Access grants tables

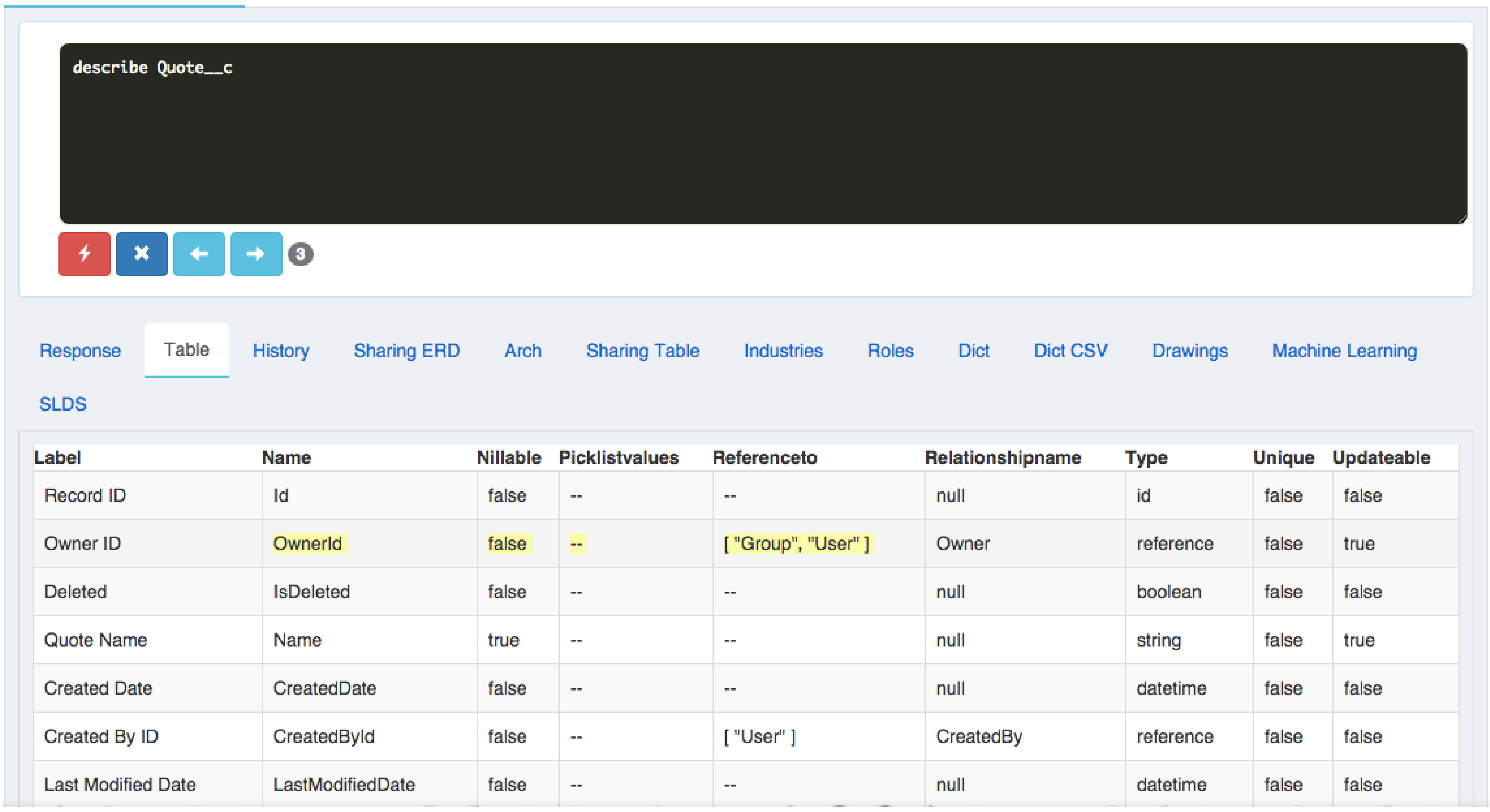
- Object Record Tables: Example: **Quote__c**
  - Store records of the object
  - Has record ownership field: **OwnerId** referencing to [**"Group", "User"**]
  - OwnerId is base field on which Platform's sharing is built-on

- Object Sharing Tables: Example: **Quote__Share**
  - Store data that supports:
    - **explicit** grants
    - **implicit** grants
  - Each Object (thus Object Record Table) has its own Object Sharing table *(unless the object is a **detail** in a master-detail relationship)*
  - In master-detail relationships, the Object Sharing table for the **master** object **controls**access to the **detail** object - since the detail objects do not have **OwnerId** field.

