UCLA Grouper Page

UCLA Grouper Deployment

Overview

UCLA's enterprise identity management program (IAMUCLA) deploys Grouper as a strategic component of its role and access management solution. Grouper is at the center of all group-like (role, access control list, service eligibility, distribution list) management activities on the IAMUCLA roadmap.

We are actively working with campus data stewards to identify/define institutional roles (types of students, types of employees, types of visitors/guests, etc.) in order to source and automate book-of-record group/role provisioning. As opportunities arise, we work with service providers to streamline and automate role-based access for existing and future applications.

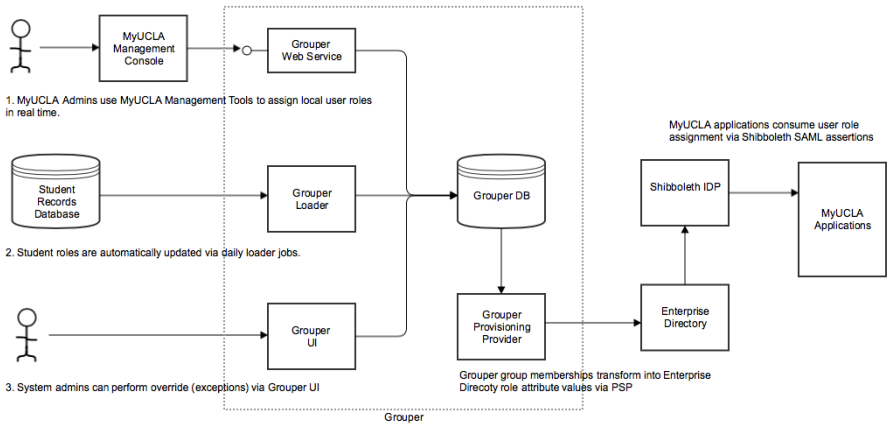
The sections below highlights several sample Grouper integration use cases at UCLA:

IAMUCLA Deployment Use Cases

Student Portal (MyUCLA) Role-Based Access

Type: Application Role-Based Access Control

MyUCLA is UCLA Student services portal. Rather a traditional portal where content is collected and delivered via widgets on a single platform, MyUCLA is made up of several distinct web applications. Each of these applications is managed by a different department at UCLA. MyUCLA produces a coherent user experience through coordinated design, development, and a set of back-end data sharing/exchange interfaces. In particular, all MyUCLA applications share a common set of Grouper-managed user roles and access memberships. Group membership is managed via a mix of book-of-record data feeds and direct updates via Grouper web service. The membership assignment in turn maps to role attribute values. All applications under the MyUCLA umbrella consume role attributes via Shibboleth to determine user access at run time.

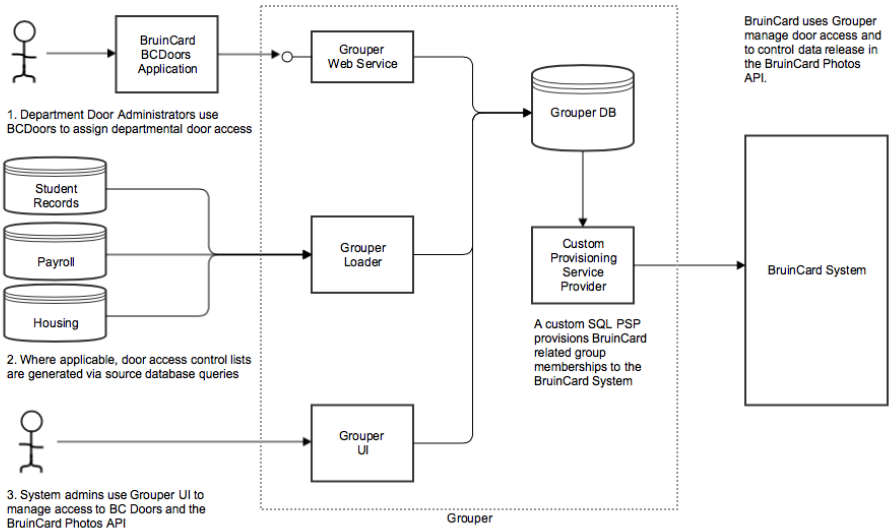


Campus ID Card / Door Access Management (BruinCard)

Type: ACL-Based Access Control

BruinCard is UCLA's employee and student photo ID card. It is a physical door access token, a debit card, and is used for meals and access to events on campus. When we replaced the BruinCard technology stack in 2015, we integrated BruinCard systems with Grouper. Grouper is now the engine behind most of BruinCard's group and role management needs. These include:

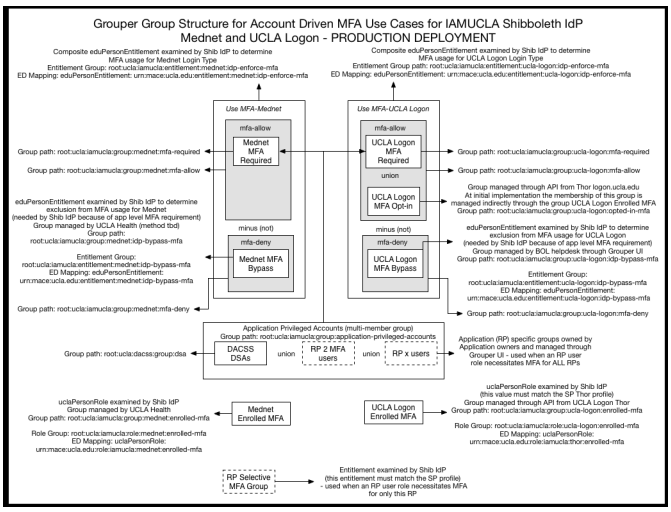
- Door access assignment - delegated function to let departmental door administrators manage door access in the departments
- Door administrator role assignment - manage who is a door administrator, and for which unit
- Photo API access - manages the ACL for BruinCard photo downloads



Shibboleth Multi-Factor Authentication Management

Type: Service Eligibility Declaration / Group Membership Management

UCLA deployed multi-factor authentication (MFA) in its Shibboleth Single Sign-On service in June 2016. Our goal, over time, is to require MFA use for all sensitive account access. On our way to that goal, we need to develop a flexible architecture enabling us to flexibly manage the MFA-required population. Grouper is the calculation engine we use to track who needs to enroll, who has enrolled, and who are the exceptions.



External Service Entitlement Attribute Management (PAC-12 TV and HBO GO)

Type: Service Eligibility Declaration/Management

UCLA uses Grouper to calculate and set eduPersonEntitlement values for a number of external services. These include PAC-12 TV Network mobile access and HBO Go access. We are in the process of converting all similar entitlement assertions (Google Apps, Gartner, etc.) to user Grouper.

Box Group Management

Type: Group Membership Management

Box (box.com) is UCLA's online file storage and collaboration service. Box's built-in group management is awkward and difficult to scale to a distributed environment. We are externalizing group management from Box to Grouper, using Grouper to:

1. automate Box group membership updates (from book-of-record data sources)
2. enable more flexible, distributed group membership management by project, department, or collaboration groups.

Application-Specific Deployment Use cases

Faculty Information System (Opus)

Separate from the Enterprise IAM deployment, UCLA's Faculty Information System Project (Opus) has adopted Grouper as an application-specific, academic hierarchy driven, role-based access management solution.

Opus intends to operate a separate Grouper instance from the enterprise instance at its initial launch. Plans to migrate/converge with the enterprise instance is TBD.

Architecture and Design

- UCLA Group Naming Guide
- UCLA Grouper Folder Registry

Presentations