SUMIT

IT SECURITY EVENT SERIES

WEEKLY IN OCTOBER

Reimagined

INFORMATION AND TECHNOLOGY SERVICES
UNIVERSITY OF MICHIGAN

Follow Along @umichTECH
Join the Coversation #SUMIT21

What's New with MCommunity Groups

Aimee Lahann
IAM BSA Senior
Grouper Implementation Lead

Chris Hable
Product Manager for Identity
and Access Management

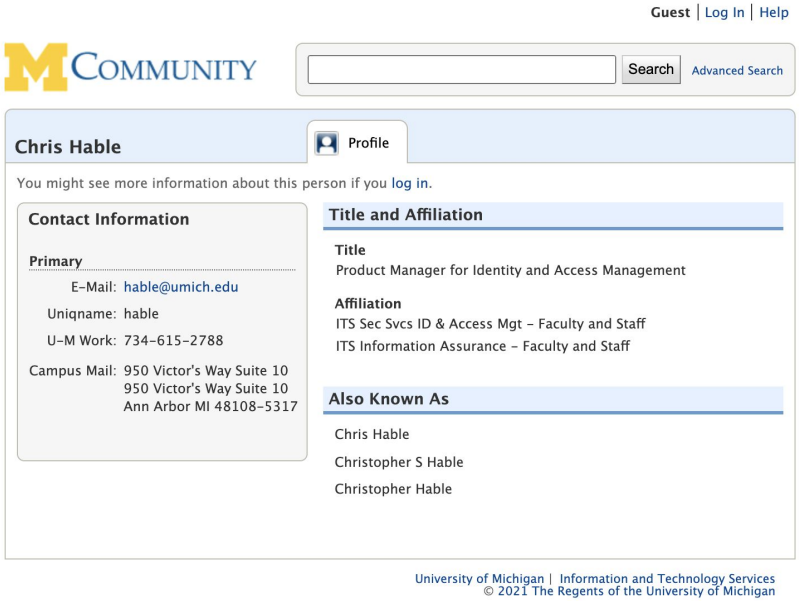
Liam Hoekenga
IAM Developer Senior
Grouper Implementation Lead

INFORMATION AND
TECHNOLOGY SERVICES
UNIVERSITY OF MICHIGAN

SUMIT Reimagined

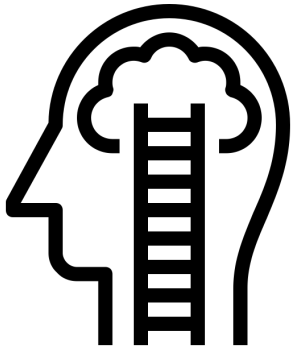
First, A Little Context

mcommunity.umich.edu



The Dream

- IT professionals across campus can quickly create and manage their own access control groups from predefined, centrally available groups of institutional data.
- Access control groups automatically update based on current institutional data.
- Access control groups are easily integrated with consuming systems.
- It is easy to know who is in an access control group, what access it provides and why.



Created by Maxim Basinski from Noun Project

Intro to Grouper

Open Source software providing group management component of the InCommon Trusted Access Platform (TAP), identity and access management suite of software designed to integrate with existing systems

- Designed by and created for higher ed to address similar challenges of creating institutional role and access management solutions for a federated environment

Benefits:

- distributed access control governance
- fast flexible provisioning integrations
- robust auditing and reporting to answer who, why, when, and how someone has access to a resource. ~Grouper Executive summary

Successful Grouper Implementations at other Campuses

UPenn (10 years)

- A/D
- Zoom
- Box
- Atlassian

Illinois (since 2019)

- Splunk - all access control is set up in Grouper.
- Azure AD Groups - connects directly to Azure AD from Grouper; it skips AD.

