knowledge14®

April 27–May 1, 2014 • Moscone Center • San Francisco, CA

Access Control Rules: Secure your Instance from the Inside

Joseph Wheeler
Sr. Solutions Consultant
ServiceNow

Erich Dobroth
Sr. Solutions Consultant
ServiceNow

servicenow®

© 2014 ServiceNow All Rights Reserved

Agenda

Introductions

Access Control Rules: What are they, and how do they work?

Access Control Rule Labs

Debugging

Encryption

© 2014 ServiceNow All Rights Reserved

Introductions

Your presenters

© 2014 ServiceNow All Rights Reserved

Securing Data in ServiceNow

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

© 2014 ServiceNow All Rights Reserved

Securing Data in ServiceNow

Which should I use?

- Why are you securing the data?
  - 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!

© 2014 ServiceNow All Rights Reserved

Access Control Rules

What are they? How do they work?

© 2014 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 the rule to gain access
  - High Security plugin creates default access rules for every table

© 2014 ServiceNow All Rights Reserved

What do Access Control Rules Apply to?

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

© 2014 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

© 2014 ServiceNow All Rights Reserved

What's Already Secured?

Essentially, everything ServiceNow provides…

- New instances have 4500+ Access Control Rules predefined
- Add in all plugins, and it's greater than 6K
- A primary use-case for new rules is for new tables and applications
  - High Security plugin default rules supply blanket protection

© 2014 ServiceNow All Rights Reserved

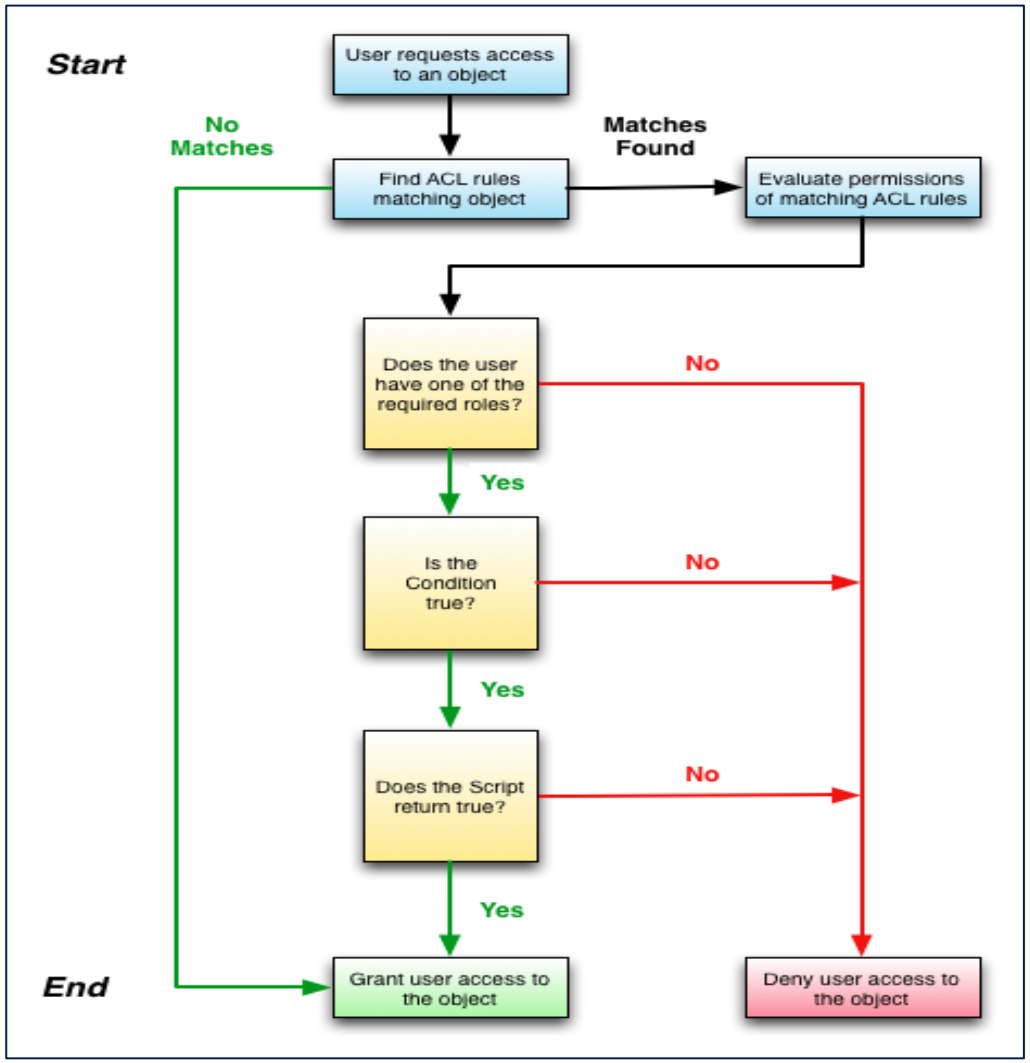
What's Already Secured?

