iRODS Security Challenges Within an Enterprise Environment

Ryan Blome

Recognition

Henry Chen, Lux Izquierdo, Simon Cook, John Hodges, Sam Newkirk, Angela Ferro Capera

05/03/2024

Intro

- My role: Senior Information Technology Analyst/Developer
- Information Research, Core R&D: Our role is to integrate and develop new innovative digital and IT solutions to accelerate R&D innovation
- What I do: Full Stack Development, mainly working on automated data processing from Lab -> Processing -> Storage

Outline

- Problem: Synchronization
  - Architecture overview
  - Solution
  - Problems
  - Ideal route
- Problem: Authentication
  - Solution
  - Problems
  - Ideal scenario
- Security Solutions
- Future Goals

Problem 1: Synchronization

- Thousands of internal DOW users need to access specific datasets stored within our iRODS instances. iRODS does not currently support security group synchronizations with services such as LDAP (Light Weight Access Protocol), Azure Security Groups, or AWS Groups.

ARCHITECTURE

Microsoft Azure

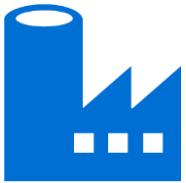
Azure Entra ID

iRODS®

GO ANYWHERE®
A HelpSystems Solution

metalnx

databricks



Data Factory

Azure DevOps

.NET

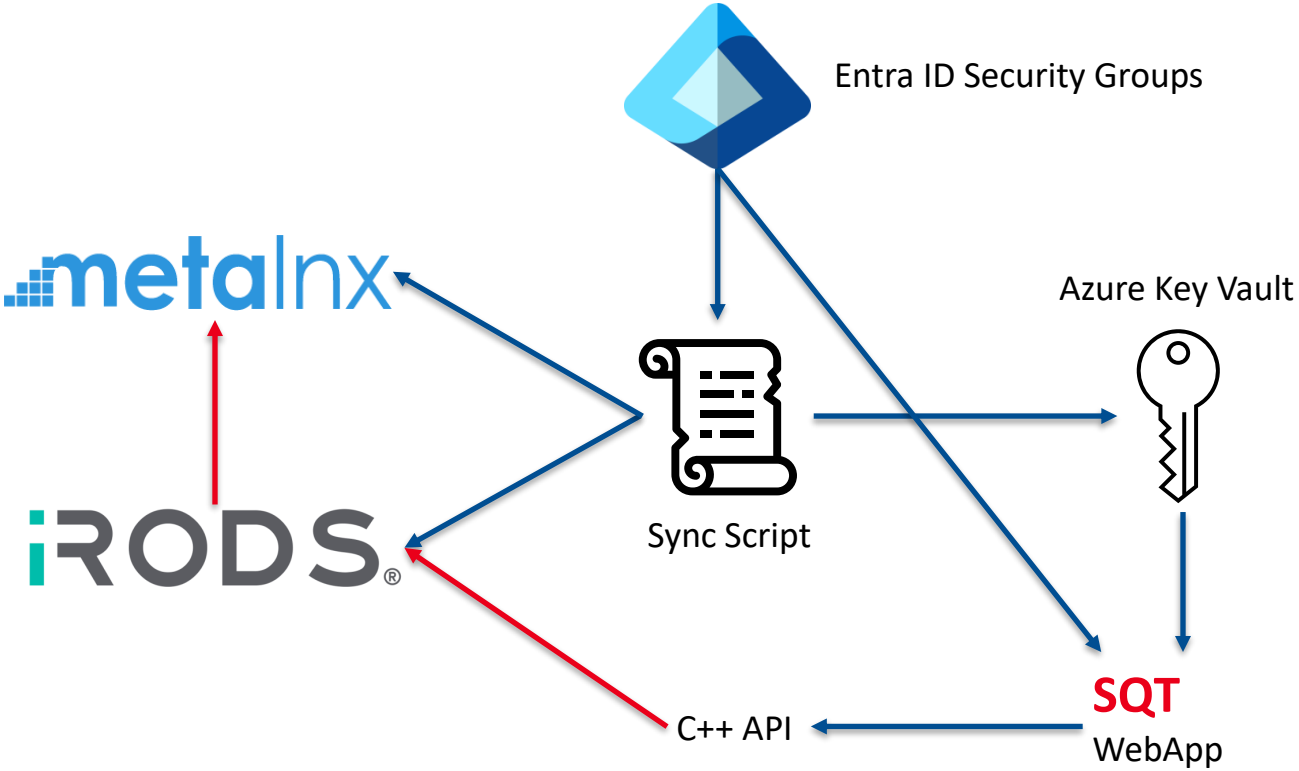
Azure Security groups

- Azure Entra ID Security Groups provide a standardized approach to user permissions across a variety of applications.
- Security groups are defined by company standards and manageable by group owners.
- Allows for simple user management and group modifications
- Set up a standard group naming scheme to easily pull the needed groups