Nebraska

- Housing has delegated access - to control door access
- Endpoint Management Team
  - Software access groups driven by Grouper
- Email lists for everyone with a specific major

University of Chicago - early adopter

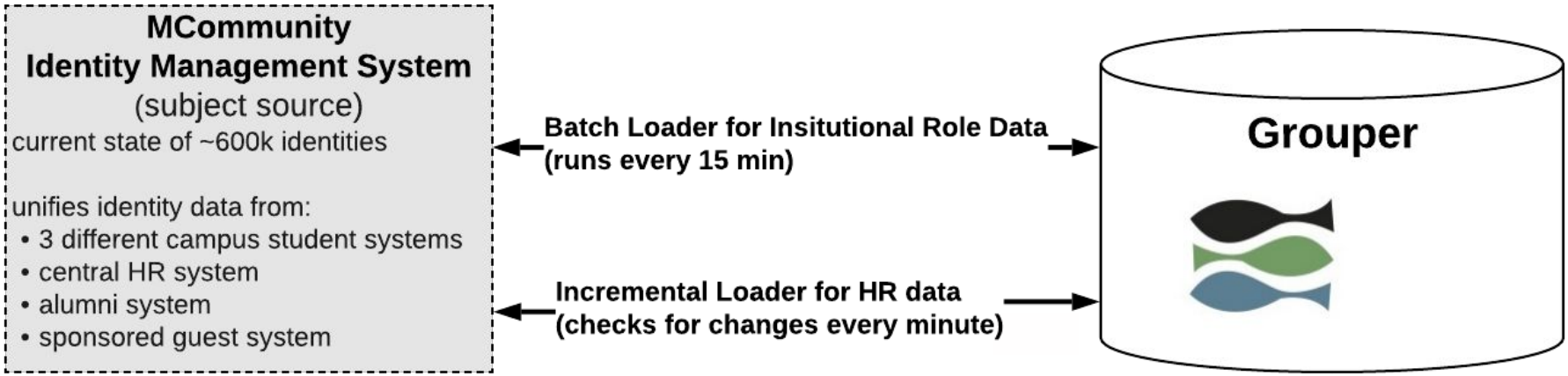
- 100 services, including wireless, Box.com, business objects, Google Apps, file sharing, web-based file storage, VOIP services, VPN, faculty class management applications, email routing, and student information system.

How does Grouper work?

1. Define an access policy.
    a. All U-M faculty on Flint, Ann Arbor, and Dearborn campuses should have access to Awesome New Service. Access to Awesome New Service must be deprovisioned after a 33 day grace period. Chris Hable never should have access.
2. Create an access policy group enforcing membership to comply with policy through use of predefined, centrally-available current institutional data.
3. Provision the access policy group where needed, automatically in near real time.

“Access to systems is then automatically kept in sync with policy as subject attributes change in underlying systems of record (ERP, etc). This provides streamlined and automated access for existing and future applications. “ ~ Grouper Deployment Guide

Loading Institutional Data into Grouper



Reference Groups: Institutional Data Organized into Meaningful Cohorts

Current Institutional Role Members

People who currently have the institutional role

- FacultyAA (ref)
- FacultyDBRN (ref)
- FacultyFLNT (ref)

