knowledge16

Experience the Service Revolution



Security: Access Control Rules

Securing Your Instance

ARNEZ NISPEROS
ADVISORY SOLUTION CONSULTANT
ServiceNow

JASON LEWKO
SOLUTION CONSULTANT
ServiceNow

© 2016 ServiceNow All Rights Reserved

servicenow

Agenda

Introductions

Access Control Rules: What Are They, and How Do They Work?

Access Control Rule Labs

Debugging

Encryption

© 2016 ServiceNow All Rights Reserved

Introductions

Your Presenters



Arnez Nisperos

Advisory Solution Consultant



Jason Lewko

Solution Consultant

© 2016 ServiceNow All Rights Reserved

Securing Data in ServiceNow

- Module Visibility
- UI Policies
- Client Scripts
- Lists and Form Views
- Catalog White Lists and Black Lists
- Access Control Rules

© 2016 ServiceNow All Rights Reserved

Securing Data in ServiceNow

Which Should I Use?

- Why are you securing the data?
  - Cosmetic or efficiency; guiding page workflow or streamlining the user interface
    - UI Policies, List and Form views
    - More complex needs? Client Scripts
  - Want to control or validate data for integrations? Data Policies
  - Really need security? Have regulatory requirements? ACLs are what you want.
- Not sure? Ask!
  - Your account team's technical resource
  - Professional Services or your implementation partner
  - The community!

© 2016 ServiceNow All Rights Reserved

Access Control Rules

What Are They? How Do They Work?

© 2016 ServiceNow All Rights Reserved

What Are Access Control Rules?

- Allow a specific operation for a specific object
  - Each ACL specifies and is named for the object(s) being secured
  - Naming allows * wildcards
- Define the criteria (permissions) necessary
- Presence of rules defines securing
  - If no rule is present, access is granted
  - If any rule is present, you must pass a rule to gain access
  - High Security plugin creates default access rules for every table

© 2016 ServiceNow All Rights Reserved

What Do Access Control Rules Apply To?

- Records
  - The focus of our labs today
- UI Pages
- Processors
- Client Callable Script Includes

© 2016 ServiceNow All Rights Reserved

What Operations Can be Secured?

- Create
- Read
- Update (Write)
- Delete
- Execute
- Edit Task Relations
- Edit CI Relations
- Save as Template
- Add to List
- List Edit
- Report on
- Personalize Choices

© 2016 ServiceNow All Rights Reserved

What’s Already Secured?

Essentially, Everything ServiceNow Provides …

- New instances have 4,500+ Access Control Rules predefined
- Add in all plugins, and it's greater than 6,000
- A primary use-case for new rules is for new tables and applications
  - High Security Plugin default rules supply blanket protection for those

© 2016 ServiceNow All Rights Reserved

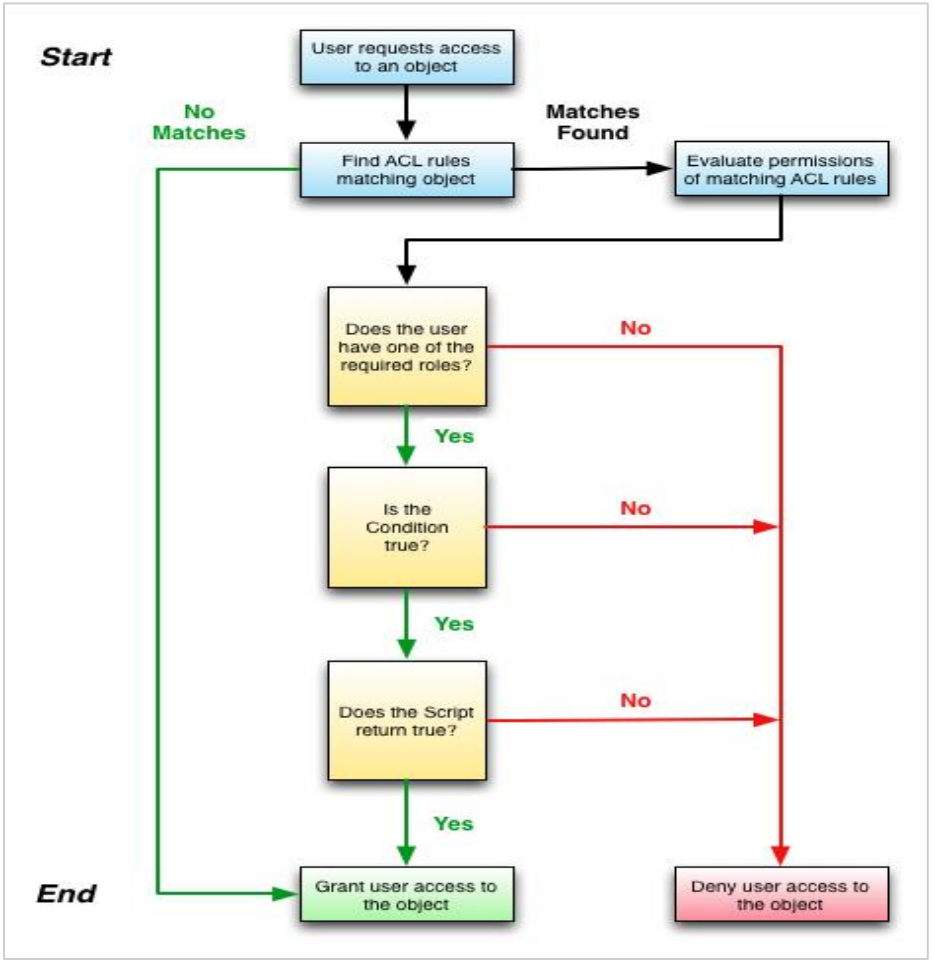
What's Already Secured?