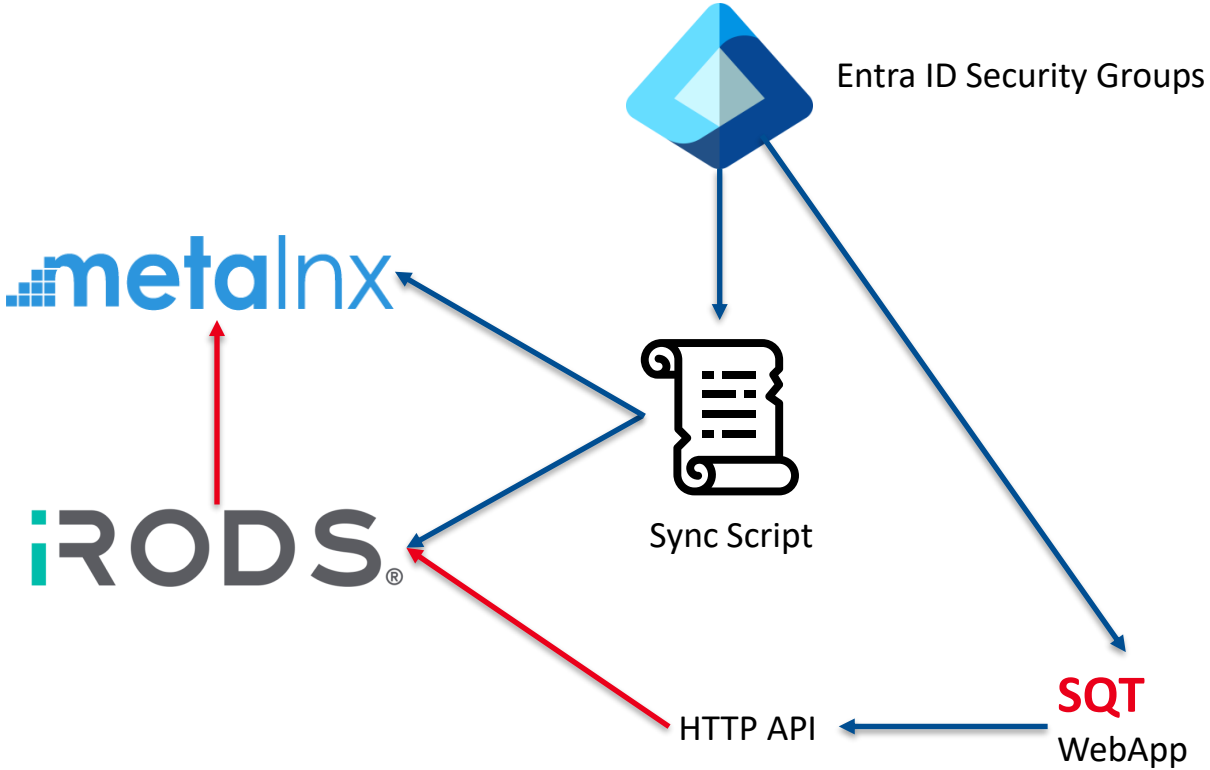
SOLUTION

- Automated Bash sync script.
  - Fetches our Entra ID Security groups from Azure
  - Loops through the Entra Group Users
  - Creates new iRODS users if someone is added to a group
  - Deletes users from iRODS if no longer in group
  - Updates user's groups if changes detected
  - Rotates Users KV Password(s) for C++ API
    - ✓ Passwords controlled by KV for API Auth