- Group Maintenance Tables
  - store the data supporting:
    - group membership
    - inherited access grants

Table	Function
Object Sharing Tables	Store access grants to individuals and groups. Each of rows (called sharing rows) grants a user or group access to a particular record
Group Maintenance Tables	Store the list of users or groups that belong to each group, indicating **group membership**. Single group membership or inherited access grant can give **several users and groups** multiple ways to access a record. Also includes including system-defined group. System-defined groups are groups of users that Salesforce creates and manages internally to support various features and behaviors, such as queues and hierarchies. For every node in role hierarchy, 2 types of system-defined groups is used : Role groups and RoleAndSubordinates groups

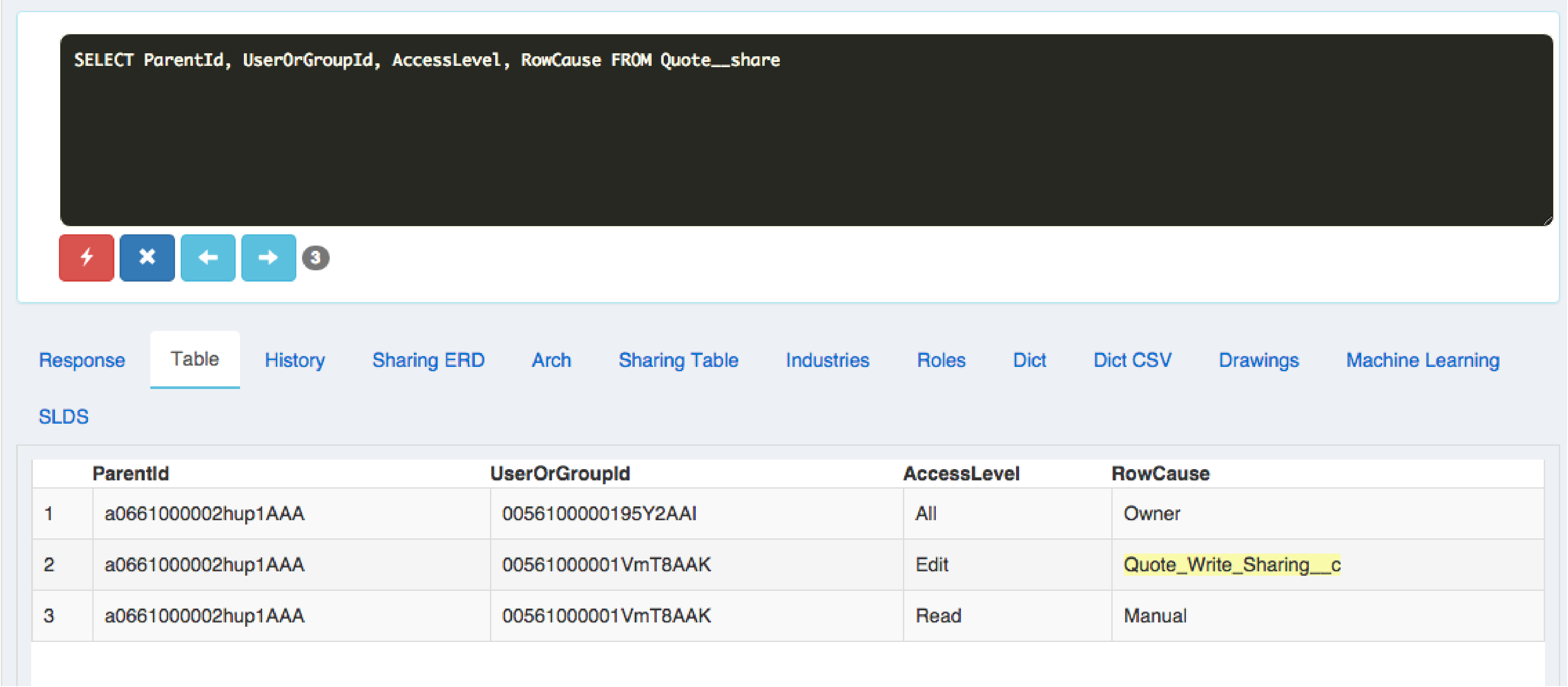
Object Record Table: **Quote__c**:



```
describe Quote__c
```

Label	Name	Nillable	Picklistvalues	Referenceto	Relationshipname	Type	Unique	Updateable
Record ID	Id	false	--	--	null	id	false	false
Owner ID	OwnerId	false	--	["Group", "User"]	Owner	reference	false	true
Deleted	IsDeleted	false	--	--	null	boolean	false	false
Quote Name	Name	true	--	--	null	string	false	true
Created Date	CreatedDate	false	--	--	null	datetime	false	false
Created By ID	CreatedById	false	--	["User"]	CreatedBy	reference	false	false
Last Modified Date	LastModifiedDate	false	--	--	null	datetime	false	false

Object Sharing Table: **Quote__sharing**:



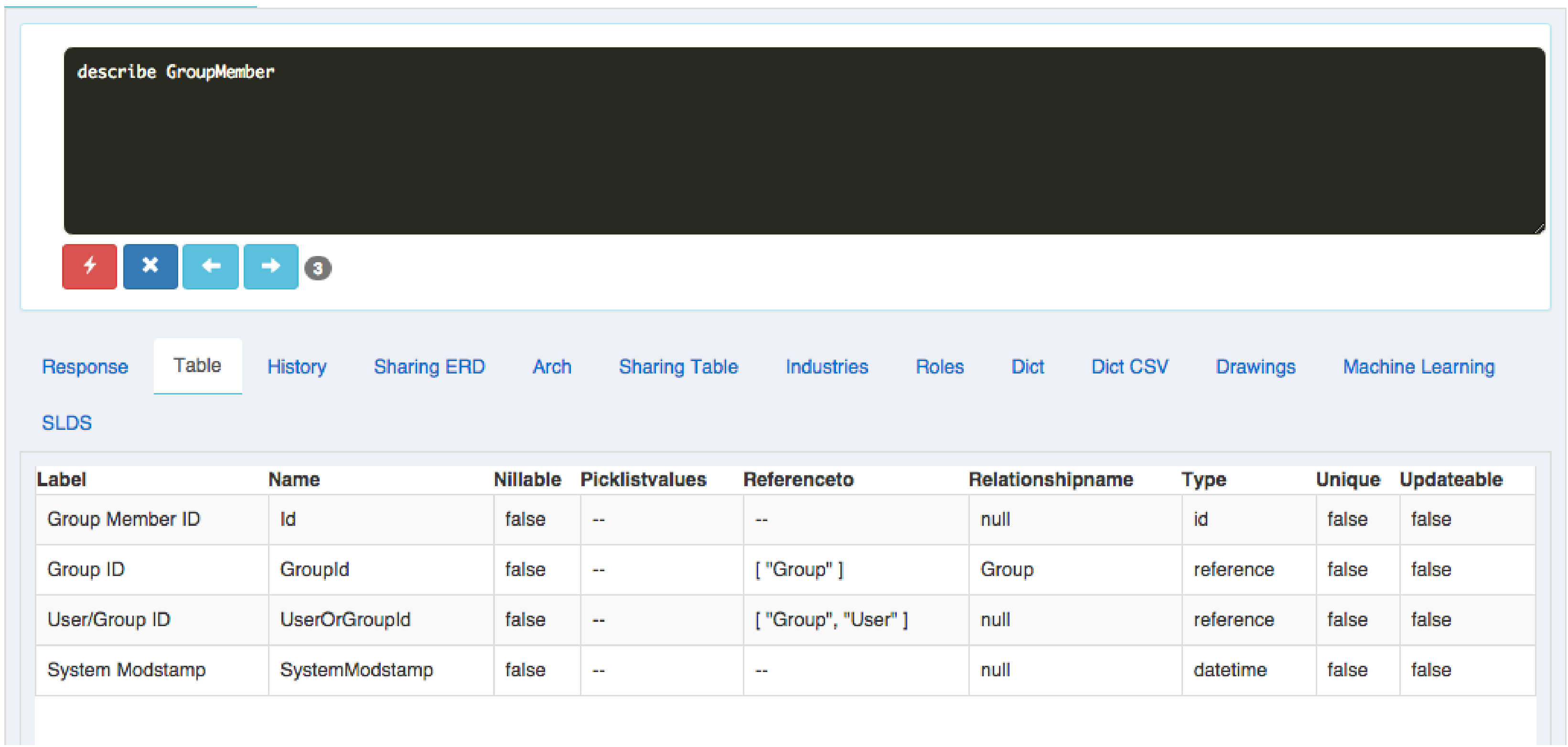
```
SELECT ParentId, UserOrGroupId, AccessLevel, RowCause FROM Quote__share
```

	ParentId	UserOrGroupId	AccessLevel	RowCause
1	a0661000002hup1AAA	0056100000195Y2AAI	All	Owner
2	a0661000002hup1AAA	00561000001VmT8AAK	Edit	Quote_Write_Sharing__c
3	a0661000002hup1AAA	00561000001VmT8AAK	Read	Manual

Group Maintenance Tables: **Group** and **GroupMember**:

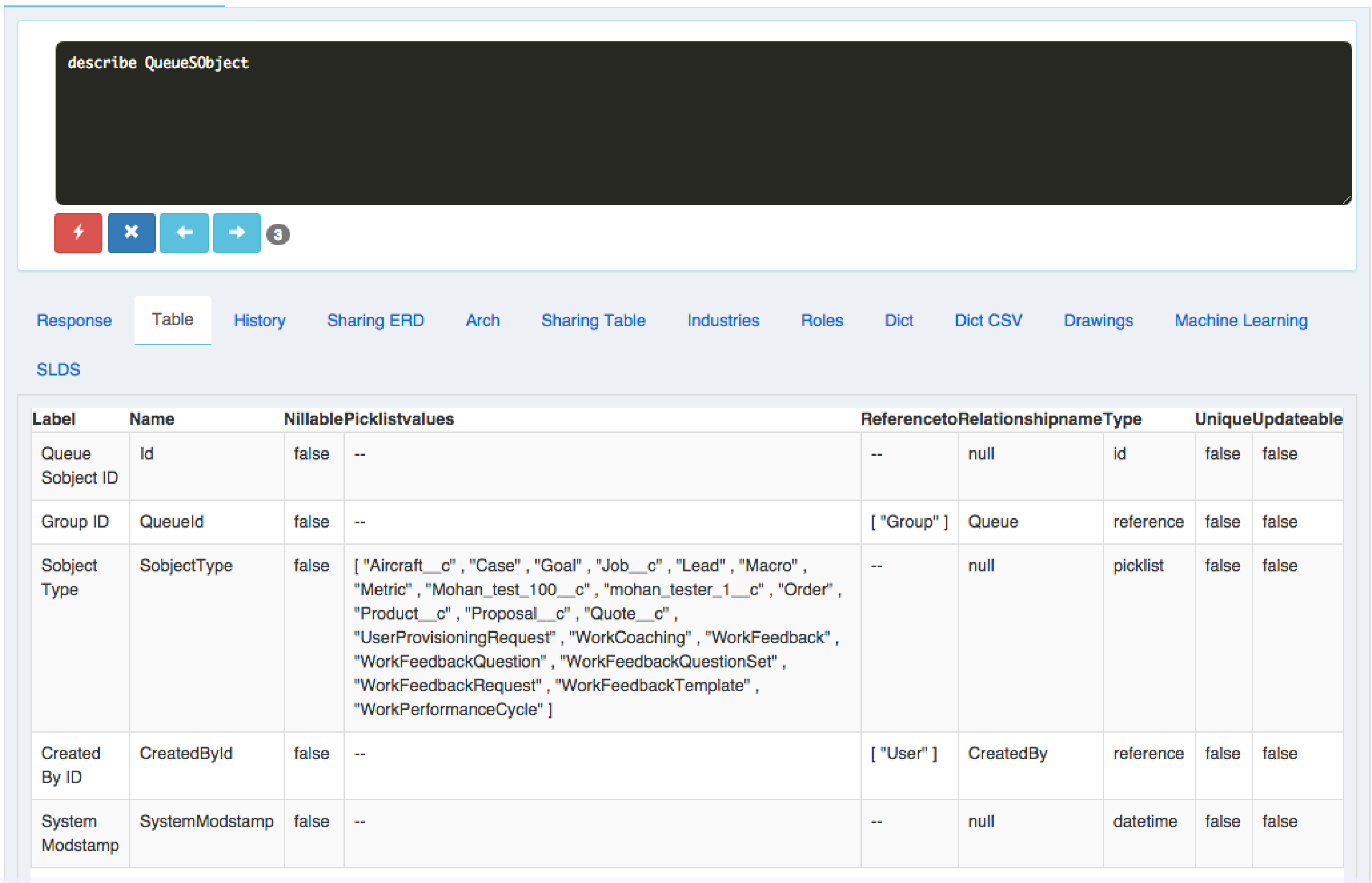
Describe Group:

Label	Name	Nillable	Picklistvalues	Referenceto	Relationshipname	Type	Unique	Updateable
Group ID	Id	FALSE	--	--	null	id	FALSE	FALSE
Name	Name	FALSE	--	--	null	string	FALSE	TRUE
Developer Name	DeveloperName	TRUE	--	--	null	string	FALSE	TRUE
Related ID	RelatedId	TRUE	--	["User", "UserRole"]	null	reference	FALSE	FALSE
Type	Type	FALSE	["AllCustomerPortal" , "CollaborationGroup" , "Manager" , "ManagerAndSubordinatesInternal" , "Organization" , "PRMOrganization" , "Queue" , "Regular" , "Role" , "RoleAndSubordinates" , "RoleAndSubordinatesInternal" , "SharingRuleGroup" , "Territory" , "TerritoryAndSubordinates"]	--	null	picklist	FALSE	FALSE
Email	Email	TRUE	--	--	null	email	FALSE	TRUE
Owner ID	OwnerId	FALSE	--	["Organization", "User"]	Owner	reference	FALSE	FALSE
Send Email to Members	DoesSendEmailToMembers	FALSE	--	--	null	boolean	FALSE	TRUE
Include Bosses	DoesIncludeBosses	FALSE	--	--	null	boolean	FALSE	TRUE