- Many default roles predefined
  - End users (Requesters)
    - Submit records in some applications (Create)
    - Read and update their own records in those applications
  - Fulfillers
    - General read and write access for applications they have a role for
    - Task assignment
  - Application/Process administrators
    - Delete records
    - Change state to closed

© 2016 ServiceNow All Rights Reserved

How Are Access Control Rules Evaluated?

- User requests access
- Find rules that match
  - If no match, grant access
  - If match, evaluate permissions
- If the permissions evaluate to true, grant access
- If the permissions evaluate to false, deny access



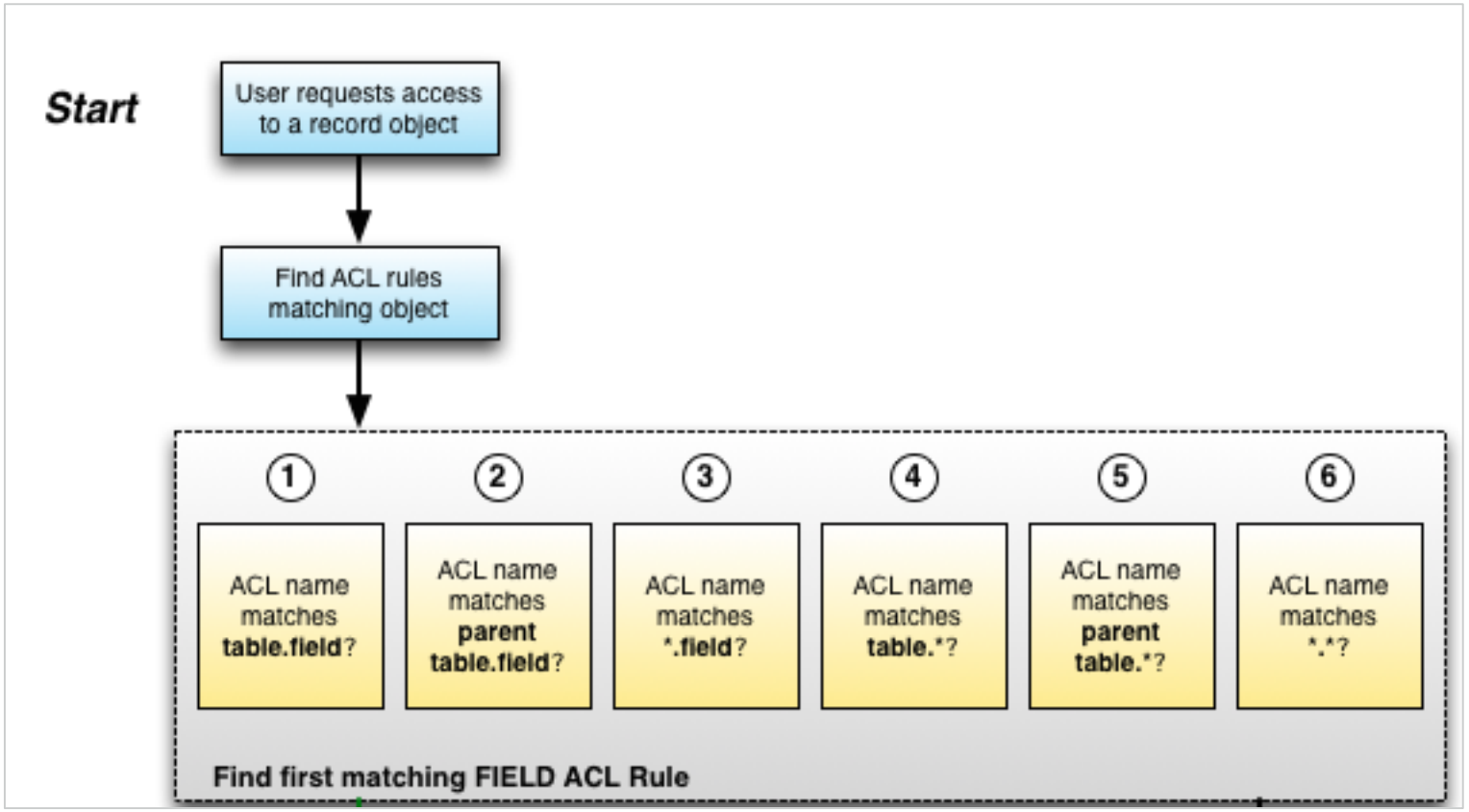
© 2016 ServiceNow All Rights Reserved

How Are Rules Matched?

- Searches are from most specific to least specific
  - Processing orders define the matching criteria
- For record rules, a table and field rule will be searched for
  - Both are evaluated
- First rule to match for both is evaluated

