ACCESS CONTROL LISTS

& MANAGING SECURITY

OVERVIEW

- Access Control List (ACL's)
- Types of ACL
- Components of ACL
- Deny Unless/Allow If

ACCESS CONTROL LISTS

- Access Control is a security rule defined to restrict the permissions of a user from viewing and interacting with data
  - Our access control rules are executed whenever a user attempts to access any ServiceNow table
- Access control can be set at the row-level (record) and/or column-level (field)
- Access control rules restrict CRUD operations (create, read, update(write), delete)
- Access control lists (ACL) contain our instance's access control rules [sys_security_acl]
  - Requires the security_admin role to maintain ACLs
- To view access controls associated with a particular table, we can select the access control tab on the dictionary entry OR type <table name>.CONFIG

COMPONENTS OF ACL

- Each access control rule specifies 3 things:
  - A valid operation – a valid action the system can take (CRUD)
  - The object being secured (table, table AND field...)
  - The permissions required to access the object – roles, conditional expressions, scripts

ACL RULE TYPES

- Table.-none-
- No specific field is selected meaning this rule applies to the whole table and ALL its records
- EX: incident.-none- means that every record in the incident table will get this ACL configuration

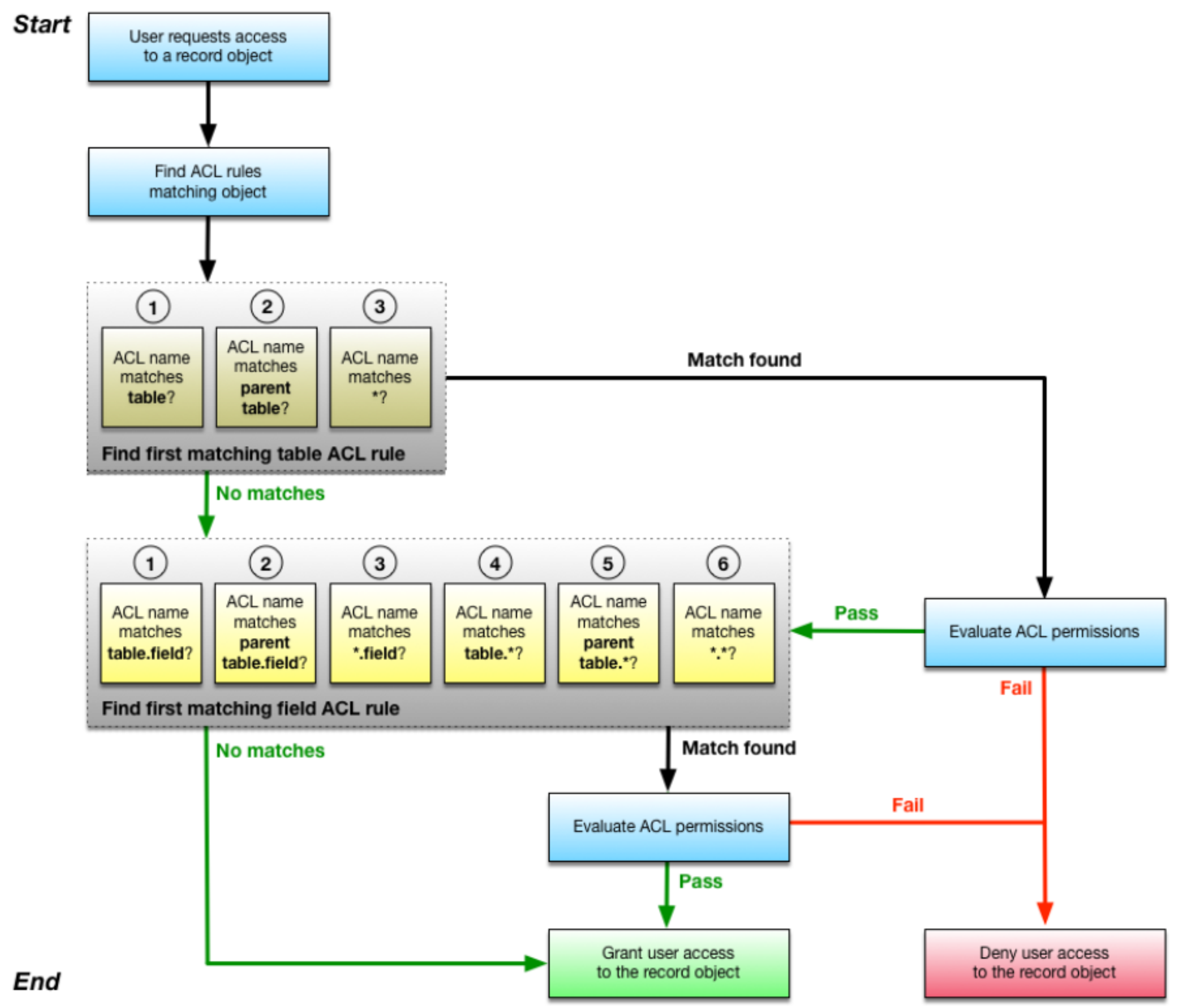
- Table.Field
- This rule only applies to ONE FIELD on a record
- EX: incident.caller means that the restrictions will apply only to the caller field on the incident table