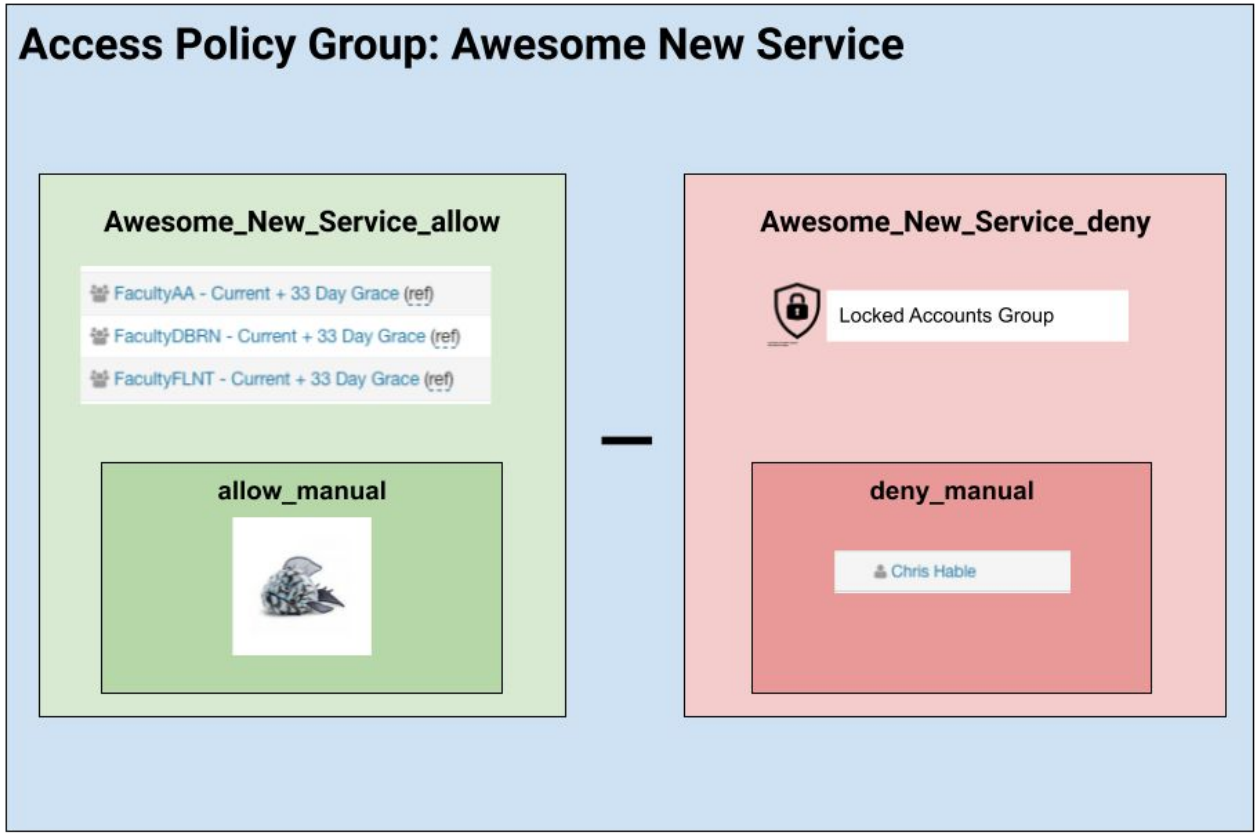
Current + 33 Day Grace

People who currently have the institutional role plus those who have lost it within the last 33 days

- FacultyAA - Current + 33 Day Grace (ref)
- FacultyDBRN - Current + 33 Day Grace (ref)
- FacultyFLNT - Current + 33 Day Grace (ref)

HR Data by Department

- Aerospace Engineering (212000) (ref)
- Aerospace Engineering 212000 (ref)
- Aerospace Engineering 212000 - Active (ref)
- Aerospace Engineering 212000 - Emeritus (ref)
- Aerospace Engineering 212000 - Faculty (ref)
- Aerospace Engineering 212000 - Faculty - Active (ref)
- Aerospace Engineering 212000 - Faculty - On Leave (ref)
- Aerospace Engineering 212000 - Faculty - Retired (ref)
- Aerospace Engineering 212000 - NewHire (ref)
- Aerospace Engineering 212000 - On Leave (ref)
- Aerospace Engineering 212000 - RegularStaff (ref)
- Aerospace Engineering 212000 - RegularStaff - Active (ref)
- Aerospace Engineering 212000 - RegularStaff - On Leave (ref)
- Aerospace Engineering 212000 - RegularStaff - Retired (ref)
- Aerospace Engineering 212000 - Retired (ref)