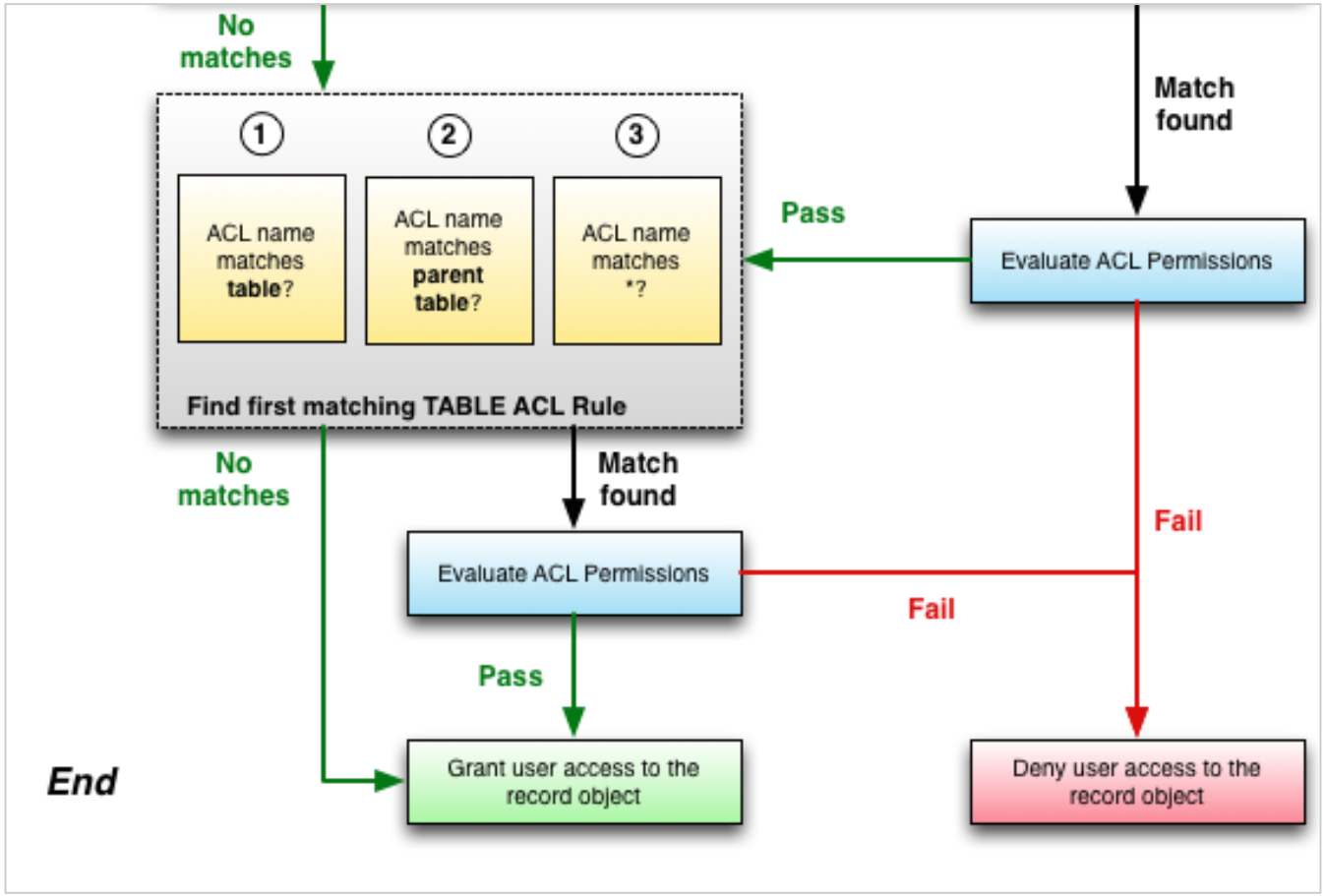
© 2016 ServiceNow All Rights Reserved

The Processing Orders



© 2016 ServiceNow All Rights Reserved

The Processing Orders



© 2016 ServiceNow All Rights Reserved

Evaluation of the Matched Rules

- A user must pass both field and table ACL rules in order to access a record object
- If a match is found, and the user fails both, then the operation will be denied
- If a user fails a field ACL rule but passes a table ACL rule, the user is denied access to the field described by the field ACL rule
- If a user fails a table ACL rule, the user is denied access to all fields in the table even if the user previously passed a field ACL rule
- If there are multiple rules at the same processing level, any passed rule will allow access

© 2016 ServiceNow All Rights Reserved

How Are Permissions Evaluated?

- Three types of evaluation
  - A condition selector
  - A script field
  - A Requires role related list
- All three must evaluate to true
  - Empty sets are true
    - If all three are empty, that's a free access pass for that operation!
  - Required Roles OR evaluated
- Admin override

© 2016 ServiceNow All Rights Reserved

Script Evaluation

- Scripts can evaluate Access Control Rule output
- GlideRecord has built in methods for GlideRecord objects
  - canRead()
  - canWrite()
  - canCreate()
  - canDelete()

© 2016 ServiceNow All Rights Reserved

Remedial Class

You're in a Lab About Access Control Rules!

- Roles are applied to users in three ways
  - User has the role directly assigned to them
  - User is member of a group that has the role
  - User or group has a role which contains the role

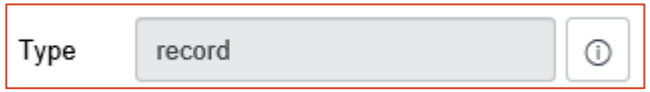
© 2016 ServiceNow All Rights Reserved

Results of Denial

- When a table read rule results in a deny, the user cannot see the record
  - Lists of the table will show security constraint messages



- When a table write rule results in a deny, the fields will all be read-only
  - When there is not a more specific field rule!
