

Oops!! Whats wrong with my Salesforce sharing rules...



First time while I was preparing for my Administration Exam I watched this video "*Who Sees What: Overview on salesforce*" (<https://www.youtube.com/watch?v=jDYfTfaqclk>)... I was very impressed! Later while working hands on I realized things can get really messy and could easily go out of hand if we don't really keep strong strategy and control.

Too many roles, too many sharing rules, complex Account teams, too many permission sets, these all could lead to loss of control on data visibility aspects in your Org. It is advisable to administer the sharing with strong change management process in place.

Who Sees What in Salesforce is fine, but when we come across a situation where we need to figure out why a particular entity, record or a field is being visible / editable by some other user - how should we approach such problem statement ?!

Recently in one of our engagements, post data migration - we had this exact issue to solve. Client said that a particular USER was not supposed to see other account information, whereas when we simulate and log in behalf of the USER, we could see much more accounts than he / she we thought should be seeing in actual!

Now, Is there a logical way to solve or get to the root cause of these kind of sharing issues! Let's check out. I am considering an ACCOUNT record visibility issue for illustration here:

PROFILE / PERMISSION SETS

Profile / Permission set controls CORE CRUD permissions for Object as well as Fields, so let's say this is bit easy. Hence let's focus more on Record visibility, ability to read or edit the records of some other user which is where a lot many permutations / combinations are possible!

OWNERSHIP:

Is the USER in question is actually the current owner of the Account record? check for this first

DEBUG LOGS:

Ok - Shall I enable Debug logs? And trace the log for any clue?! -- Nopes, this won't help. In salesforce the sharing reason is not revealed via debug logs ...

OWD:

Hey!! What about OWD? Is it Public Read-only / Public Read write already? If yes, then you already got your answers... else if OWD = private, keep checking further...

SHARING RULES (Public group, Role, Role/Subordinate, Queue):

Is there any Sharing rule on Account? Is sharing rule based on Public group? Or Role and its subordinates? If yes, then quickly see if the USER in question is part of Public group!? Or see if the Sharing rule is directly sharing to a particular ROLE? Or Access is rolling up the hierarchy? Or sharing rule is for ROLE+Sub-ordinates?! If No sharing rule is found, then move on...

SHARING RULE OVERRIDE:

See if there are any Sharing rule over-ride? I.e. exactly PROFILE / PERMISSION SET with VIEW ALL / MODIFY ALL permissions?! Permission set - not associated either.

ACCOUNT TEAM:

Account team - is a feature to enable users with different level of access on a particular Account so they can work as a team, hence check if the USER in question is part of Account team?! Or at-least see if any of the Account team user is beneath this USER in the ROLE hierarchy? Or if the USER is manager of the Account team member?!

ACCOUNT TEAM MEMBER / ACCOUNT SHARE:

You may use Workbench to query the Accountteammember entity along with AccountShare entity to see which all entities are shared with this USER and in what level?! I.e. READ / EDIT?

Did you get to root cause yet?! else keep continuing ...

ACCOUNT SHARE (Implicit, Manual, Owner, Team):

When you search on Accountshare - some sharing reason will be due to IMPLICIT permission, which means - because the USER is the owner of some of the child entities (i.e. if USER is owner of Contact , then implicitly this USER will have READ access on the Account to which his Contact is linked to), same applied b/w Opportunity and ACCOUNTs

APEX SHARING:

Code based sharing is possible, however this is more of invoking a Class as system user or as a specific user and execute a logic

SHARING SETS:

If you are dealing with Communities user - better to check Sharing sets to see if there are any sharing b/w external users to internal users?!

OWD RECENT CHANGES:

See if someone changed OWD recently? This might lead to re-calculation of sharing - but at times, this will take more time. This might have led to USER ability to see the record.

SFDC SUPPORT:

Are you tired, still not able to figure out root cause, raise a SFDC case and hope for some help!