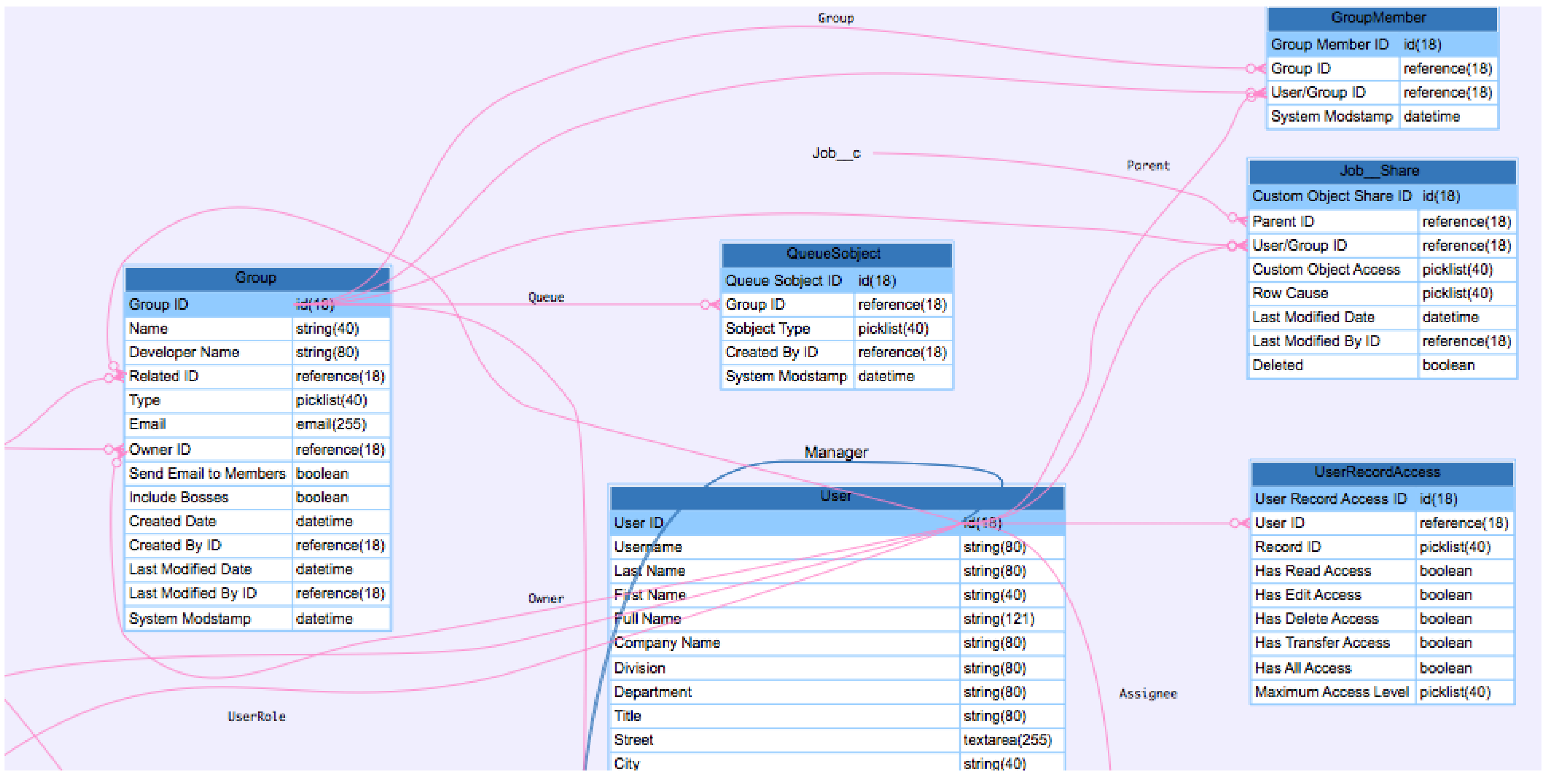
```
describe GroupMember
```

Label	Name	Nillable	Picklistvalues	Referenceto	Relationshipname	Type	Unique	Updateable
Group Member ID	Id	false	--	--	null	id	false	false
Group ID	GroupId	false	--	["Group"]	Group	reference	false	false
User/Group ID	UserOrGroupId	false	--	["Group", "User"]	null	reference	false	false
System Modstamp	SystemModstamp	false	--	--	null	datetime	false	false



```
describe QueueSObject
```

Label	Name	Nillable	Picklistvalues	Referenceto	Relationshipname	Type	Unique	Updateable
Queue Sobject ID	Id	false	--	--	null	id	false	false
Group ID	QueueId	false	--	["Group"]	Queue	reference	false	false
Sobject Type	SobjectType	false	["Aircraft__c" , "Case" , "Goal" , "Job__c" , "Lead" , "Macro" , "Metric" , "Mohan_test_100__c" , "mohan_tester_1__c" , "Order" , "Product__c" , "Proposal__c" , "Quote__c" , "UserProvisioningRequest" , "WorkCoaching" , "WorkFeedback" , "WorkFeedbackQuestion" , "WorkFeedbackQuestionSet" , "WorkFeedbackRequest" , "WorkFeedbackTemplate" , "WorkPerformanceCycle"]	--	null	picklist	false	false
Created By ID	CreatedById	false	--	["User"]	CreatedBy	reference	false	false
System Modstamp	SystemModstamp	false	--	--	null	datetime	false	false



Group	
Group ID	id(18)
Name	string(40)
Developer Name	string(80)
Related ID	reference(18)
Type	picklist(40)
Email	email(255)
Owner ID	reference(18)
Send Email to Members	boolean
Include Bosses	boolean
Created Date	datetime
Created By ID	reference(18)
Last Modified Date	datetime
Last Modified By ID	reference(18)
System Modstamp	datetime

QueueSobject	
Queue Sobject ID	id(18)
Group ID	reference(18)
Sobject Type	picklist(40)
Created By ID	reference(18)
System Modstamp	datetime

User	
User ID	id(18)
Username	string(80)
Last Name	string(80)
First Name	string(40)
Full Name	string(121)
Company Name	string(80)
Division	string(80)
Department	string(80)
Title	string(80)
Street	textarea(255)
City	string(40)

