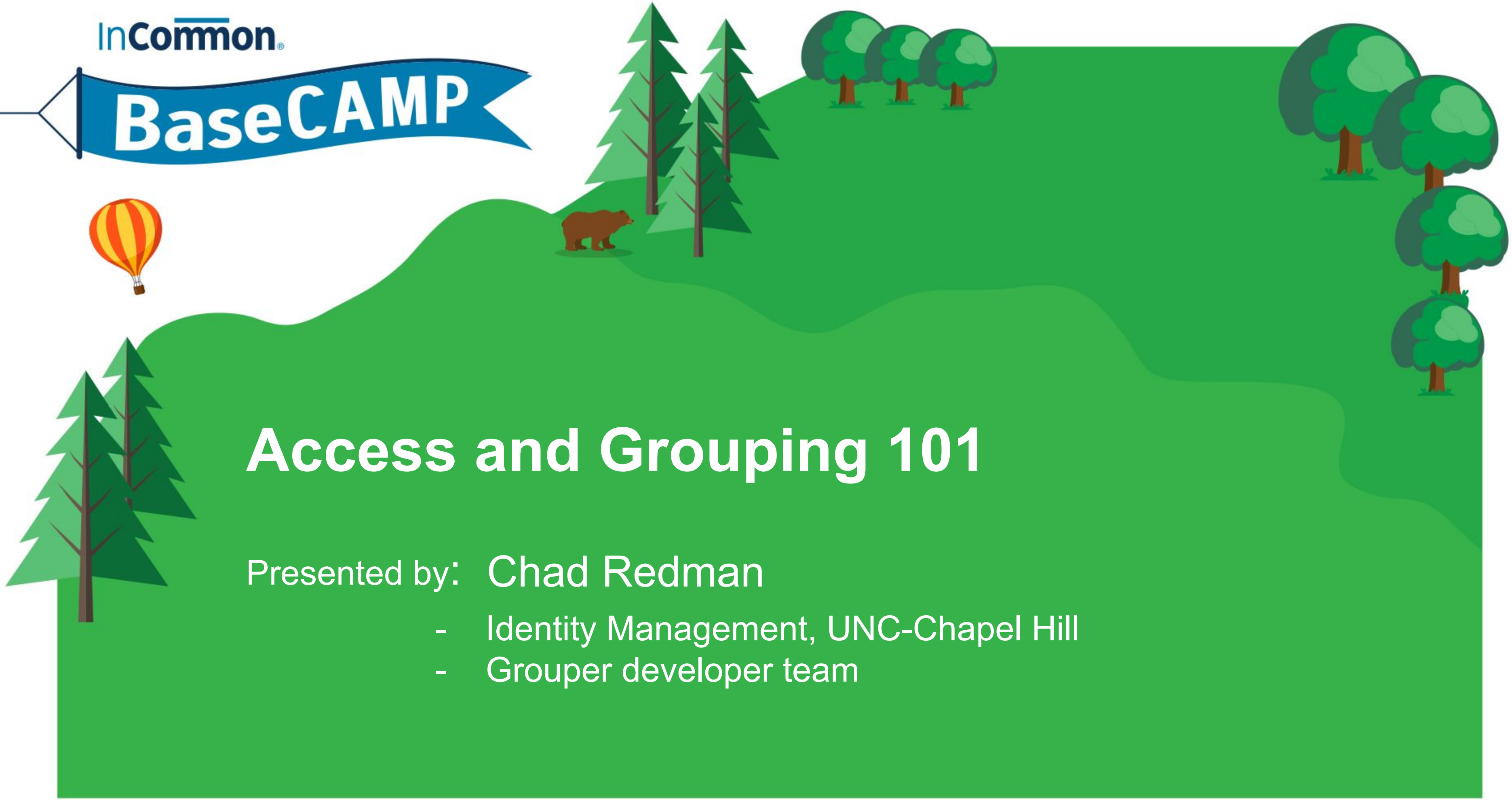
InCommon

BaseCAMP



Access and Grouping 101

Presented by: Chad Redman

- Identity Management, UNC-Chapel Hill
- Grouper developer team

IAM

Identity and

Access

Management

Working Together...

