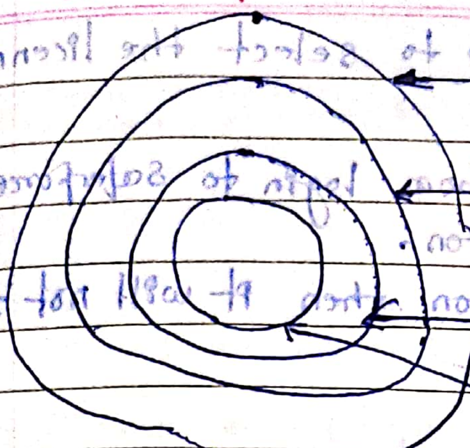
Security



① Org level security — ① password policies. ② Network Security.

② Object Level Security — ① from profile. ② from permission set.

③ field level security — ① from profile. ② from permission set.

④ Record level Security — ① OWD (Org wide default) ② Sharing rule. ③ manual sharing. ④ Role hierarchy.

means Senior have access to see the junior records but junior doesn't have access of his.

profile.

① we have 2 type of profile, i.e. ⓐ std. ⓑ custom

② How to create profile, we can create a new profile by cloning existing profile (std or custom).

③ profile defines how much access that user can have.
किस level तक access है वो, i.e. Sr. Engg., Tr. Engg.

Roles

means जो company में Job Description है वो।

① Role defines the job profile which you can hold in your organization.

② Roles are placed into a hierarchy

Users

① If you want to create any persons account in salesforce then you have to create record of user object

② To login into salesforce Email, UserID & password is important.

③ To create any user we have to select the licence.

④ freeze button :-

To prevent any user from login to Salesforce temp then we use freeze button.

⑤ When we use freeze button then it will not remove any access from user.

⑥ Active checkbox :-

- If Active checkbox is true then user can login into Salesforce Account.
- If Deactivate any user then license which he/she holds it will get free from all that user.

नाम के बाद जो लिखते उसे postfix & आगे जो लिखते उसे prefix

Organizational Security :- It is 1st level of Security.

- It is used to restrict someone from login, & if we want to give permission to user then we can managed from Organizational Security.
- Just like password, वगैरह.

कोई भी company में organizational security में नहीं जाना रहता fix, its nature in company, because lock होते

Use of Organizational Security :-

① users can login but by using O.S. we verify of enter password.

i.e. 8 chara. चाहिये, ये symbol चाहिये, वगैरह

② We can defined IP Address Range..

i.e. particular area में जा कर ही login करेगा वरना नहीं.

① If you want to give permission to all Users then Answer &
→ password policies under Administration section.

password policies &

① User password expiration & कितने दिनों में expiry होना चाहिए इसलिए।
② Never expiry के लिए manually change करना पड़ता है।
Enforced password history & Latest password याद रखता है। 3-4 password.
③ Minimum password length & कितने character चाहिए। ①
④ password complexity req. & मतलब Alpha + numeric. No, character use करना।
⑤ password question requirement & इसमें password नहीं आना चाहिए। कम और question होना born, nickname
⑥ Max. invalid login Attempt & कितनी Attempt if password wrong.
⑥ Locked out effective period & If password is wrong multiple time then it will locked for 15 minutes. just like that.
⑦ Obscure Secret Answer for password reset & मतलब password reset at the time हमें password question पूछेगा। which city you born?
⑧ Require a min. 1 day password resetting & मतलब password reset करने के 24 hr में reset नहीं कर सकता।
⑨ Allow use of setpassword() API for self reset. & API User होते हैं जो external user होते हैं। यह API user से login करते हैं।

forget Password. &

Message & message दे सकता।
Help Link & help Link दे सकता।

Network policies & It is used to lock some one & restrict & use at particular location, से Access के लिए
① Black listed IP Address & मतलब यह API Range set करते उसमें Block करता No. Block list API
② White listed API Adder & मतलब API Range मतलब जो होता White listed API Adder.
Start API Adder & Last API Adder

Security Model (Org Level Security)

Q.1. from where we can give Org level security?