- Table.*
- Wildcard – this rule applies to EVERY FIELD on a record that DOES NOT HAVE a table.field rule
- EX: incident.* means that the restrictions will apply to all fields EXCEPT the caller field(see left)

DENY UNLESS/ ALLOW IF

- We have 2 different decision types that we can apply to our ACLs
- Deny Unless: these rules focus on denying access specific conditions are met
  - These rules are more restrictive and have to be satisfied before any Allow rules are considered
  - Deny access unless you have the key to the house (table/field)
- Allow If: these rules specify who is allowed to access under certain conditions
  - If ANY of these conditions are met, a user is granted access
  - Allow if the bedroom you are trying to access is yours or you are the owner of the house
- The system first evaluates Deny rules before evaluating Allow rules
  - If a deny rule should block a user's access, access is immediately denied and allow rules are NOT run
  - Allow rules are only run if there are no Deny rules that apply

ACL EVALUATION


Start
User requests access to a record object
Find ACL rules matching object
1 ACL name matches table?
2 ACL name matches parent table?
3 ACL name matches *?
Find first matching table ACL rule
Match found
No matches
1 ACL name matches table.field?
2 ACL name matches parent table.field?
3 ACL name matches *.field?
4 ACL name matches table.*?
5 ACL name matches parent table.*?
6 ACL name matches *.*?
Find first matching field ACL rule
Pass
Evaluate ACL permissions
Fail
No matches
Match found
Evaluate ACL permissions
Fail
Pass
Grant user access to the record object
Deny user access to the record object
End

EXAMPLE 1

- Table: u_owner
- ACL 1: u_owner.none
  - Read
  - Condition: current.userID == gs.getUserID()
- ACL 2: u_owner.*
  - Read
  - Condition: Role = requestor

- If the user trying to access the table has the requestor role to view a record that is not theirs, will they be able to read it?

EXAMPLE 1

- Table: u_owner
- ACL 1: u_owner.none
  - Read
  - Condition: current.userID == gs.getUserID()
- ACL 2: u_owner.*
  - Read
  - Condition: Role = requestor

- If the user trying to access the table has the requestor role to view a record that is not theirs, will they be able to read it?
- No – because u_owner.none blocks record-level read access, even though u_owner.* grants access via role
  - Record access fails

EXAMPLE 2

- Table: incident
- ACL 1: incident.none
  - Read
  - Condition: role = requestor
- ACL 2: incident.*
  - Read
  - Condition: role = requestor

- If a user with the requestor role attempts to access an incident record, will they have access? What fields?
- If a user without the requestor role attempts to access an incident record, will they have access? What fields?

EXAMPLE 2

- Table: incident
- ACL 1: incident.none
  - Read
  - Condition: role = requestor
- ACL 2: incident.*
  - Read
  - Condition: role = requestor

- If a user with the requestor role attempts to access an incident record, will they have access? What fields?
  - Yes – they will have access to the table via incident.none
  - They will see all fields via incident.* AND the absence of any incident.FIELD ACLs
- If a user without the requestor role attempts to access an incident record, will they have access? What fields?
  - No – they will not have access to the entire table and the 2nd ACL will not be evaluated

EXAMPLE 3

- Table: incident
- ACL 1: incident.none
  - Read
  - Condition: role = requestor
- ACL 2: incident.*
  - Read
  - Condition: role = requestor
- ACL 3: incident.urgency
  - Read
  - Condition: current.created_by == gs.getUserID()

- If a user with the requestor role attempts to access an incident record, will they have access? What fields?

EXAMPLE 3

- Table: incident
- ACL 1: incident.none
  - Read
  - Condition: role = requestor
- ACL 2: incident.*
  - Read
  - Condition: role = requestor
- ACL 3: incident.urgency
  - Read
  - Condition: current.created_by == gs.getUserID()

- If a user with the requestor role attempts to access an incident record, will they have access? What fields?
  - Yes – they will have access to the table via incident.none
  - All fields will be available on records that were created by the user
  - All fields EXCEPT urgency will be available on records that were created by other users

DEMO

- Let's create an access control rule!

TERMINOLOGY

- Access Control - a security rule defined to restrict the permissions of a user from viewing and interacting with data
- ACL – Access Control List that contains our Access Control rules
- Deny Unless - rules that focus on denying access specific conditions are met
- Allow If - rules that specify who is allowed to access under certain conditions