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

© 2014 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 permissions evaluate to false, deny access



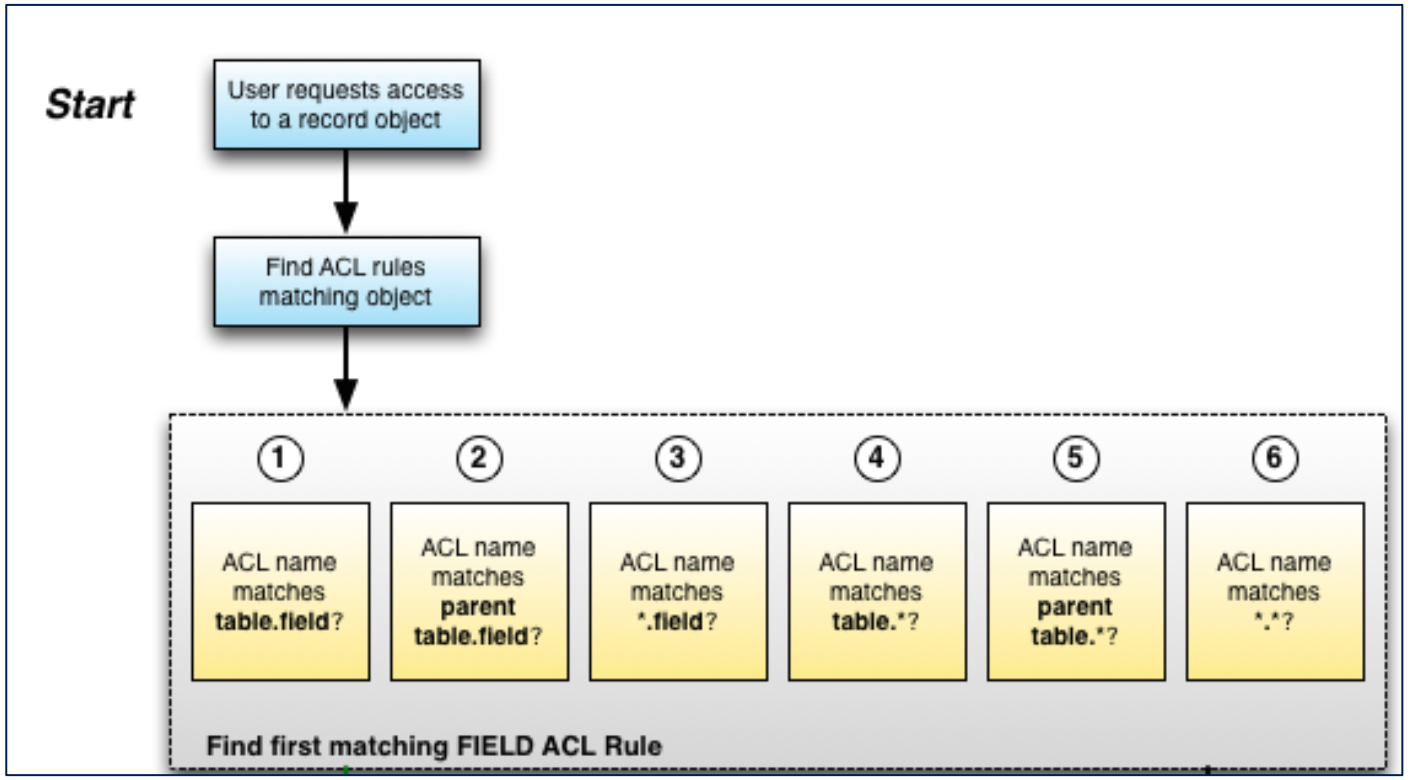
© 2014 ServiceNow All Rights Reserved

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

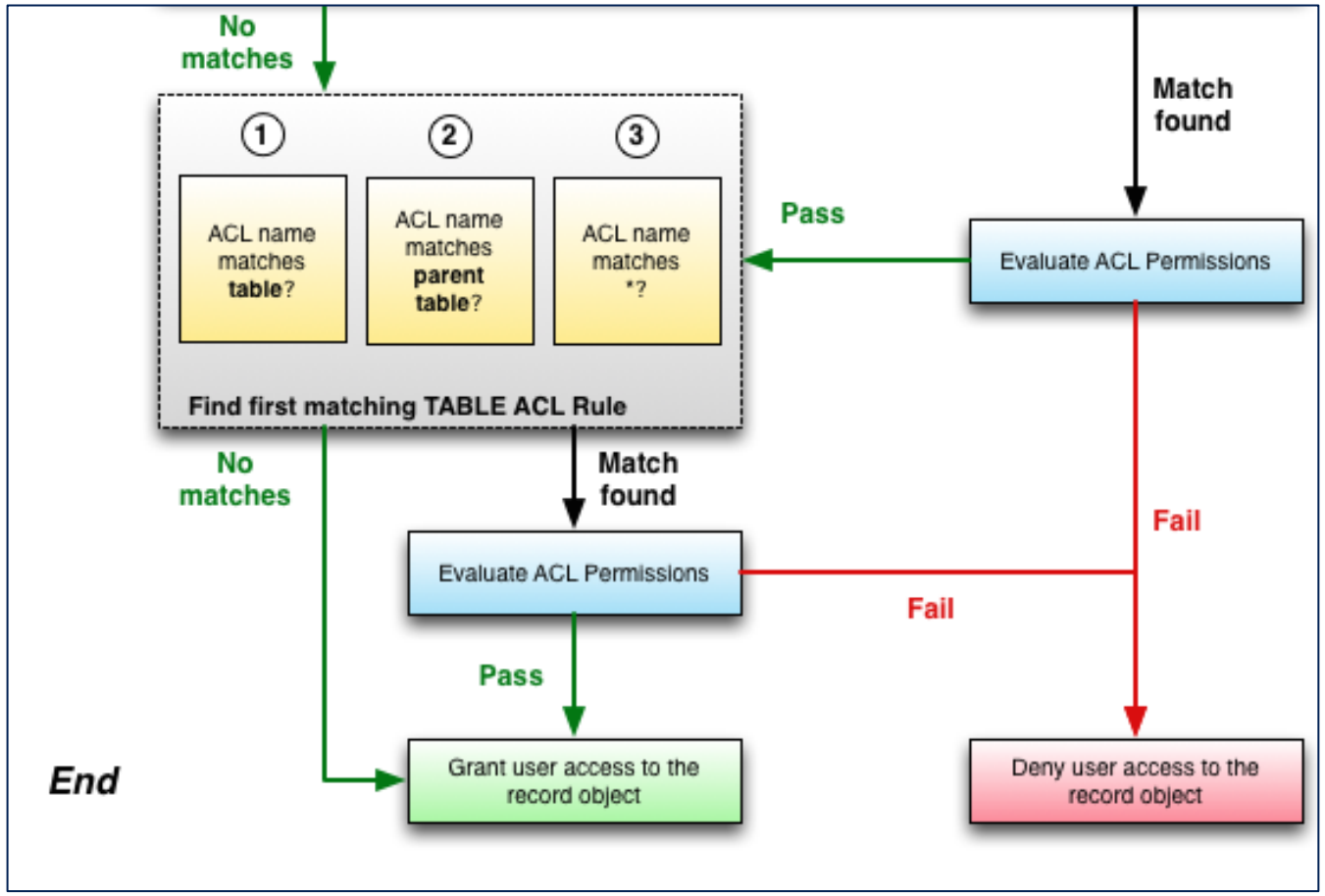
© 2014 ServiceNow All Rights Reserved

The Processing Orders



© 2014 ServiceNow All Rights Reserved

The Processing Orders



© 2014 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.

© 2014 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

© 2014 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()

© 2014 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

© 2014 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.



© 2014 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!