→ - There are two ways of give org level security
- We can restrict user by using.

① password policies.
② IP Ranges restrictions.

① How to apply password policies (Applicable for All Users)

① Setup → Setup → Administer → Security Controls → password policies.

② Setup → Administer → Manage Users → profile
(Then click on profile, we have to the end of the page)

② How to apply IP Ranges (This Applicable for Single User)

Setup → Administer → Security Control → Network Access

Q.2. Which options do we have while giving Org Level Security

→ ① password policies.
② IP Ranges Restrictions.

Q.3. What is mean by IP white listing ?

→ IP White Listing :- The IP Address which lies both start IP address & End IP Address is called as IP White listing.

Q.4. What is exact diff. of applying org level security through profile & setup ?

→ Setup :- Whenever we apply org level security through setup, it will get apply to all users in org.

profile :- Whenever we apply org level security from profile, it will get apply to the user whom that profile is assigned.

Q.5. From where we can set login hours & why we use it ?

→ Setup → Administer → Manage Users → profile → click on profile name → System → login hours.

Suppose, we want to access the org only from 9am to 5pm & from monday & friday

Q.7. What is the meaning of User password policies expire in field of password policies?

→ User password policies expire : ① Means giving time span for user password, i.e. in that time span user can access the password, After that time span user password will expires. for that user have to changed that time span.

② By default 90 days.

③ It is the length of time a user password expire, f must be changed.

Q.8. What is the use of enforce password history field in password policies?

→ Enforce password history : Nothing but a remembering latest password enter by user.

Set → By default they will remember 3 latest password enter by users.

Note : you can select no password remembered when only when you have to select Never expire for that in user password policies expiry.

This setting is not available for self-service portal.

Q.9. How many password system can remember ?

→ 24 password. in Enforce password history.

Q.10. What is the minimum password length ratio ?

→

- Minimum password length must be bet 5 to 50 character
- By default char. length is 8.

Q.11. Which options we can see in password complexity requirements

→

1. No restriction user
2. Must include alpha & numeric character.
3. must include alpha, numeric & special characters.
4. Must include number, uppercase & lowercase letter.
5. Must include number, uppercase & lowercase letter & special characters.
6. Must include 3 of the following - Numbers, Uppercase, lowercase & Special characters.

Q.12. Which option we can see in user password expire in ?

→

1. 30 days.
2. 60 days.
3. 90 days.
4. 180 days.
5. one year.
6. Never Expires.

Scanned with OKEN Scanner

Q. 13. What is the use of password question Requirement?

→ Use of password question requirement is that to identify wheather it is a particular user or not, for security purpose it is used.

None – No restriction on the answer, The user must provide answer to the password hint question.
– This setting is default.

Cannot contain password – In both password question requirement of giving Answers, password must not be included.

Q. 14. Which options are available for max invalid login attempts?

→

(1) 3
(2) 5
(3) 10
(4) No limit.

Q:15 What is locked effective period out for the option?

→ **Locked Effective period out** means locked the user for a particular time period, such like, 15, 30, 60 min or forever, When user exceed level of entering (By entity multiple time wrong password).

#Note:- A locked user must wait until the locked period expire.

Alternatively, a user with the reset user password & unlock permission can unlock a user from setup.

Setup → user → select user → click unlock.

This button is only available when a user is locked out

Q:16 What happens if we check require a minimum, 1 day password lifetime?

→ if user check this check box,

Mean's once password is changed then it will can't be changed for 24 hrs.

This policy applies to all password changes, including password reset by the Admin.

Object level Security

Profile में permission :-

Object level Security :- There are 6 type of permission/Action we can give i.e. ① Creat, ② Edit ③ Read ④ Delete ⑤ View all ⑥ modify all.

⑤ View All & ⑥ modify all → गलती से भी देनी नहीं होती है। ये Adiministrative permission होते हैं।

सब के Record देख सकते हैं। किसी का भी Record modify कर सकते हैं।
Read, creat, edit, Delete.