Authentication

PLUS

Authorization

What is Access Management?

- Permission to use a resource (building, application, application feature)
- Implements resource-specific access control policies
- Policy decision could be based on different factors
    - authenticated vs. anonymous
    - identity provider (which institution did the authentication)
    - origin (e.g. their email domain)
    - location (on-site/off-site)
    - time of day
    - level of assurance (e.g. MFA)
    - identity (a specific user)
    - user roles and attributes

Access Control Models

Role-Based (RBAC)

- Users are associated with one or more roles

Attribute-Based (ABAC)

- Users have attributes
- Can mix and match to calculate policy

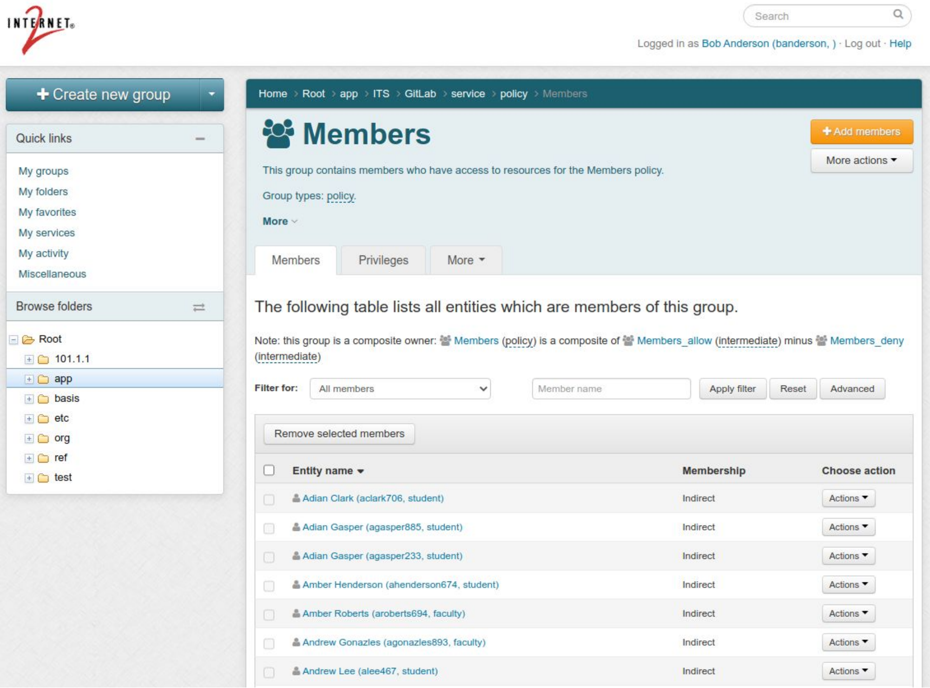
Example Access Policy
Enterprise GitLab

1) All ITS staff and contractors
2) All Computer Science faculty
3) Students enrolled in CS 301
4) Other users allowed by CS faculty
5) **Disallowed if account has been compromised!**

A good access management system should have...

- Centralization, with delegation
- Automation
- Auditing

Grouper



Logged in as Bob Anderson (banderson,) · Log out · Help

Members

This group contains members who have access to resources for the Members policy.

Group types: policy.

