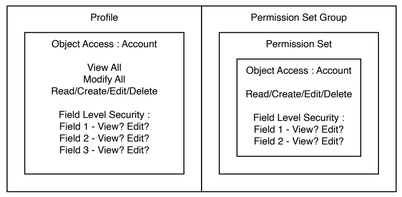
SALESFORCE ARCHITECTURE REFERENCE - SHARING ARCHITECTURE SU20 - FOR INFORMATION PURPOSES ONLY - V1.0 - MARK CANE - 2020-10-22

Salesforce Sharing Architecture

Object Level Access

Profiles define how users access objects and data, and what they can do within the Salesforce application. Permission sets can extend this baseline with additional object-level and field level access.



Profiles and Permission Sets :
Object Access -
Read, Create, Edit, Delete permissions.
View All / Modify All -
Permissions override the Sharing Model to provide access to all records.

Field Level Security - Read, Edit permissions per Field.

Permission Set Groups - Permission Sets can be combined for streamlined management and assignment. One Muting Permission Set can be added to remove permissions from a Permission Set Group (to avoid duplication).

Object Record Tables

Standard Object and **Custom Object** Record-Level access is controlled by OWD and the Sharing Model (Declarative and Programmatic Sharing).

Object-Level and Field-Level access permissions can be managed via Profile or Permission Set.

Standard Object : **Account**

RecordId	Name	Owner
001…A	Acme Inc	User A
001…B	Universal Containers	User B
001…C	Fabrikam Ltd	Queue A

Account Org Wide Default (Internal) : Private

Custom Object : **MyCustomObject__c**

RecordId	Name	Owner
00X…A	Custom Record 1	User A
00X…B	Custom Record 2	Queue A

MyCustomObject__c Org Wide Default (Internal) : Private

External Objects do not support OWD or Record-Level access. Object-Level and Field-Level access permissions can be managed via Profile or Permission Set.

Big Objects do not support OWD or Record-Level access. Object-Level and Field-Level access permissions can be managed via Profile or Permission Set.

Org Wide Defaults

Org Wide Defaults (OWD) set the baseline record access per Object for Internal and External users. OWD is the only (restrictive) record access feature which removes access. All other features add access to the OWD baseline.

Internal OWD :
Internal Salesforce license types.

External OWD :
External Salesforce license types i.e. Community, portal users.

OWD Settings (Setup > Sharing Settings) **:**
Private - Record Owner and those above in the Role Hierarchy can view and edit records.

Controlled by Parent - For detail objects in a master-detail relationship record access is controlled by the master object.

Public Read-only - As Private plus all Users have read access.

Public Read/Write - All Users can read and edit records.

Public Read/Write/Transfer - All Users can read, edit and transfer records (Case & Lead).

Public Full Access - All Users can read, edit and delete records (Campaign).

Grant Access Using Hierarchies :
Custom Objects only. If deselected then Users in higher roles or territories in the hierarchy don't receive automatic access.

Record Level Access (or Sharing)

It is recommended to reduce the Portal Roles count from 3 to 1 to reduce complexity.

Sharing Rules (Setup > Sharing Settings)

Sharing rules provide lateral Record-Level access based on statically defined conditions.

Rule Types :

Ownership Based Sharing (OBS) -
Records owner by [Public Group] or [Role and Internal Subordinates].

Criteria Based Sharing (CBS) - Field equals Value conditions with Filter Logic.

Records shared with [Public Group] or [Role and Internal Subordinates].

Account > Default Account Contract, Asset access; Read-only, Read-write.
Opportunity Access, Case Access (Private Read-only, Read-write).

Custom Object > Access Level (Private Read-only, Read-write).

Account Sharing Rules : OBS

Type	Owned By	Shared With	Default	Opp	Case
Ownership	00G…A	00G…B	RW	RO	RO
Ownership	005…A	00G…C	RW	RO	RO

My Custom Object Sharing Rules : CBS

Type	Conditions		Logic	Shared With	Access
Criteria	Field=Value	Field=Value	AND	00G…B	RO

Record Access Concepts

Grant Types :

Explicit - the record is shared directly to Users or Groups.

Group Membership - User, Personal or Public Group, Queue, Role or Territory is a member of a Group that has explicit access to the record.

Inherited - User, Personal or Public group, Queue, Role, or Territory inherits access through a Role or Territory hierarchy, or is a member of a Group that inherits access through a Group hierarchy.

Implicit (aka Built-in sharing) - Users can view a parent Account if they have access to its child Opportunity, Case, or Contact. If those Users have access to a parent Account, they can also access its child Opportunity, Case, and Contact records.

Record Access Logic :

When a User attempts to access one or more records:
.. a SQL statement is generated that searches the Object Record table for records matching the query filter.
.. If records exist, the SQL statement is extended to join the Object Records table with the Object Sharing table, and the Object Sharing table with the Group Maintenance tables.
.. Salesforce executes the query and checks for access grants that give the User access to the records.
.. The least restrictive access grants are used.