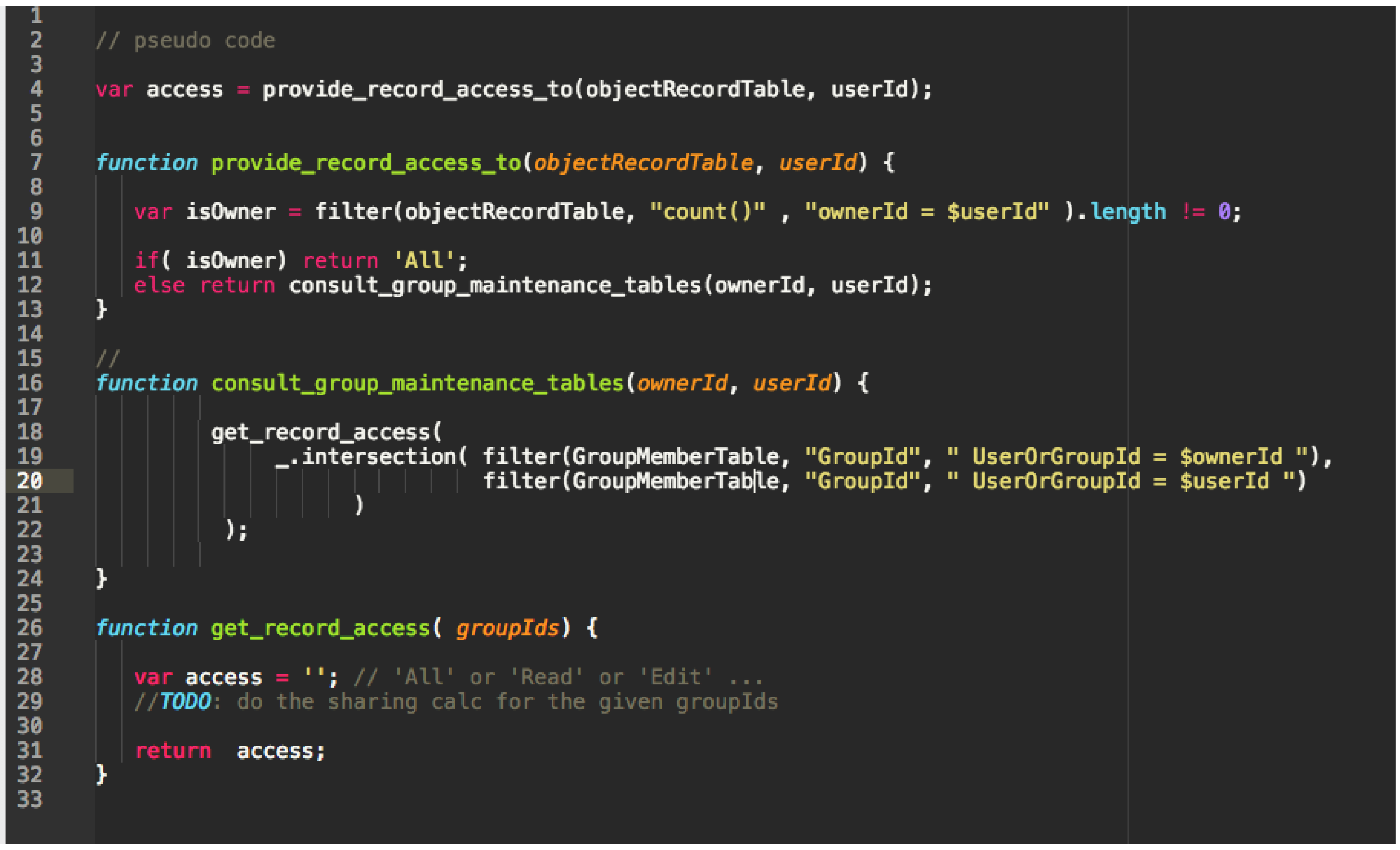
GroupMember	
Group Member ID	id(18)
Group ID	reference(18)
User/Group ID	reference(18)
System Modstamp	datetime

Job__Share	
Custom Object Share ID	id(18)
Parent ID	reference(18)
User/Group ID	reference(18)
Custom Object Access	picklist(40)
Row Cause	picklist(40)
Last Modified Date	datetime
Last Modified By ID	reference(18)
Deleted	boolean

UserRecordAccess	
User Record Access ID	id(18)
User ID	reference(18)
Record ID	picklist(40)
Has Read Access	boolean
Has Edit Access	boolean
Has Delete Access	boolean
Has Transfer Access	boolean
Has All Access	boolean
Maximum Access Level	picklist(40)