More

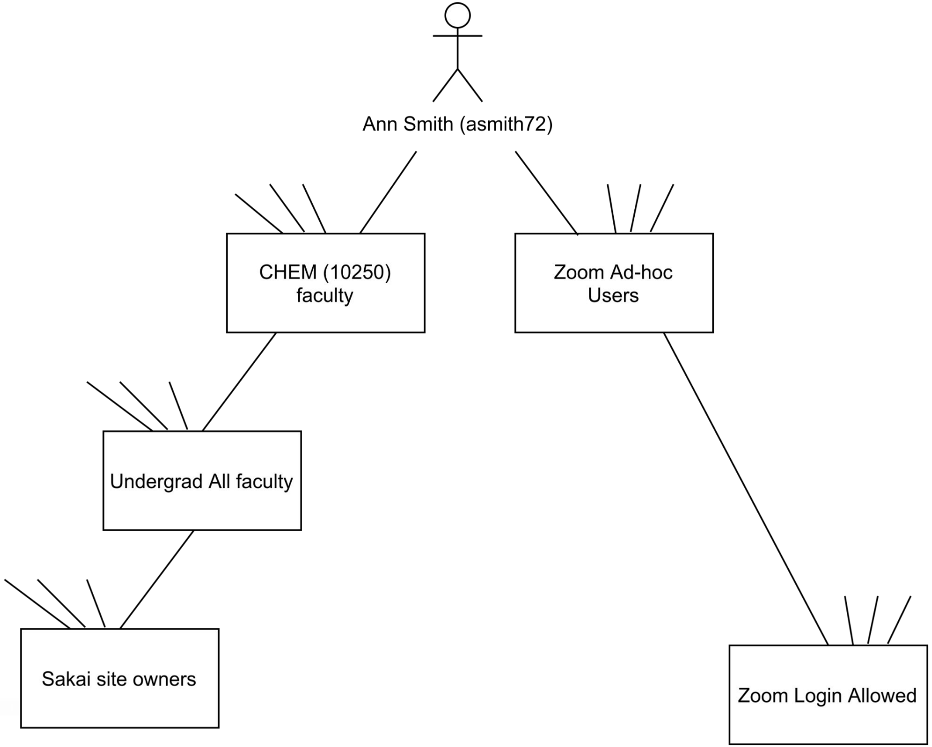
The following table lists all entities which are members of this group.

Note: this group is a composite owner: Members (policy) is a composite of Members_allow (intermediate) minus Members_deny (intermediate)

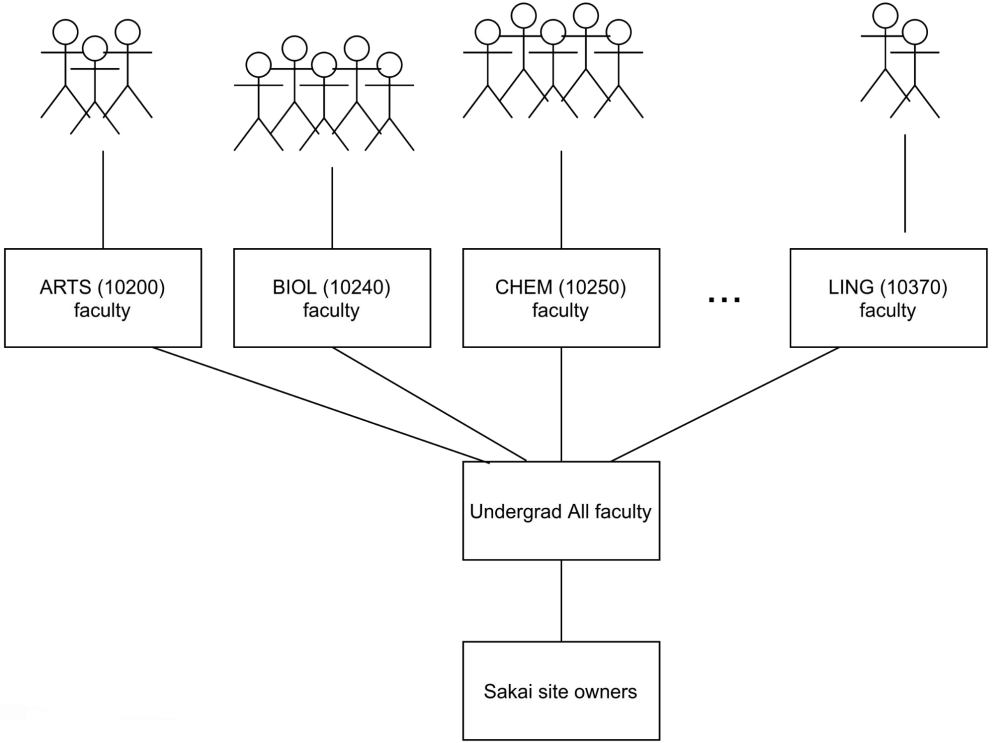
Filter for: All members | Member name

□	Entity name	Membership	Choose action
□	Adian Clark (aclark706, student)	Indirect	Actions
□	Adian Gasper (agasper885, student)	Indirect	Actions
□	Adian Gasper (agasper233, student)	Indirect	Actions
□	Amber Henderson (ahenderson674, student)	Indirect	Actions
□	Amber Roberts (aroberts694, faculty)	Indirect	Actions
□	Andrew Gonazles (agonazles893, faculty)	Indirect	Actions
□	Andrew Lee (alee467, student)	Indirect	Actions

