

- Manual Sharing allows owners of particular records to share them with another users.
- Manual sharing is not automated like Org-wide defaults, Role hierarchy or sharing rules.
- It can be useful in some situation where you manually want to share a record with another user.

21.

Q : What is Public Group?

A :

- A group of users
- You can add or remove users from one public group any time.
- Following can be member of a public group:
  - Public Group
  - Roles
  - Roles and Subordinates
  - Users
- You can also control Grant Access using Hierarchies while creating public group.

22.

Q : Object does not have EDIT permission but OWD is Public Read/Write?

A :

- User won't be able to edit the record.

23.

Q : View All & Modify All?

A :

- Grant access to all records of the object regardless of the sharing and security settings.
- View all and Modify all permissions ignore the sharing model, roles and sharing rules.