Managing User Access: How to Manage the Herd

August 8, 2018
UCCSC 2018 – UC Davis
Jeffrey Crawford – UCLA – IDM Solutions Architect
Warren Leung – UCLA – IDM Program Manager

What challenges do you face when managing access for your users?

The Challenges

- Takes too long

- Repetitive

- Unsure of what access users need or have

- Removing access?

Why is Identity no longer enough?

Problems

- Access based on account status
- Modify access on account change
- Access under departmental control
- Audit access across the enterprise
- Maintain access sanity
- Exception cases
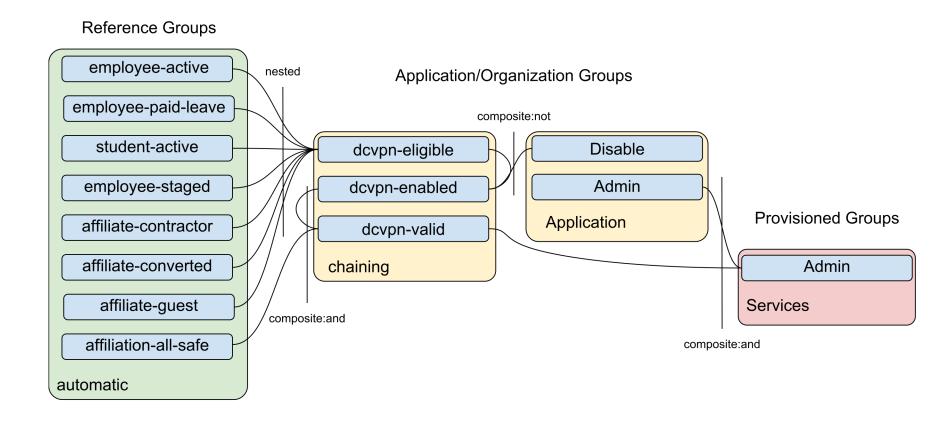
Internet2 Grouper

What is Grouper

- Distributed enterprise access management system
- Trust and Identity in Education and Research (TIER) Initiative
- NIST 800-162 – Attribute Based Access Control (ABAC)

Key Grouper Features

- Auditing

- Delegation

- Group Math

- Grouper Rules (Triggers)

- Web Service

- Attestation

- Time based Management

Examples: Data Center VPN Access

Reference Groups

automatic
- employee-active
- employee-paid-leave
- student-active
- employee-staged
- affiliate-contractor
- affiliate-converted
- affiliate-guest
- affiliation-all-safe

nested

Application/Organization Groups

composite:not

chaining
- dcvpn-eligible
- dcvpn-enabled
- dcvpn-valid

composite:and

Application
- Disable
- Admin

Provisioned Groups

Services
- Admin

composite:and

Delegation

- Departments know their access best
- IAM doesn't need to know the details
- Access granting/removal is tracked
- Departments can use reference groups
- Based off the Grouper Deployment Guide
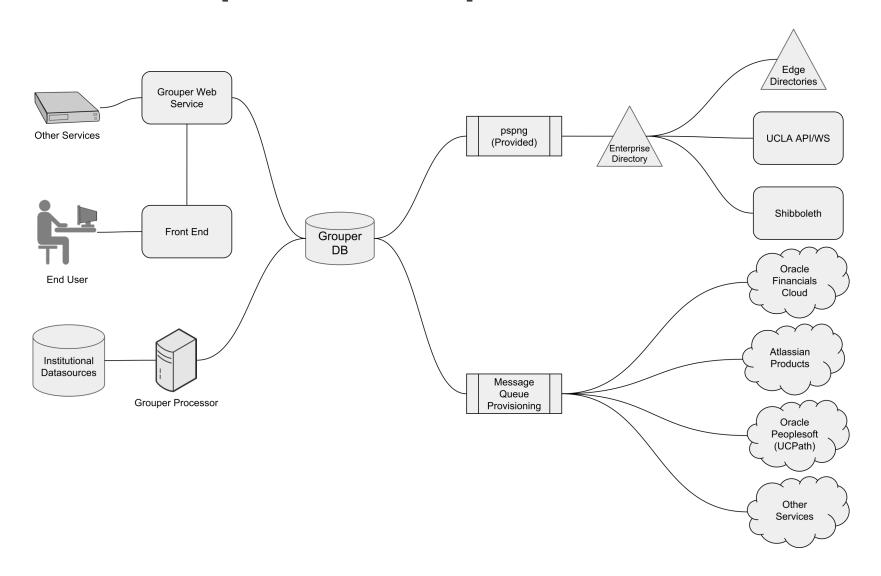
Grouper at UCLA

Distributed Administrative Computing Security System (DACSS) at UCLA

- Legacy system

- Delegated administration

- Fine grained access control

- How do we transition to Grouper?
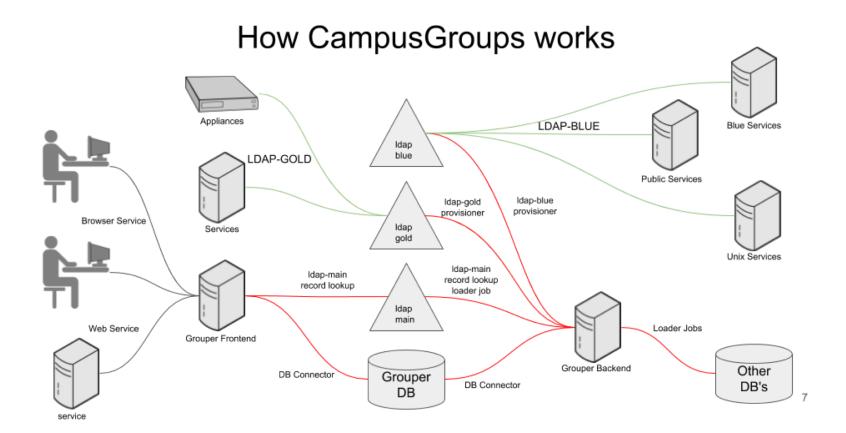
UCLA Grouper Use Cases

- Multi-factor Authentication
- MyUCLA (Student Portal)
- BruinCard (Door Access Management)
- AWS Management

UCLA Proposed Grouper Architecture

Grouper at UCSC

UCSC Grouper Architecture

How CampusGroups works

UCSC Grouper Use Cases

- VPN Access

- CruzID Manager (Access Control)

- Public Groups

- Campus Group Access

Best Practices for Deployment

- Note the lack of structural differences
- Use TIER as a starting point
- Talk to your developers and functional teams to understand their application
- Talk to Security about sensitivity of groups

Resources

- Grouper: https://www.internet2.edu/products-services/trust-identity/grouper/

- IAMUCLA: https://www.it.ucla.edu/iamucla

- TIER Grouper Deployment: https://spaces.at.internet2.edu/x/mgAZBg

- Contacts: jcrawford@it.ucla.edu, wleung@it.ucla.edu