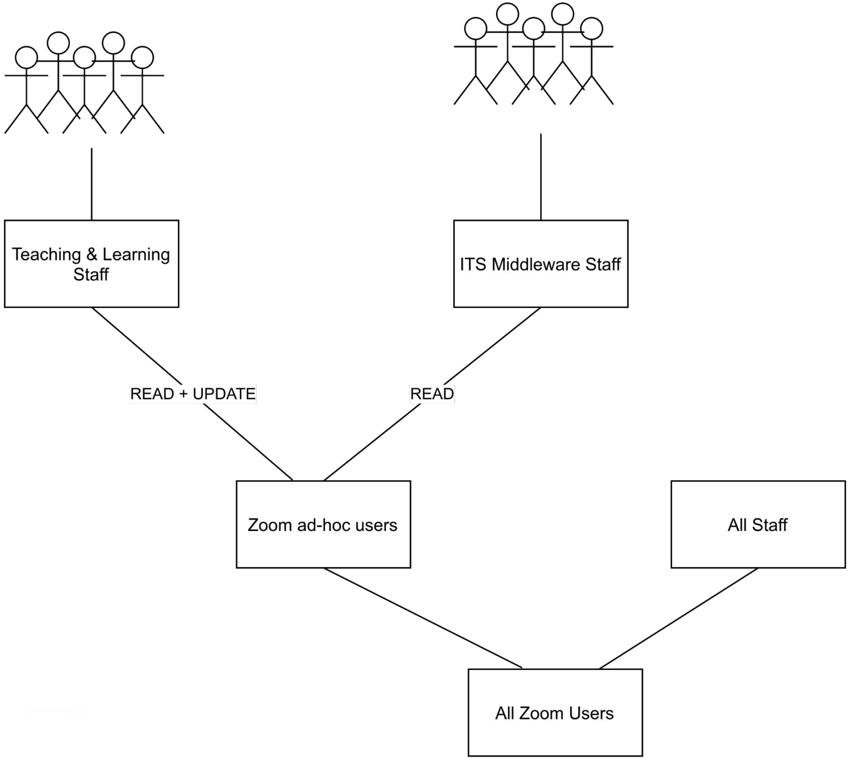
Membership Inheritance



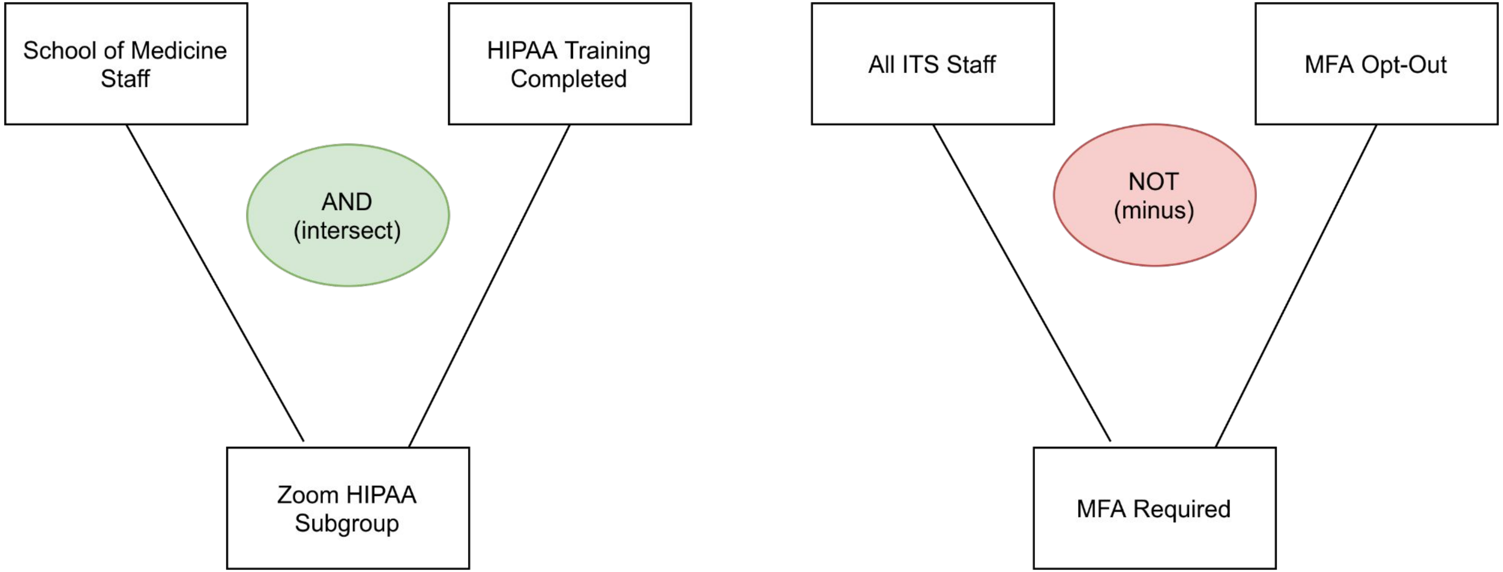
Group Member Inheritance



Grouper Privileges



Grouper Set Operations