© 2014 ServiceNow All Rights Reserved

Lab Environment

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

© 2014 ServiceNow All Rights Reserved

Lab 1
Working with Roles

© 2014 ServiceNow All Rights Reserved

Lab 1

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

© 2014 ServiceNow All Rights Reserved

Lab 2
A little pre-work

© 2014 ServiceNow All Rights Reserved

Lab 2

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

© 2014 ServiceNow All Rights Reserved

Lab 3

Your first Access Control Rule: Table rules

© 2014 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

© 2014 ServiceNow All Rights Reserved

Lab 4

Field level access control rules

© 2014 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

© 2014 ServiceNow All Rights Reserved

Lab 5
Cleaning up the interface

© 2014 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!

© 2014 ServiceNow All Rights Reserved

Lab 6

Reporting Access Control rules, and a practical example

© 2014 ServiceNow All Rights Reserved

Lab 6

- Create a Report
- Create a report_on Rule
- 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

© 2014 ServiceNow All Rights Reserved

Debugging

A little help figuring out what's up

© 2014 ServiceNow All Rights Reserved

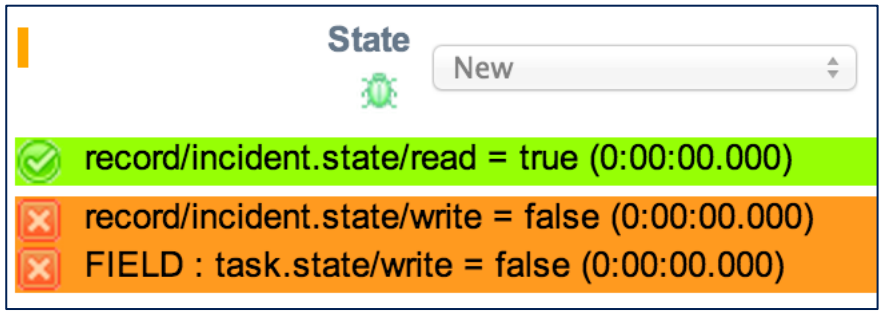
Debugging

- 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

© 2014 ServiceNow All Rights Reserved

Debugging

- Field debugging
  - Neat little bug!
- Debug output



15:49:42.994: TIME = 0:00:00.000 PATH = record/sys_history_set/read CONTEXT = sys_history_set.sys_id=null RC = false RULE =

record/*/read

15:49:43.838: TIME = 0:00:00.000 PATH = record/incident/write CONTEXT = INC0000051 RC = true RULE =

record/incident/write

© 2014 ServiceNow All Rights Reserved

Lab 7
Debugging

© 2014 ServiceNow All Rights Reserved

Lab 7

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

© 2014 ServiceNow All Rights Reserved

Lab 8
Encryption

© 2014 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

© 2014 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

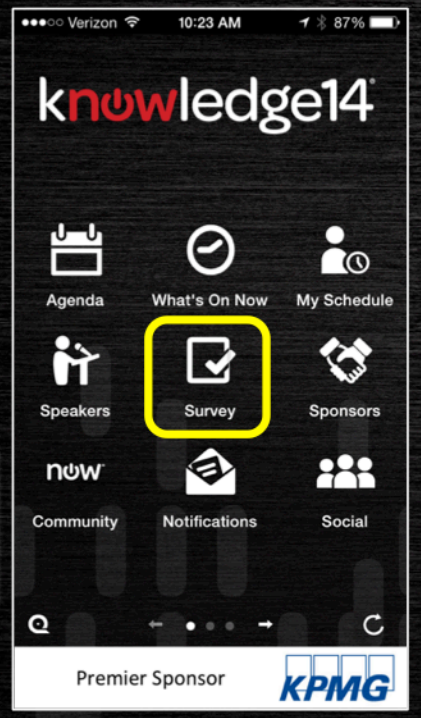
© 2014 ServiceNow All Rights Reserved

For more information, please visit the wiki:

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

© 2014 ServiceNow All Rights Reserved

Tell us what you think!



Click on the survey link in your Knowledge14 mobile app. Help us make Knowledge 15 even more valuable!

Thank You

Joseph Wheeler

Sr. Solutions Consultant

ServiceNow

joseph.wheeler@servicenow.com

Erich Dobroth

Sr. Solutions Consultant

ServiceNow

erich.dobroth@servicenow.com

Want a copy of this deck?

Sign into the BuzzHub to unlock all the slides and lab guides from Knowledge14 sessions

