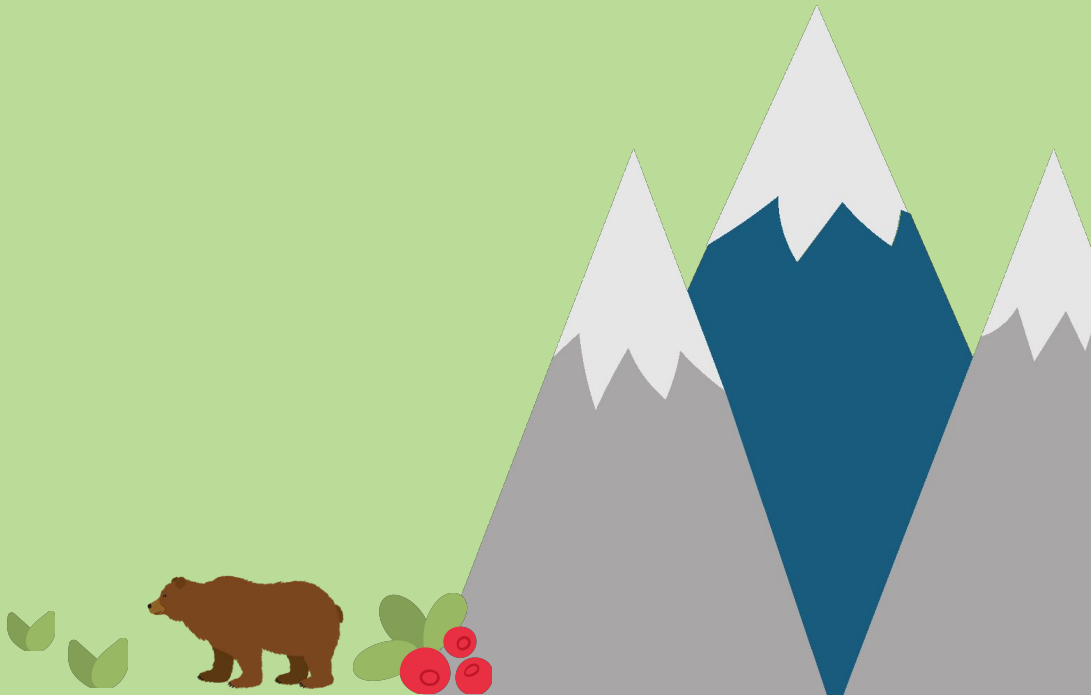
Core Concepts of Access & Grouping

Kellen Murphy, Identity Architect | University of Virginia

Date: June 5, 2025



Overview

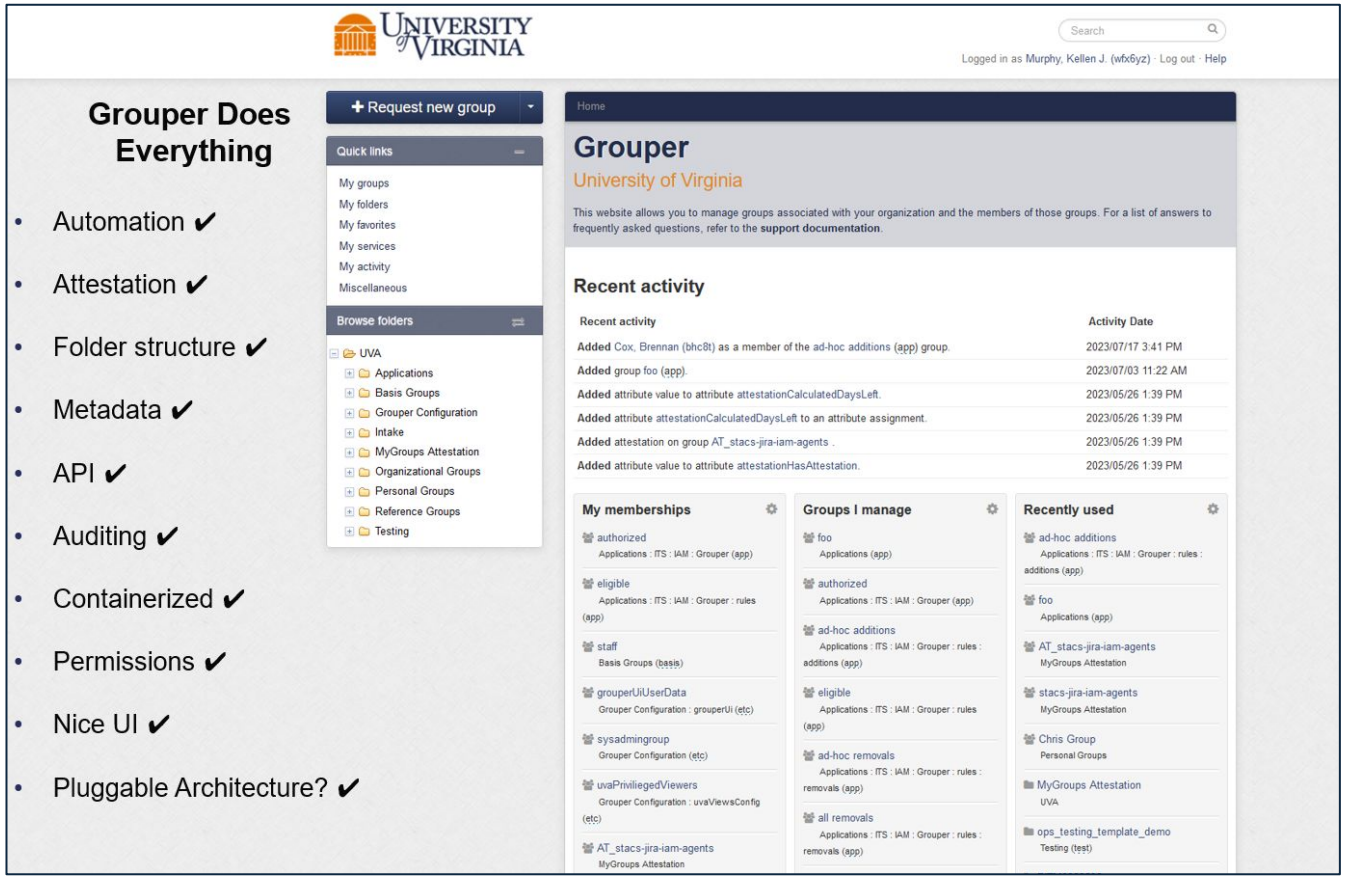
- **Why am I here?**
- Authentication vs Authorization
- Access Control Methods
- Grouping
  - Group Data Structures
  - Manual vs Automated
  - Attestation
  - Examples
- Q&A

Group Management @ UVA

- “MyGroups” — Legacy, home-grown tool that dated back to ca. 2000
  - UI was refreshed in 2018
- Missing a LOT of features…
- MyGroups groups were not viewed as “trusted” for high-sensitivity things…

Group Management @ UVA

- Replaced with Grouper… why?
- Took us ~2 years to take over all groups.
- Still improving our service.
- I'm the "Grouper Guy" @ UVA



Kellen Murphy
grouper-guy@virginia.edu (also saml-guy@virginia.edu)

Overview

- Why am I here?
- **Authentication vs Authorization**
- Access Control Methods
- Grouping
  - Group Data Structures
  - Manual vs Automated
  - Attestation
  - Examples
- Q&A

AuthN vs AuthZ

"Who are you?"

"What are you allowed to do?"

- **Authentication (AuthN)**
  - Verification of the user's identity.
    - Single-factor Authentication (SFA)
    - Multi-factor Authentication (MFA)
  - Happens at the Identity Provider (IDP)

- **Authorization (AuthZ)**
  - Can happen at IDP or at Service Provider (SP)
  - Need something to distinguish what rights or privileges are associated with activity.
    - SAML Attributes!
    - OIDC Claim!
    - REST API calls!

Four Capabilities / IAM Reference Architecture

- SSO & Federation == Authentication
- Groups & Access Policy == Authorization
- AuthZ management:
  - centrally inside the IAM system (e.g. Grouper groups, defined entitlements)
  - locally managed at the resource
- AuthZ can be linked to:
  - People: Institutionally meaningful cohorts (“Groups”)
    - e.g. “IAM Engineering Staff”
  - Resources: something that dictates actions on something (“Access Policies”)
    - e.g. “Can update workflows inside the IGA platform.”