किसी भी Object के सामने के permission Uncheck रहे तो हम वो secondary User को hidden रहता है। सब के लिए उसके अंदर के लिए

① # Read permission :- Object visible रहता है। Record दिखते हैं but create & edit नहीं कर सकता है।

② Create Peremission :- Create permission देते समय Read, अपना-अपना आती है। जब create Unchecked रहा तो Read भी हो जाता है।
Create permission में Record देख सकते हैं। plus new create कर सकते Record clone करके new Record कर सकते। But edit or delete option नहीं रहता।

③ Edit permission :- Edit permission देते समय हम New Record नहीं कर सकते। But we can edit Record मतलब Edit का button रहता।

④ Delete permission :- सिर्फ खुद का Record Delete कर सकते हैं, दूसरे का नहीं सकते option रहता दूसरे के Record के पास but error देता है।

इसमें सिर्फ Read, edit, delete रहता है।

Q ① Delete के साथ edit की button or permission क्यों आती है?

→ edit मतलब Database value update कर रहे हैं, Normal edit करते तो 1 value में दूसरी value change करते हैं। तो एक value को Blank करके भी हम Update कर सकते हैं, और हम पूरी Row blank करते हैं तो हम उस record को Delete करेंगे, तो उसमें क्या होता है एक value ~~update~~ present होती है उसमें update होके Blank होती है मतलब Delete होती है।

--- इसलिए Delete भी edit option होता है क्योंकि Delete भी Blank करता है.

Permission Set :-

Use :- It is used to set permission for individual to give extra permission

⑦ Why we can not give any access to child if parent does not have any access?

→

Object level Security.

(1) How many ways we can give object level security?

→ There are 2 ways we can give object level security
By going to
(1) profile
(2) permission set

(2) What is permision set?

→ permission set ← It is used to set permission for individual
by using permission set we can assign
extra permission

(3) Can we restrict the access through permission set?

→ No.

(4) Which options we have while giving object level security?

→
(1) Read,
(2) Create,
(3) Edit.
(4) Delete
(5) View All,
(6) Modify All.

Scanned with OKEN Scanner

Object level Security

(5) Can We give only creater accers not Read, Edit, Delete to any profile?

→

No, We can not give only create accers, because at the time of giving creater accers bydefault there is Read accers, thats Way.

(6) Can We give only delete accers not Read, delete, edit to profile?.

→

No, We can not give only delete accers, because at the time of giving delete accers bydefault there is read & edit accer comes, thats way.

(6) If We have create on Read accers from profile level then can we give delete accer without Edit accers through PS?.

→

No, We cannot give because at the time of giving delete accers, ~~then~~ read, edit by default accers are there, thats way.

(7) If how many ways we can hide any object?.

→

By don't arrign any permision such, Read, create, edit

Object Level Security.

(8) If We have 100 users for a particular profile & we want to give create access for 2 users, 50 Us should have edit access & rest of others should have full access then how to achieve pt?

→ Through profile we give create access 2 User. Through permission set give edit access to 50 person through new permission set give full access to remaining 48 persons.

(9) What is meaning of View All, Modify All?

→ View all & modify all are administrative permissions

View all → permit all users to view all the records

modify all → permit all user to update/edit all records.

(10) What is profile?

→ profiles → ① It is define ur how much access that user can have.

② There are 2 type of profile ⓐ Standard User ⓑ Custom User.

③ How to create profile. → By cloning existing profile we can create new profile.

(11) Can we create profile without cloning Sanity profile?

→ No.

(12) Can We create new profile by cloning custom profile?

→ Yes.

(13) Suppose If we have object A (parent/master) & object B (child) so can we give edit Accer to object B. without giving any accer to object A.

→ No. Because at the time of giving edit Accer to child (object B) then by default Read accer are gone to parent (object A).

(14) Suppose we have only Read accer to master object then can we give delete accer to child object?

→ Yes.

(15) Suppose we have lookup beth two objects then can we give edit accer to child if parent read accer only?

→ Yes.