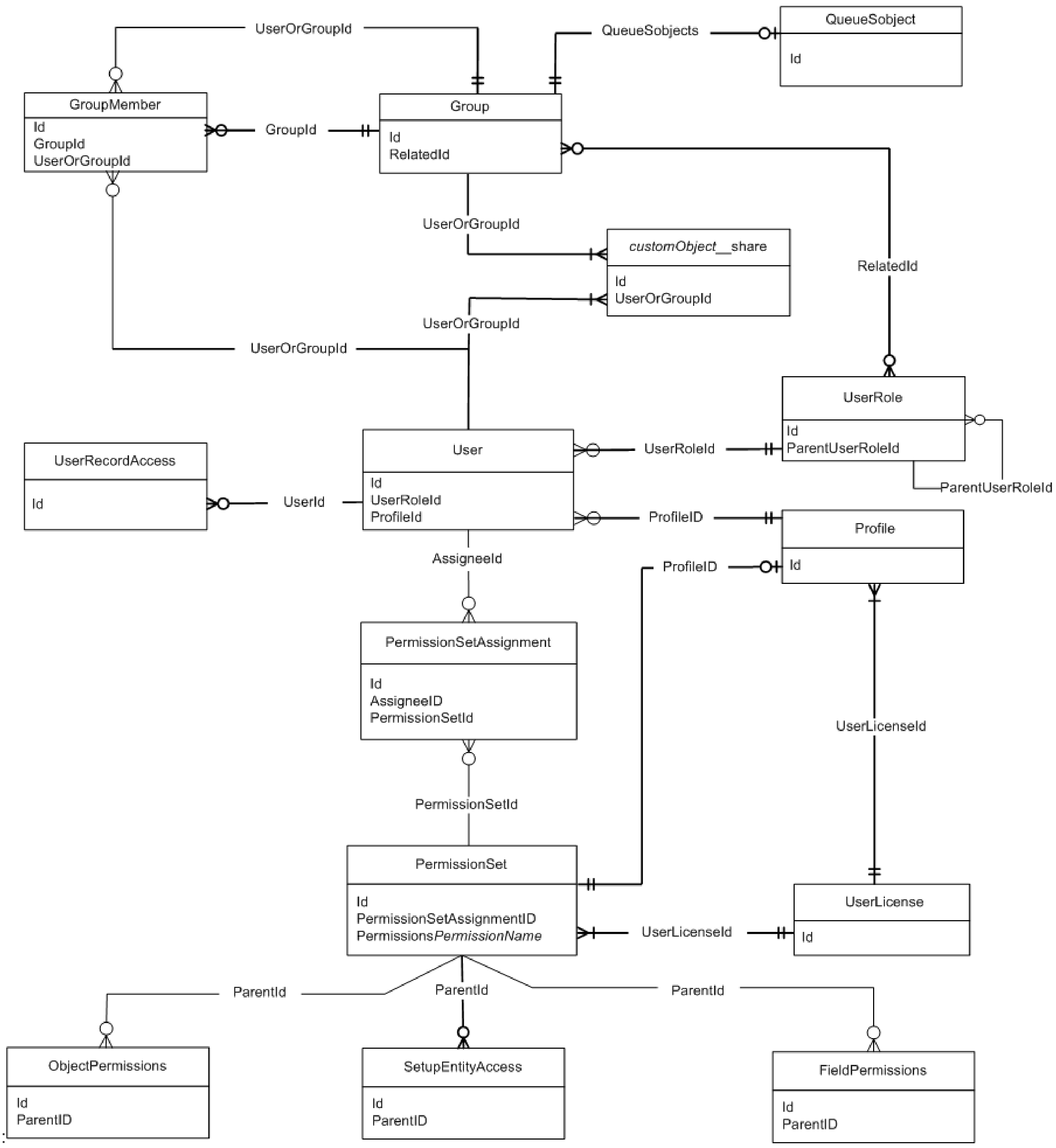
How Salesforce joins entities to providing access to record (RecordId) of ObjectRecordTable:

- Org wide Filter: orgId
- Logged in user: userId
- Get the **OwnerId** of the record (recordId) the user seeking access from ObjectRecordTable (**recordId**, **OwnerId**, ...)