External User Record Access

Customer Community (High Volume Portal User)

Users with HVPU license types are not assigned a Role and can't have records shared to them via Sharing Rules.

Sharing Sets - Provide record access to HVPU users (by Profile) for an Object relationship from the User's Account or Contact.

Direct - Account=>Case
Indirect - Account=>Asset=>Case

Sharing Groups - Provide internal Users with access to records owned by HVPU users. The Sharing Group is associated to a Sharing Set and provides access by Role, R&S or User.

Customer Community Plus / Partner Portal

When an External User is first added 3 roles are created for the Partner (or Customer) below the Account Owner's role; Executive, Manager and User. Sharing Rules can then be added.

The Super User permission provides access to records owned by other partner users with the same role or below.

Other Access Types

Listview Access

"Manage Public List View" permission.
Access can be provided to;

Me
All Users (including Community)
Certain Groups of Users
—>Public Groups
—>Roles
—>Roles & Subordinates

Report Folder Access

"Manage Reports in Public Folders"
"Manage Dashboards in Public Folders" permissions.

Share with;
Users, Roles, Public Groups, Roles and Internal Subordinates, Roles, Internal and Portal Subordinates, Territories, and Territories and Subordinates.

Access level; View, Edit and Manage permission

Object Sharing Tables

Object Sharing tables store Explicit and Implicit access grants grant in separate rows called sharing rows, each of which grants a User or Group record access. Share objects do not exist for Detail objects in a Master-detail relationship and where both Internal and External OWD is Public Read/write.

When a record owner changes; Manual (Row Cause) sharing rows are deleted.

Share Object : **AccountShare**

RecordId	UserId or GroupId	Access Level	Row Cause
001…A	005…A	Full	Owner
001…B	005…A	Full	Owner
001…C	00G…A	Full	Owner
001…A	005…B	Read	Manual
001…B	005…A	Read/Write	Rule
001…C	005…A	Read/Write	APEX

Share Object : **MyCustomObject__Share**

RecordId	UserId or GroupId	Access Level	Row Cause
00X…A	005…A	Full	Owner
00X…B	00G…A	Full	Owner

Access Level :
—> Full
—> Read/Write
—> Read

Row Cause : Indicates the reason for the access grant.
—> Owner
—> Manual
—> Rule
—> ImplicitChild
—> ImplicitParent
—> Team
—> Territory
—> *Custom*; For Custom Objects edit the Apex Sharing Sharing Reasons related list. Up to 10 max.

Group Maintenance Tables

Group Maintenance tables store the list of Users or Groups that belong to each Group, indicating direct or indirect membership (i.e. Inherited access grants).

Established in advance following Group (or Role or Territory) creation or membership changes. The Granular locking setting can avoid lock contention during recalculation.

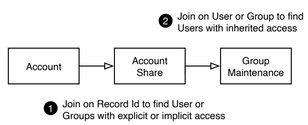
During Sharing Recalculation the system creates 3 System-defined Groups for each Node in the Role Hierarchy (the same logic applies to the Territory Hierarchy) :
—> Role (User is assigned to the Role or a parent role)
Usage; Manager record access
Membership; Direct (Users assigned to the Role)

—> RoleAndSubordinates (User is assigned to the Role or a parent role or a child role)
Usage; Sharing rule grants access to Role and Subordinates
Membership; Direct (Users assigned to the Role or Subordinate Roles), Indirect (other)

—> RoleAndInternalSubordinates (as above but excludes portal roles)

To identify the Users who inherit access from a given User search groups where the User is a Direct Member and return the distinct set of Indirect Members.

UserId	GroupId	Group (System Roles)	Membership Type
005…A	00G…M	England Support Role	Direct
005…A	00G…N	England Support R&S	Direct
005…B	00G…N	England Support R&S	Direct
005…C	00G…N	England Support R&S	Direct
005…A	00G…N	Northern Support Role	Indirect
005…B	00G…N	Northern Support Role	Direct
005…A	00G…N	Northern Support R&S	Indirect
005…B	00G…N	Northern Support R&S	Direct
005…A	00G…N	Southern Support Role	Indirect
005…C	00G…N	Southern Support Role	Direct
005…A	00G…N	Southern Support R&S	Indirect
005…C	00G…N	Southern Support R&S	Direct



Record Access Types

#1 - Profile & Permissions Sets
Object-level and Field-level permissions.
Modify All and View All permissions (Profile) override the Sharing model for an Object.

#2 - Org Wide Defaults
OWD set the sharing baseline for an Object for Internal and External Users; Private, Public Read-only, Public Read/Write.
OWD is the only restrictive access feature.

#3 - Record Ownership [RowCause=Owner]
Record Ownership assigns Full permissions and drives Inherited Sharing and Ownership based sharing rules.