Access Policy Group: Awesome New Service
Awesome_New_Service_allow
FacultyAA - Current + 33 Day Grace (ref)
FacultyDBRN - Current + 33 Day Grace (ref)
FacultyFLNT - Current + 33 Day Grace (ref)
allow_manual
Awesome_New_Service_deny
Locked Accounts Group
deny_manual
Chris Hable

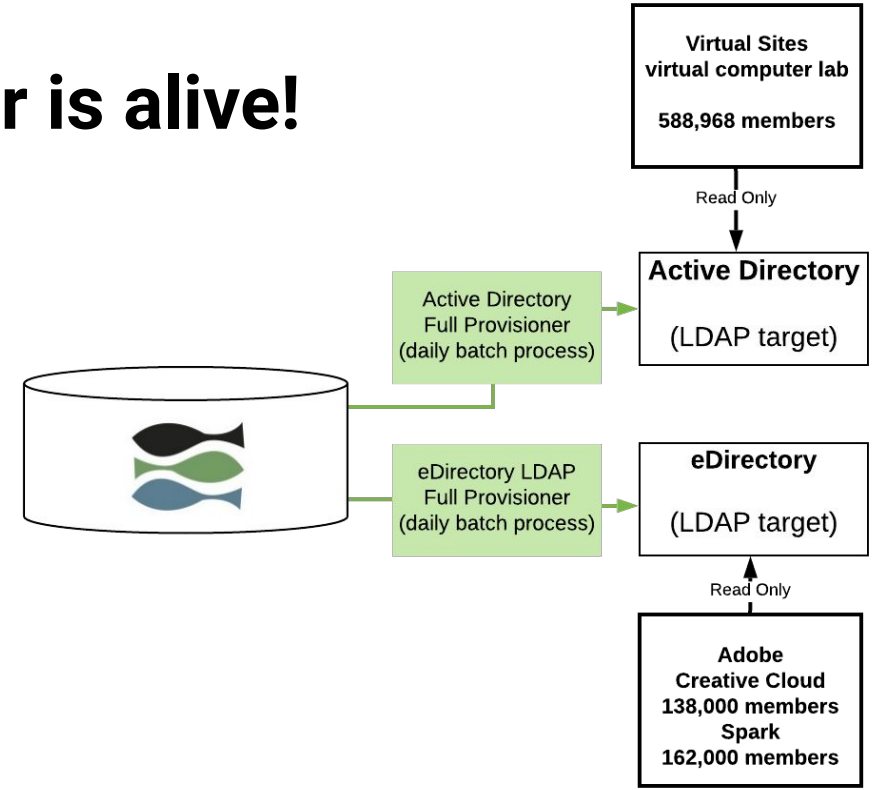
Provisioning Models

1. **Direct from Grouper to target service**" covers Grouper specific components and plugins for various targets such as AD/LDAP, Duo, etc. Grouper contains a change log for loosely coupled connections to external systems.
2. "**Message queue based delivery**" relies on a message queue infrastructure to communicate changes to appropriate provisioning components. In this model the logic for communicating with the external system would not be executed / managed / monitored / audited inside of Grouper
3. **External systems** can use web services or LDAP to pull data from Grouper into their data repository.