- When a table create rule results in a deny, users will not see the New button
- When a field read rule results in a deny, the field will not be visible in forms or lists
- When a field write rule results in a deny, the field will be read-only



© 2016 ServiceNow All Rights Reserved

Elevated Security

Access Control Rules Are Security!

- Security_admin role
  - System Administrator has role by default
  - Having the ‘admin’ role insufficient by itself
- Elevated session
  - Manual action!

© 2016 ServiceNow All Rights Reserved

Lab Environment

- Instance URL will be similar to: https://acr-###.lab.service-now.com
- Please raise your hand if you have difficulties logging into your instance
- Submit feedback via the application in your instance

© 2016 ServiceNow All Rights Reserved

Lab 1

Working with Roles

© 2016 ServiceNow All Rights Reserved

Lab 1

- Create a Role
- Apply Role to a User
- Apply Role to a Group
- Create a Nested Role

© 2016 ServiceNow All Rights Reserved

Lab 2

A Little Pre-work

© 2016 ServiceNow All Rights Reserved

Lab 2

- Create a New Table
- Create Fields
- Create Records
- Required Role for the Module

© 2016 ServiceNow All Rights Reserved

Lab 3

Your First Access Control Rule: Table Rules

© 2016 ServiceNow All Rights Reserved

Lab 3

- Elevate to security_admin
- Create a New Table Access Control Rule
  - Simple, only Required Role to evaluate
- Validate with Another Browser

© 2016 ServiceNow All Rights Reserved

Lab 4

Field Level Access Control Rules

© 2016 ServiceNow All Rights Reserved

Lab 4

- Create new records
- Modify the Table Read Access Control Rule
  - Not as simple anymore!
  - This has value in a later lab!
- Create a Field Read Access Control Rule
- Create a Table Write Rule

© 2016 ServiceNow All Rights Reserved

Lab 5

Cleaning Up the Interface

© 2016 ServiceNow All Rights Reserved

Lab 5

- Create a list_edit Rule
- Remove a Field from the Default List Layout
- Create an add_to_list Rule
- Create a Before Query Business Rule
  - There's scripting here!