(16) What happens If we do not give any accers from object level Security?

→ then object will be hidden for secondary user.

Field level Security

(1) How to give field level security ?.

→ (1) By going to profiler. 1st Way of

Setup → Administer → manage User → profiles

Then we go to field level security. Page. (By editing the field we can give field level security)

← Then go to object ← custom field level security setting, from that we have to view our custom Appln. click on view button.

← Then we have to select profiler. & click on profiler Name

(2) By going to permision set. 2nd way of — for extra permi

Setup → Administer → manage User → permision s

Then we have to select object ← Then we have to go to object setting (checkout) ← Then we have to enter P.S Information. (i.e. Label, API Name). ← By click on P.S. Then we have to select (New button)

↳ By clicking on object then we go to field permision setting from that we can give/edit permision of fields.

(2) Which options we have, we can give while giving field le security ?.

→

(1) Read Access.

(2) Edit Access. (Whenever we checked edit Access then by default read Access is given.)

(3) If we any user has creater accer from profile & has edit permision set for obj level security & has no accer from field level security then what should be the final result &.

→

- Then User can creater record, read, and User can edit already creater record, Because they have given creatr. & edit permision.
- But User cannot see field & edit field accer, i.e. not appear on UI, Because they have not given any accer to fieldr (mean permision of Read & edit).

(4) If we have 50 Users & from 50 we want to give Edit, Creater, & Read Accer to 5 Users & For there 5 user we need to hide the fieldr, & other 10 user should able to only edit the recordr. but fieldr should be read only then how to achieve it &

→

(12) for which types of fields we can not change field level security?

→ for standard fields, for required fields, fields which is getting created while object creation for these fields FLS is provided by Salesforce & we can not change it.

(5) Can we give edit access if we do not have read access?

→ No, Because at the time of giving edit access read access automatically given, if there is read access not checked, then edit access not work, Because whenever we want edit record, for it all we have to read

(6) We have junior engineer in company & he has ones read, edit access for object & have if we have another junior engineer & he have read access for object & edit access for field then he is able to edit the field value?

→

Scanned with OKEN Scanner

(11) What if field level security for created By field &
Read Accer.

→

(7) If we have no accer for any object & have edit accer for field then what will be the output &

→

(8) Can we assign permision set to profile. &

→

No, Because permision set is user specific, & profile is assign to all user come under profile.

(9) If we have no accer for any object & have edit accer for field then what will be the output &

→

(10) Can we assign permision set to multiple user at the same time &

→

Yes we can assign permision set to group of people. (mean group of user).

Scanned with OKEN Scanner

Record level Security

(1) How many type of record level security we have ?

→

(1) OWD (organization wide default.)

(2) What is OWD ?

→ (1) OWD → stand for organization wide default.
(2) It is bareline security for your salesforce instance
(3) It is used to restrict accer.
(4) By using organization wide default. we can give acce
to default internal user & default external i.e. (1) private, (2) public
read only (3) public read/write (4) public read/write/transfer.

(3) Which option we can see while giving OWD ?

→ There we will see 4 column, i.e.
(i) object (ii) Default Internal User (iii) Default External
(iv) Grant Accer Using Hierarchies. → it is unchecker for
custom object. & check
for standard object always

from.

In default internal user → (1) private
In default external user → (2) public read only.
we give — (3) public read/write.
there 4 type (4) public read/write/transfer
of Accer
to user.

④ What is mean by private OWD ?

→ private OWD ⇒ mean only record owner can see his records., other user will not have any access to her records.

⑤ What is public Read only ?

→ public Read only ⇒ mean primary user records secondary user can see only.
OWD
or
Other user can see only primary user records.

⑥ What is public Read/write ?

→ public Read/write ⇒ mean primary user records secondary user can see, & he able to write something in it.
OWD
or
other user can read & write in primary user records.

⑤ What is controlled by parent ?

→ Mean if there is in between 2 object masterrelation is happen.
then the access of child is controlled by parent.
that way we are not able give any access to child object because there is MDR happen between 2 object & child object is controlled parent.