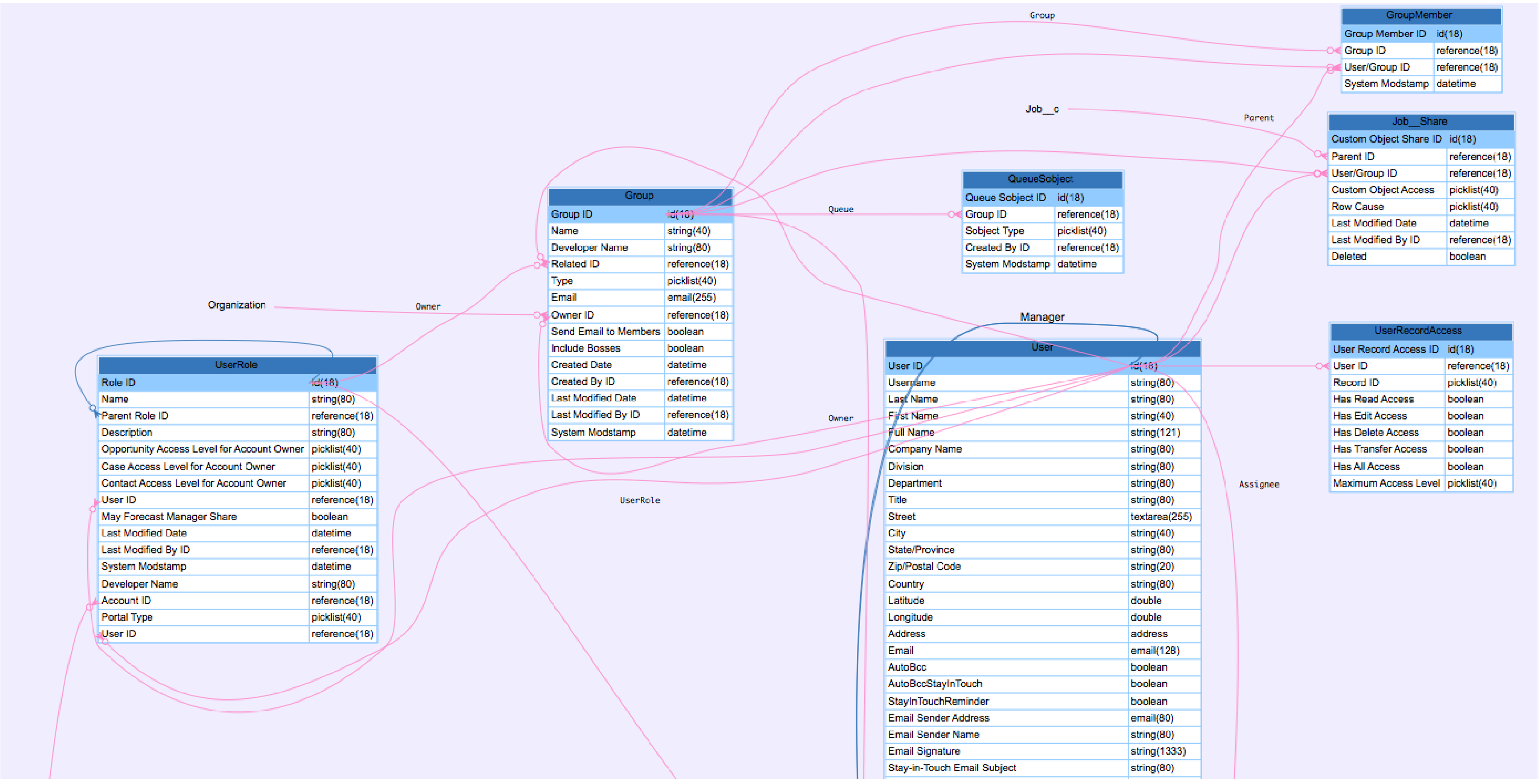


```
// pseudo code

var access = provide_record_access_to(objectRecordTable, userId);


function provide_record_access_to(objectRecordTable, userId) {

    var isOwner = filter(objectRecordTable, "count()" , "ownerId = $userId" ).length != 0;

    if( isOwner) return 'All';
    else return consult_group_maintenance_tables(ownerId, userId);
}

//
function consult_group_maintenance_tables(ownerId, userId) {

            get_record_access(
                  _.intersection( filter(GroupMemberTable, "GroupId", " UserOrGroupId = $ownerId "),
                                  filter(GroupMemberTable, "GroupId", " UserOrGroupId = $userId ")
                  )
              );

}

function get_record_access( groupIds) {

    var access = ''; // 'All' or 'Read' or 'Edit' ...
    //TODO: do the sharing calc for the given groupIds

    return  access;
}

```

- record must exist
- either the Object Sharing Table or the Group Maintenance tables must grant access



ERD:



GroupMember	
Group Member ID	id(18)
Group ID	reference(18)
User/Group ID	reference(18)
System Modstamp	datetime

Job__Share	
Custom Object Share ID	id(18)
Parent ID	reference(18)
User/Group ID	reference(18)
Custom Object Access	picklist(40)
Row Cause	picklist(40)
Last Modified Date	datetime
Last Modified By ID	reference(18)
Deleted	boolean

QueueSobject	
Queue Sobject ID	id(18)
Group ID	reference(18)
Sobject Type	picklist(40)
Created By ID	reference(18)
System Modstamp	datetime

Group	
Group ID	id(18)
Name	string(40)
Developer Name	string(80)
Related ID	reference(18)
Type	picklist(40)
Email	email(255)
Owner ID	reference(18)
Send Email to Members	boolean
Include Bosses	boolean
Created Date	datetime
Created By ID	reference(18)
Last Modified Date	datetime
Last Modified By ID	reference(18)
System Modstamp	datetime

UserRecordAccess	
User Record Access ID	id(18)
User ID	reference(18)
Record ID	picklist(40)
Has Read Access	boolean
Has Edit Access	boolean
Has Delete Access	boolean
Has Transfer Access	boolean
Has All Access	boolean
Maximum Access Level	picklist(40)

UserRole	
Role ID	id(18)
Name	string(80)
Parent Role ID	reference(18)
Description	string(80)
Opportunity Access Level for Account Owner	picklist(40)
Case Access Level for Account Owner	picklist(40)
Contact Access Level for Account Owner	picklist(40)
User ID	reference(18)
May Forecast Manager Share	boolean
Last Modified Date	datetime
Last Modified By ID	reference(18)
System Modstamp	datetime
Developer Name	string(80)
Account ID	reference(18)
Portal Type	picklist(40)
User ID	reference(18)

User	
User ID	id(18)
Username	string(80)
Last Name	string(80)
First Name	string(40)
Full Name	string(121)
Company Name	string(80)
Division	string(80)
Department	string(80)
Title	string(80)
Street	textarea(255)
City	string(40)
State/Province	string(80)
Zip/Postal Code	string(20)
Country	string(80)
Latitude	double
Longitude	double
Address	address
Email	email(128)
AutoBcc	boolean
AutoBccStayInTouch	boolean
StayInTouchReminder	boolean
Email Sender Address	email(80)
Email Sender Name	string(80)
Email Signature	string(1333)
Stay-in-Touch Email Subject	string(80)