© 2016 ServiceNow All Rights Reserved

Lab 6

A Practical Example

© 2016 ServiceNow All Rights Reserved

Lab 6

- A Practical Example
  - Create report_on rules very like the default deny rules
  - Create report_on rules to allow specific access
    - Demonstrates rule inheritance from extended tables

© 2016 ServiceNow All Rights Reserved

Debugging

A Little Help Figuring Out What's Up

© 2016 ServiceNow All Rights Reserved

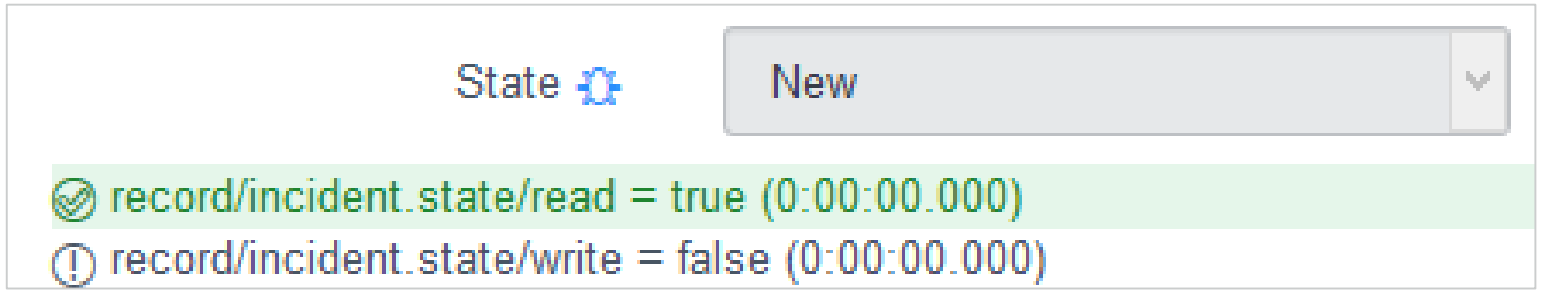
Debugging

- First stop when troubleshooting
  - Is the wiki, of course: https://wiki.servicenow.com/index.php?title=Using_Access_Control_Rules#Troubleshooting
- But also the Debugger
  - Failing to secure something?
  - Failing to see something you thought you allowed?
  - Session specific

© 2016 ServiceNow All Rights Reserved

Debugging

- Field debugging
  - Neat little bug!
- Debug output



11:49:31.549: TIME = 0:00:00.000 PATH = record/incident.opened_at/write CONTEXT = INC0010335 RC = false RULE =
record/incident/write
record/incident/write
record/task.opened_at/write

11:43:34.83: TIME = 0:00:00.000 PATH = record/incident/write CONTEXT = INC0010330 RC = true RULE =
record/incident/write

© 2016 ServiceNow All Rights Reserved

Lab 7

Debugging

© 2016 ServiceNow All Rights Reserved

Lab 7

- Disable the Business Rule
- Enable Security Debugging
- Impersonate Another User

© 2016 ServiceNow All Rights Reserved

Lab 8

Encryption

© 2016 ServiceNow All Rights Reserved

Lab 8

- Enable the Encryption Support Plugin
- Create an Encryption Context
- Add the Context to a Role
- Add an Encrypted Field to the Table

© 2016 ServiceNow All Rights Reserved

Top Takeaways

1. Access control rules provide true security.
2. Access control rules evaluate from specific to general.
3. ServiceNow provides tools to enable security.

© 2016 ServiceNow All Rights Reserved

For more information, please visit the wiki:

https://wiki.servicenow.com/index.php?title=Using_Access_Control_Rules

© 2016 ServiceNow All Rights Reserved

Take the Survey

Please take a moment to complete a session survey in the Knowledge16 app.

Thank You

Arnez Nisperos

Advisory Solution Consultant

ServiceNow

Jason Lewko

Solution Consultant

ServiceNow

© 2016 ServiceNow All Rights Reserved