(6) In OWD we have column default External Access, what it represents?

→ Default External Access means External user can login on record through there API Address, for external user, we granted access i.e. private, public Read only, public read/write, public read transfer.

(7) for calender object which OWD options do we have?

→ There is 4 OWD happen.

(i) Hide Details.
(ii) Hide Details & Add Events.
(iii) Show Details.
(iv) show Details & Add ~~External~~

(8) If we have 5 Users in a company & we want that only owner of record can see his record then what type of OWD we will apply?

→ ① for that we will give private OWD.
② & Uncheck the hierarchy checkbox.

(9) If we want that we have 100 users & we need that only owner can edit the record an other can only read the record then what we need to do?

→ public read only – OWD.

(10) If we have read access through object level & public Read/write at OWD then what will happen?

→ User will not be able to edit/create, new record if only read access is given through object level security.

(11) If we have 3 users & one is manager & 2 are employees, Now we want only manager can edit both employee peer records, employee can see their own records only.

→ for that we have to give public read only OWD & checked hierarchy access.

(12) If what is the use of Grant access using Role hierarchy?

→ It controls the data access to records on a selective object based on job role of user.

Page No.
Date: /

(13) If we have 3 users & one is manager & 2 are employees, now we want that only manager can read both employees records, employees can see their own records only & one employee should be able to see & edit others but second employee should be able to see first employee. How to achieve it.

→

Assume 3 persons are A, B, C. Requirement:

(1) Manager (A) can see / edit records of B & C.
(2) B & C can see their own records.
(3) B can see / edit records of C.
(4) C can't see records of B.

Assign roles as below,

Manager (A)
↓
B (Senior Analyst)
↓
C (Analyst)

set OWD to private & check hierarchy access

(14) If we have 3 users, & one is manager & 2 are employees we want that all users can see & edit their own records, manager also can't see records of employees, then what should we do

→

2 ways to achieve this.

① Set OWD to private & uncheck hierarchy accer.

② Keep all user on same role if you are not able to uncheck hierarchy accer. Then set OWD to private.

(11) What is diff. bet manual sharing & sharing Rule?

→ With sharing ruler & manual sharing one can share records with users when don't have accer to record.

Manual Sharing	Sharing Ruler.
① It is used to give accer to (single) specific record.	① It is used to give accer to multiple records that meet the criteria / record owner.
② It is a permission to accer one record of any object	② It is a set of predefinite condition on object & if objectr record meet there cond' then record is automatically shared to predefined role / group.
③ manual sharing can be granted by record owner.	④ You can't share record to single user

Scanned with OKEN Scanner

(18) What is the diff. bet^n sharing rules & hierarchies

→

Sharing Rules	Hierarchies
(1) It is set of predefined condition on an object & if object record meet there it will be shared with predefined role/ group.	(1) Role hierarchies is defined structure of records should be shared within your salesforce org. Users higher up in hierarchy will have complete access to records own by them & their subordinates
(2) With sharing rules you can share records with user that are not part of hierarchy	(2) Record will not be shared with users which are lower in hierarchy & not part of hierarchy.

(19) Which rule type we have in sharing rules?

→

(1) Based on record owner.
(2) Based on criteria.

(1) In record owner you need select record owned by members of
   (a) public groups.
   (b) Roles.
   (c) Roles & subordinates

(20) With Whom are, we can share records using sharing rule &

→

You can share with,

(a) public Groups.
(b) Roles.
(c) Roles & Sub-ordinates.

(21) Can we share records to individual user by using sharing rules.

→ No

(22) Can we share records to individual user by using manual sharing &

→ yes.

(23) Can we use manual sharing in lightning instance &.

→ yes.

(24) Which levels of access we can give through sharing rules &.

→

(1) Read only.
(2) Read / write.

(25) Suppose we have grant access to role hierarchy but manager does not have access to object A & employee under him have access to the object, so could manager can see the records of employee or not &

→ No, manager should have access to object A to see / edit the records.

Scanned with OKEN Scanner