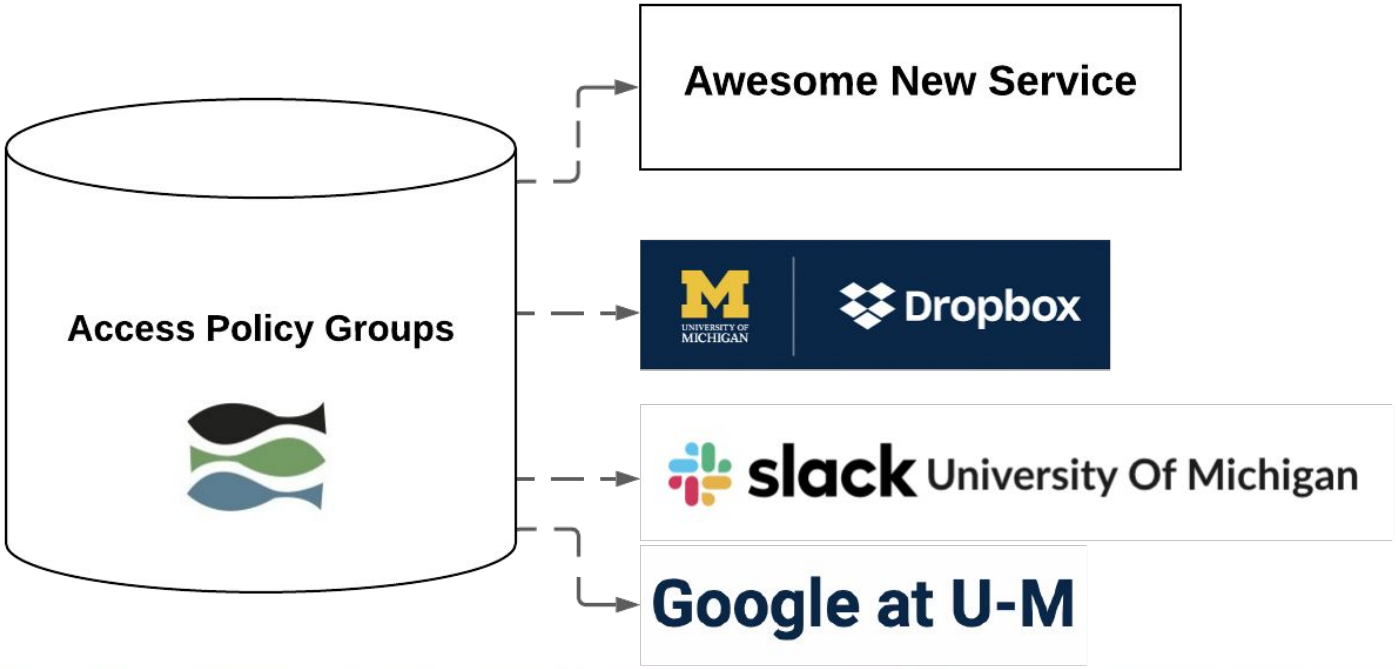
Two Main Strategies to Provision to Target Services

1. **Full-sync batch scheduled provisioning** looks at the source and the target and fully synchronizes the data
2. **Incremental near real-time provisioning** looks at the change log to send focused events to the target. ~ Grouper Deployment Guide

Grouper is alive!



We will build beyond on our current provisioning patterns.



Security Benefits

The right people have the right access at the right time

Enforced access policy - especially helpful for timely deprovisioning

Reports show membership changes over time

Easy to see who is in an access policy group and why

View of an individual's membership across all access policy groups in Grouper

Who will be able to use Grouper?

Decentralized service offered to units* across campus to quickly create and manage their own access policy groups to meet business requirements.

Security scaffolding is in place which prevents viewing and/or updating access policy groups you do not administer.

*with training to guide responsible use of identity data

its-grouper@umich.edu

Institutional Roles

Faculty -defined as academic, instructional, and research appointments; includes emeritus faculty (job families 8,9,10,11,13,14,19,20,22-emeritus)

Regular Staff - identified as Regular with current appointment not in the faculty job families and with a status of active, suspended, short-work break, leave, or paid leave

Temporary Staff - identified as Temporary with current appointment not in faculty job families with a status of active, suspended, short-work break, leave, or paid leave

EnrolledStudent - enrolled in at least one credit hour for ""current"" term; next term information is used during gap between terms

Student - continuing and incoming students regardless of enrollment; includes detached study

SponsoredAffiliate - identities from the Sponsor System - only includes active

NewHire - some employee information and future start date

Retiree - retired from any U-M campus, regardless of other appointments that may still be active