#4 - Implicit Sharing [RowCause=ImplictParent/Child]
ImplicitChild; Users can view a parent Account if they have access to child Opportunity, Case, or Contact.
ImplicitParent; If Users have access to a parent Account, they can view its child Opportunity, Case, and Contact records.

#5 - Manager Groups (Inherited Grant)
When enabled (Setup > Sharing Settings > Other Settings > Manager Groups) for every User 2 System defined groups are created [Manager] and [Manager and Subordinates].

When creating Sharing Rules or Manual Shares the [Manager] or [Manager and Subordinates] groups are selected for a specific User.

#6 - Role Hierarchy (Inherited Grant)
The Role Hierarchy reflects the organisation structure when viewed from the perspective of record visibility. Parent Role members inherit access to records owned by Users at lower levels in the hierarchy.

For every Role System defined groups are created [Role] and [Role and Internal Subordinates].

When creating Sharing Rules the [Role and Subordinates] system defined group can be selected for "owned by" and "shared with".

Roles have Opportunity Access and Case Access settings;
Cannot access Record where Account not owned,
View all Records where Account is owned or
Edit all Records where Account is owned.

The Role Hierarchy is a fundamental sharing concept which should be designed for efficient ownership based sharing and thereby reduce the need for configured exceptions (i.e. rules).

#7 - Queue Membership
Queues support record ownership for Case, Lead and Custom Object records. Queues support routing and assignment use cases. Queue Members can be Users, Public Groups, Roles, Roles and Subordinates. Queue Members can take ownership of a record owned by a Queue.

System Groups allow Queues to be handled as Groups.

#8 - Teams [RowCause=Team]
Teams are groups of users that collaborate on an Account, Opportunity or Case and require access.

Account, Opportunity, Case Teams created by record owner. 1 team per record. Owner, User higher in the role hierarchy and admins can manage membership. 2 records are created; AccountTeam and AccountShare for each team member added.

Team members access level; Read Only, Read Write.
Team member roles; custom list.

Account >
User, Account (RW),Opp+Case Access(P,RO,RW),Team Role
Default Account Teams (Add Default Team Button)

Case > Team Role defines access level.
Predefined Teams.

Opportunity > Opportunity Teams are 1st class objects
Default Account Teams

#9 - Manual Sharing [RowCause=Manual]
Access via the Sharing button on Record pages.
Select [Public Groups], Users, [Manager Groups] and specify an Access level RO/RW.

The Sharing page displays the current access for the record based on the Object Sharing Table records.

Manual sharing is removed when the record owner changes.

#10 - Sharing Rules

Sharing rules provide flexible sharing exceptions which satisfy access requirements outside of the ownership and implicit sharing model. Sharing rules enable sharing based on Ownership conditions or static criteria based conditions (Field=X, Field=Y etc.).

A high number of Sharing Rules can indicate that the OWD setting is incorrect or that Role Hierarchy design is suboptimal, and can also impact on record save performance.

#11 - Territory Hierarchy

Territory management is an account sharing system that grants access to accounts based on the characteristics of the accounts i.e. the Sales Territory. The Territory Hierarchy is comprised of nodes with Account, Case and Opportunity access levels, account assignment rules, assigned users and manually assigned accounts.

Account has Assigned Territories related list.
Opportunity has Territory field.

Key Concepts (TM2.0) :
Territory Model - A complete territory management system with state; Planning, Cloning, Active, Archived state. 2 allowed, 1 active.
Territory Type - Key characteristics and priority.

For every Territory System defined groups are created [Territory] and [Territory and Subordinates]. The System groups can be used in Manual Sharing and Sharing Rules.

#12 - Programmatic Sharing

Apex Sharing :
Apex code can insert to Object Sharing Tables; Access Level:Edit,Read,All. Manual Row Cause for standard objects and Custom row for custom objects. Manual (default) records can be managed in the UI.

Apex Managed Sharing :
Maintained across record owner changes.
Setup requires Modify All permission.
Must use an Apex Sharing Reason.
`Schema.CustomObject__Share.rowCause.SharingReason__c`

Recalculation;
BatchApex class set under Custom Object>Apex Sharing Recalculation. Recalculate button for manual invocation otherwise class executes automatically when OWD change.

With Sharing :
Apex Code runs With Sharing to respect the sharing model. Without sharing is the default.

Inner classes don't inherit sharing setting from Container.
Classes inherit from parent when extends or implements.

Sharing - UserRecordAccess :
Can be used to check permissions via FK or object query.
UserRecordAccess.HasReadAccess,
UserRecordAccess.HasTransferAccess,
UserRecordAccess.MaxAccessLevel

Apex Describes :
Object and field describes are used to test the current users object access and field level security permissions.

Other :
(i) Execute Anonymous always runs in full User Context.
(ii) Test.runAs() allows test code to run execute for specific Users to test record access and object access permissions.

Legend
Declarative Sharing
Performance and Scalability
Programmatic Sharing