University of Waterloo

Grouper was implemented as part of an IAM renewal program for the university in the spring of 2018. Version 2.4 is currently in production and an upgrade to 2.5 is currently being tested.

Overall Strategy

Our IAM strategy for determining access was introduced as two step process in Grouper:

1. Determine all the ways an individual is affiliated with the university
2. Use affiliation populations to build access definitions

The Grouper Loader is used to introduce affiliation groups based on available campus data that is linked to identity:

- Employee
    - Employee Types (Faculty, Staff)
    - Departmental Hierarchy
- Student
    - Undergraduate/Graduate/Applicant/Alumni
    - Faculty affiliation
    - Program of study
    - Course Enrollment

Delegated access is rolled out to the various units across campus on as need arises. These administrators are asked to build further affiliations that aid in required access definitions, things like:

- Project group members
- Committee members
- Research groups

Access definitions are then built using the available affiliations. Access definitions typically require X groups:

1. A "members" group that collects affiliations that require access
2. A "manual adds" group that allows the delegated admin to inject "one off" members that are not affiliated in the typical way
3. An "unfiltered members" group that collects #1 and #2
4. A "manual removals" group that allows the delegated admin to remove
5. The "access definition" group that subtracts #4 from #3

Some access definitions are contained within a department while others are spread across the university.

Provisioning Access

A custom connector was built to allow the campus IDM system to track Grouper group memberships. The access definitions group memberships are used in the campus IDM to detect entitlements required by an identity. Accounts and access provisioning using these groups are currently targeted towards services like:

- Active directory group memberships
    - Departmental content
    - Project content
- O365 account licensing
- Email account entitlement
- Jira and Confluence access

We're also using PSPNG to provision to an Active Directory that was put in place while Grouper was being piloted and has been left in place.

Current State

The system has been in use since spring 2018. There are currently 540 delegated administrators across campus working with 29,000 groups (the bulk of which are loaded).

The production system runs using two smaller VMs acting as user interface servers, and one running the daemon (loader & PSPNG).