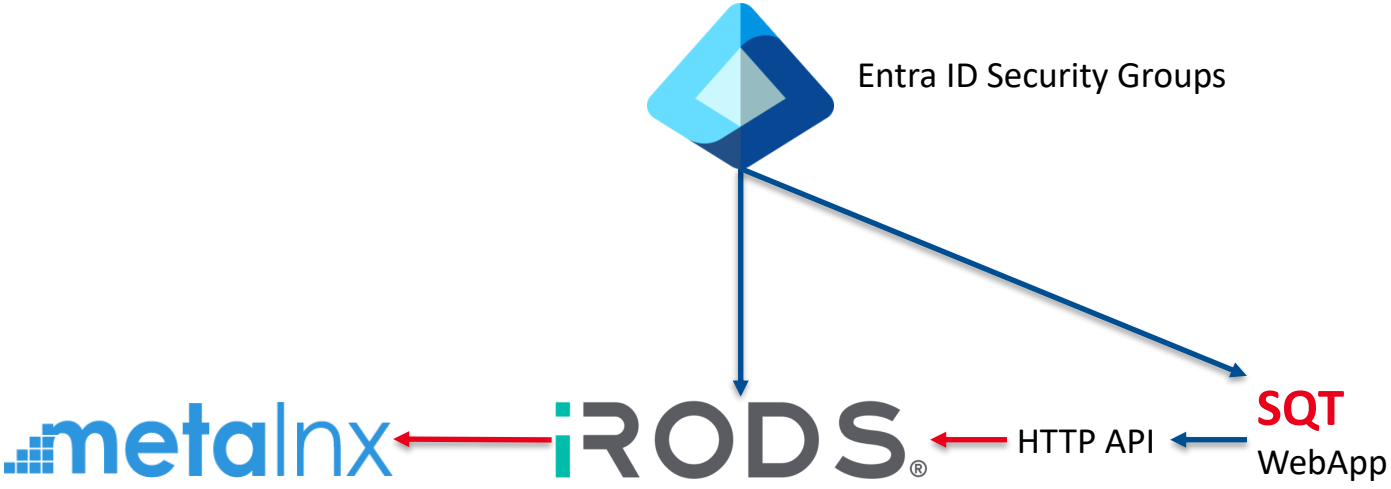
Architecture : Current State



Architecture : HTTP API Migration



SOLUTION: IDEAL STATE



Known Issues

- Runs several times daily
  - Needs manual activation when outside update window
  - If Issues occur requires manual intervention to re-run
- Increases overall level of tech debt
  - Maintenance
  - Deployments
  - Security scanning
- “universal” Passwords
- Requires directly updating two separate user tables daily.

IDEAL SCENARIO

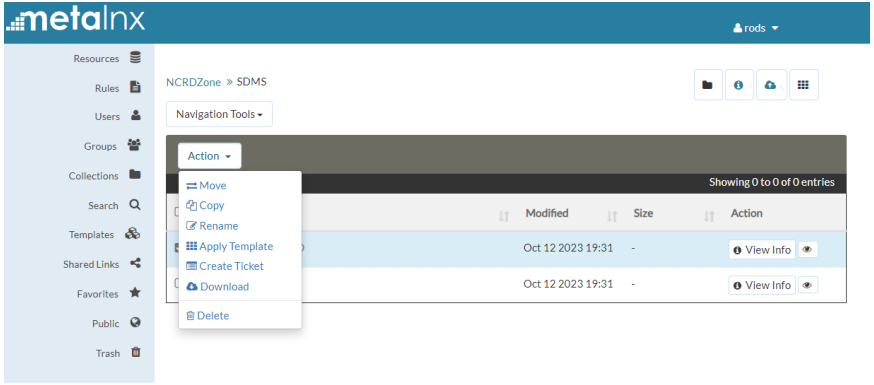
- iRODS supports group permission synchronization, updating at predetermined intervals or upon user login. Eliminating the need for custom-made synchronization scripts.
- “Permission Templates” have been established for OAuth groups to define access levels, such as Zones, Read-Write, Admin, etc..

Problem 2: Authentication

- Metalnx is currently the primary out of the box iRODS GUI management tool. This is a very powerful application but is missing some granular permission settings.
- The C++ API has been our primary connection to iRODS for the Past 2 years and has only supported Basic Authentication.

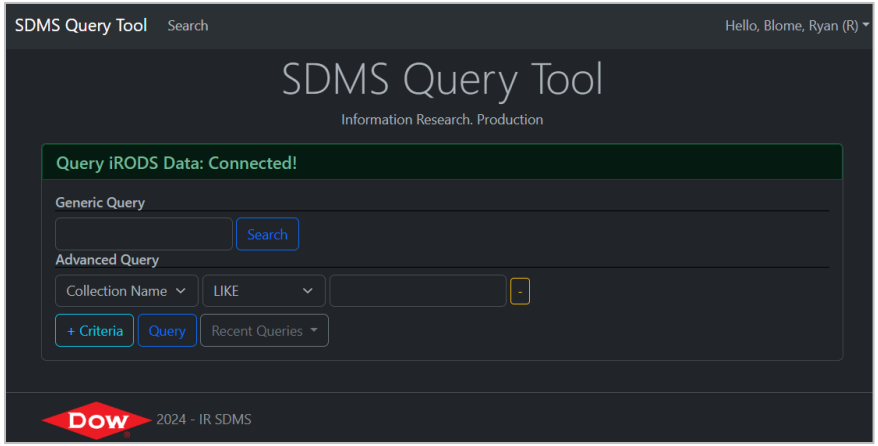
METALNX

- Metalnx
  - Direct Uploads
  - Delete (anything)
  - Modifying (anything)
  - Little auditability
  - Not easy to modify (many) users
  - Separate Metalnx/iRODS User DB's



SOLUTION

- SQT:
  - .NET Web Application
  - Read only access
  - Simplified user interface
  - Application Insights user action and error logging.
  - Automatic Login
  - URL Querying



Current Challenges

- Running on C++ API (Basic Auth)
- Requires the rotating Passwords for the users for seamless login
- Have had API crashing issues in the past
- More internally supported software increasing technical debt

IDEAL FUTURE

- HTTP API:
  - Integrate the new OAuth functionality for user info pass through
  - Mitigate C++ API instability
- Remove rotating Passwords requirement for SQT
- See more customizability of user permissions available through the group/user controls in iRODS/Metalnx
- SQT Future functionalities:
  - Meta Data dropdown searching
  - Controlled file uploads

QUESTIONS

- Questions?

Seek

Together™