School of Medicine Staff

HIPAA Training Completed

AND (intersect)

Zoom HIPAA Subgroup

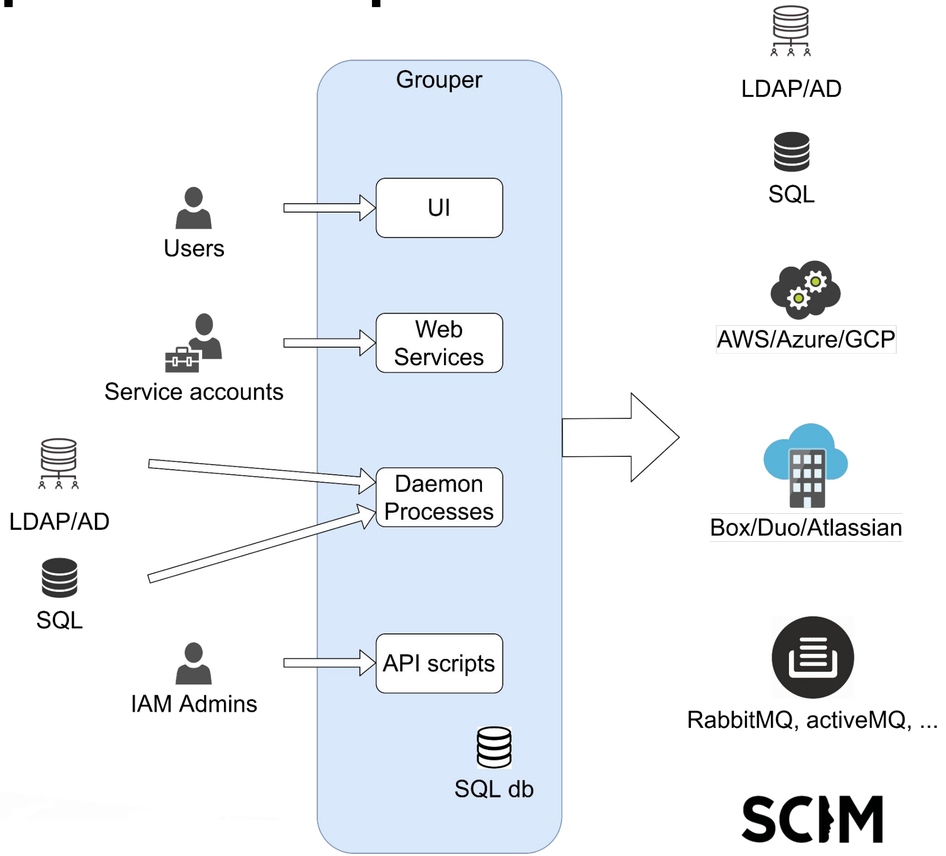
All ITS Staff

MFA Opt-Out

NOT (minus)

