Q.59) what can be Control through a profile. ?

→ ① Assigned App & Assigned Connected App

② object Setting

③ App permission

④ Apex class & VF page Access

⑤ External Data Source Access

⑥ Name Credential Access

⑦ Flow Access

⑧ custom permission & custom metadata Type.

⑨ Custom Setting Definitions

⑩ System permission.

Q.60) Enhanced ~~User~~ profile user interface ?

→ (i) you can switch to Enhanced profile user interface through.

Setup > user management Setting.

(ii) if enabled then you can Browse. Search and modify setting & permission in a profile through a Streamlined User interface.

Q.61) what is permission Set ?

→ permission Set are used to extend permission to specific users without changing their profile.

Scanned with OKEN Scanner

① A permission set is a collection of setting and permissions that give users access to various tools & functions.

② Permission sets extend users function access without changing their profile.

③ Through permission sets permission can be granted and any time it can be taken away as well.

④ Users can have only one profile but they can have multiple permission set assigned.

Q-62) what can be addon through a permission set

→ ① Assigned App & Assigned Connected App

② object Setting

③ App permission

④ Apex class & VF page Access

⑤ External Data Source Access

⑥ Named credential Access

⑦ Flow Access

⑧ custom permission & custom Meta-data Type.

⑨ custom Setting Definitions

⑩ System permission.

Q-63) what is permission Set Group?

→ ① permission Set Group bundles different permission sets together based on a persona.

(1) A permission Set Group includes all The permissions available in the permission sets.

(3). One permission set can be included in more than one permission set groups

(4) A user can be assigned one or more permission set Groups.

(5) Also we can assign permission set and permission set Groups together to users.

(Q-63) what is MUTE in permission set Group?

Set? → (1) One can mute some permissions in permission Set Groups so that they won't be given to the users.

All

(2) If you mute particular permission in permission set Group then it won't impact individual permission set, they remain intact.

(3) You can anytime unmute the permissions in permission set Group.

(Q-64) How many profile can be assigned to a user?

→ One

(Q-65) How many Permission Set can be assigned to a User?

→ Zero or Any number of permission sets

Scanned with OKEN Scanner

Q-66). what is Record level Security ?

ows, Sharing Rule, Role Hierarchy

→ ① you can restrict access to records for users, even if user has object level permissions.

② For example. a User can view his own records but not others.

③ you can manage Record level Access in following ways:

(i) Organization - wide defaults.

(ii) Role hierarchies

(iii) Sharing Rules

(iv) manual sharing.

Q-67) what are Organization - wide defaults

→ ows Setting control the default level of access users have to each other's records. It can be private, public Read only, or public Read / write.

(i) It specifies the defaults level of acc of records.

(ii) Org- wide sharing setting lock down the data to the most restrictive level.

(iii) Here you have three access level.

(i) private

(ii) public Read - only

(iii) Public Read / write

(iv) you Can use others Record level Security and sharing tools to open up the sharing of records.

Scanned with OKEN Scanner

Security ?
Role Hierarchy
to records/
has object level

view his own

l level Access

efaults.

wide Defaults | owd)
default level
each other's
vote, Public Read
write.

lts level of access

tring lock down
restrictive level.
access level.

cord level Security
en up the

(Q-68) what is Role Hierarchy ?

→ ① Role Hierarchy gives access for Users higher in the hierarchy.

② That User can access all records owned by the Users below them in the hierarchy.

③ Each role in the hierarchy should respresent a level of data access that a user or group of user needs.

④ You can assign Users to role through Role Hierarchy or User detail page.

(Q-69) what is Grant Access using Hierarchies ?

→ ① This feature controls whether the User who is above in the role hierarchy can access the records of subordinates or not

② it is checked by default for all standard object.

③ we can control it for custom objects.

(Q-70) what are sharing Rules ?

→ Sharing Rules extend record access beyond the OWD setting to users who need additional access.

① sharing Rules are exceptions to org-wide defaults.

② Through sharing rules you can share records to a group of users or to roles, roles & subordinates.

③ So that, they can get access to the records they don't own or cann't manually see.

Q-71) Two ways to Create Sharing Rule ?

→ Owner Based Sharing Rule
Criteria Based Sharing Rule.

Q-72) What is Manual Sharing ?

→ ① Manual Sharing allows Owners of particular records to share them with another users

② Manual sharing is not automated like Org-wide defaults, Role hierarchy or Sharing Rules

③ It can be useful in some situation where you manually want to share a record with another user.

Q-73) What is Public Group ?

→ ① A group of users.

② you can add or remove users from one public group any time.

③ Following can be members of a public group.

① public Group
② Roles
③ Roles and Subordinates
④ Users

④ You can also control Grant Access Using Hierarchies while creating public Group.

Q-74) object does not have Edit permission but owd is public Read / write ?

→ Users won't be able to edit the record.

Scanned with OKEN Scanner