Link to 2023 ACAMP Wiki

Advance CAMP Thu. Sept 21, 2023

Room - I

Session Title: Role based access provisioning

CONVENER: Gretchen, Renalto

MAIN SCRIBE(S): Gretchen, Andrew,

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: Full room ~60

DISCUSSION:

At Harvard: “Communities” - a group of affiliates, reflected as groups within Grouper
Looking to sync these groups to our IAM system (Sailpoint).
Also using Midpoint for specific casual affiliate population

Terminology
Role-based access control (RBAC) -
Grouper is heading to (ABAC) Attribute Based Access Control - move away from term “role” (gettes), ‘role’ is a 4-letter word, almost meaningless anymore. Hyzer likes the word ‘role’, fwiw.
(Hyzer) *Birthright* is also problematic, doesn’t follow Grouper Deployment Guide

There are challenges in provisioning group memberships to Google. Goal to connect Grouper directly to O365 using the Grouper connector (provisioner framework).
Michigan uses the new provisioner to O365. Not here but would be worth having a conversation.

Get on the latest Grouper (recommended quarterly updates).

What are thoughts on Group based provisioning of Sailpoint?
UPenn is using SailPoint - replaced homegrown identity system. Serves as subject source for Grouper. Sailpoint writes to a SQL table and Grouper uses that as a Subject source. Grouper creates policies from the basis data and sends policies back to SailPoint. Uses change log tables.

Messaging queues: Traditional message queues vs DB table queues with DB triggers

- Always need a full sync process

Base full syncs schedule on the time it takes to run. Short runs may be done hourly, longer runs possibly daily. Also schedule carefully so not all are syncing at the same time.

Incremental puts changes into a table that grow and grow. Full sync tends to be take current state and put it into the table.

Grouper > MidPoint Connector uses timestamp columns to see what changes. Don't need to have a change log table.

How are Grouper groups being used to automate provisioning? (Jeff Crawford)

- Raw groups from SOR (HR, Student)
- Become source for affiliations
- Globally defined grace periods (e.g. 30 days) (also have ability for more custom ability)
- Rolls up into policy groups

Paul - Unicon

- Most clients use Grouper to provision groups to LDAP, other targets
- SMU looking to do full provisioning from midPoint
-

Birthright provisioning (Hyzer)
WIth Grouper deployment guide, student = reference group. Policy group for Google would give account, not reference group.

Hyzer: Role = group of entities that are allowed to do something (policy group) vs. institutional roles (student, faculty, staff)

- If you have the google role you have a google account

Grace periods by application complicate things
Policy groups are the result of all math

Every app should have its own group. You can then customize for that specific application. (See Grouper Deployment Guide - Policy Groups)

High-level reference groups - institutional populations - SOR data
Libraries then have their own set of business populations they define.

Hyzer - Penn

- Students get access to O365
- Students on specific types of leave keep their email
    - Add population to O365 policy group
    - You can see who was in group at what point and when policy changed

Have single place to define rules - who has access to what and why?

With Grouper Visualization, you can quickly see what services an individual has access to.

Andrew (Wisconsin) Grouper should be your brain - midPoint should be the brawn, doing the hard work in downstream systems.

- Alternate view - IdM system is getting bogged down (Oracle Identity Manager). Would like to do more in Grouper.
-

Jeffrey - we provision to LDAP and everything reads there.
Grouper auditing is really helpful - you can see who changed what when.

Bert - Georgia Tech

- Some applications have such a rich permissions system that you can't externalize that
- Apps are sending CSV files to manage membership

- Ideally want to understand who has admin access vs. regular access so we can differentiate their login security

Best practice (Jeffrey): Do application-based membership in Grouper. Then how it gets to application is less important. (Define the access in Grouper with the reason WHY then inform other systems.

Hyzer - when onboarding application, slurp as much information into Grouper. Can have people see who has what, attest to membership,
Certification - Report in Grouper showing who has what, when affiliation last changed, etc.

Virginia Tech - Pushback on needing to understand who has admin roles.

Access Request mechanisms?

- Jeffrey (UCLA) - SNOW request to service owner, SO adds membership in Grouper, sets End date using feature in Grouper (approvals workflows in SNOW?)
    - Could be potentially automated via API but no budget
- midPoint has rich functionality around access requests - self-service????
    - Get more information from midPoint team
- Opt in exists in Grouper but people have trouble figuring that out
    - Custom UI simplifies this
- Docusign

ARTIFACTS / LINKS

linked