MFA Required

Input / Output



Grouper Deployment Guide

- “Basis” groups pulled from external systems
- “Reference” groups built from basis groups or other reference groups
- Policy groups and privileges use reference groups
- Avoid putting subjects directly into policies! Leverage group inheritance

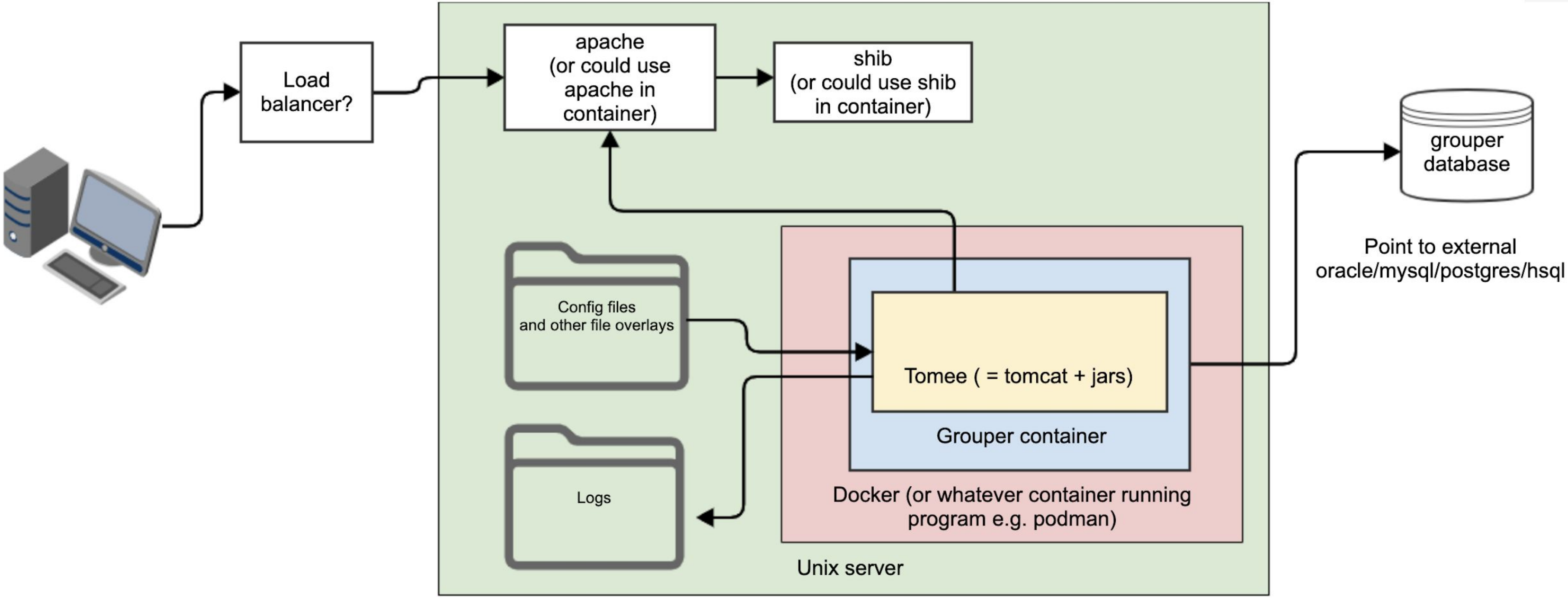
UI Demo

- Navigation
  - subjects, groups, folders
- Subject sources
- Basis groups
- Loader jobs
- Reference groups
- Policy groups
- Visualization
- Privileges
- Provisioning
- Auditing
- Attestation

Example Access Policy
Enterprise GitLab

1) All ITS staff and contractors
2) All Computer Science faculty
3) Students enrolled in CS 301
4) Other users allowed by CS faculty
5) **Disallowed if account has been compromised!**

Deployment


Load balancer?
apache (or could use apache in container)
shib (or could use shib in container)
grouper database
Point to external oracle/mysql/postgres/hsql
Config files and other file overlays
Logs
Tomee (= tomcat + jars)
Grouper container
Docker (or whatever container running program e.g. podman)
Unix server

Questions/Discussion

Content