Stolen from Tom Jordan’s Monday talk. Thanks Tom! 😉

Overview

- Why am I here?
- Authentication vs Authorization
- **Access Control Methods**
- Grouping
  - Group Data Structures
  - Manual vs Automated
  - Attestation
  - Examples
- Q&A

Access Control Methods: In Theory

RBAC

Role-based Access Control

- uses “roles”
  - broad categories of users
- coarse-grained
- static

PBAC

Policy-based Access Control

- uses “policies”
  - pre-defined
  - complexity is easy
  - centralized mgmt
- fine-grained
- dynamic
- complex tools

ABAC

Attribute-based Access Control

- uses “attributes”
  - person info
  - environment info
  - sensitivity info
- fine-grained
- dynamic
- complex rules

Access Control Methods: In Practice

RBAC	PBAC	ABAC
Role-based Access Control	Policy-based Access Control	Attribute-based Access Control

- No <u>one</u> methodology fits all use cases.
  - Real-world authorization will often be a blend.

- RBAC can be difficult in higher-ed: multiple roles → role explosion
- ABAC can be hard to maintain → data completeness is key (and hard)
- PBAC requires centralized enforcement of policies → $$$

Question: Where do Groups fit into all of this?

Overview

- Why am I here?
- Authentication vs Authorization
- Access Control Methods
- **Grouping**
  - Group Data Structures
  - Manual vs Automated
  - Attestation
  - Examples
- Q&A

Where do Groups fit into all of this?

- Groups can define **roles** that are more granular than the base roles of the IAM system.
- Groups are usually surfaced as an **attribute**.

staff

↓

Information Technology Services + staff

↓

ITS + Deputy CIO + staff

↓

ITS + DCIO + Identity and Access Management + staff

↓

ITS + DCIO + IAM + Identity Engineering & Architecture + staff

description	Staff
displayName	Kellen J. Murphy
eduPersonAffiliation	employee
eduPersonAffiliation	member
eduPersonAffiliation	staff
eduPersonOrgDN	o=University of Virginia,c=US
eduPersonOrgUnitDN	ou=IT-DCIO Identity Services,o=University of Virginia,c=US
eduPersonPrimaryAffiliation	staff
eduPersonPrincipalName	wfx6yz@virginia.edu
eduPersonScopedAffiliation	employee@virginia.edu
eduPersonScopedAffiliation	member@virginia.edu
eduPersonScopedAffiliation	staff@virginia.edu
gecos	Kellen J. Murphy

LDAP attributes

iam-engineering

Group consisting of all identity and access management engineers.

Where do Groups fit into all of this?

- Groups can define **roles** that are more granular than the base roles of the IAM system.
- Groups are usually surfaced as an **attribute**.

RBAC (core role)

staff

ABAC RBAC (group)

Information Technology Services + staff

↓

ITS + Deputy CIO + staff

↓

ITS + DCIO + Identity and Access Management + staff

RBAC (group)

↓

ITS + DCIO + IAM + Identity Engineering & Architecture + staff

description	Staff
displayName	Kellen J. Murphy
eduPersonAffiliation	employee
eduPersonAffiliation	member
eduPersonAffiliation	staff
eduPersonOrgDN	o=University of Virginia,c=US
eduPersonOrgUnitDN	ou=IT-DCIO Identity Services,o=University of Virginia,c=US
eduPersonPrimaryAffiliation	staff
eduPersonPrincipalName	wfx6yz@virginia.edu
eduPersonScopedAffiliation	employee@virginia.edu
eduPersonScopedAffiliation	member@virginia.edu
eduPersonScopedAffiliation	staff@virginia.edu
gecos	Kellen J. Murphy

LDAP attributes

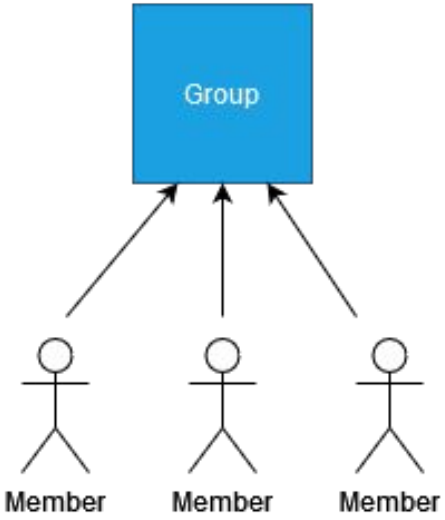
iam-engineering

Group consisting of all identity and access management engineers.

memberOf	cn=iam-dev-admins,ou=groups,o=university of virginia,c=us
memberOf	cn=iam-engineering,ou=automated,ou=groups,o=university of virginia,c=us
memberOf	cn=iam-engineering_sympa-owners,ou=personal,ou=groups,o=university of virginia,c=us
memberOf	cn=iam-harbor-projadmin,ou=groups,o=university of virginia,c=us

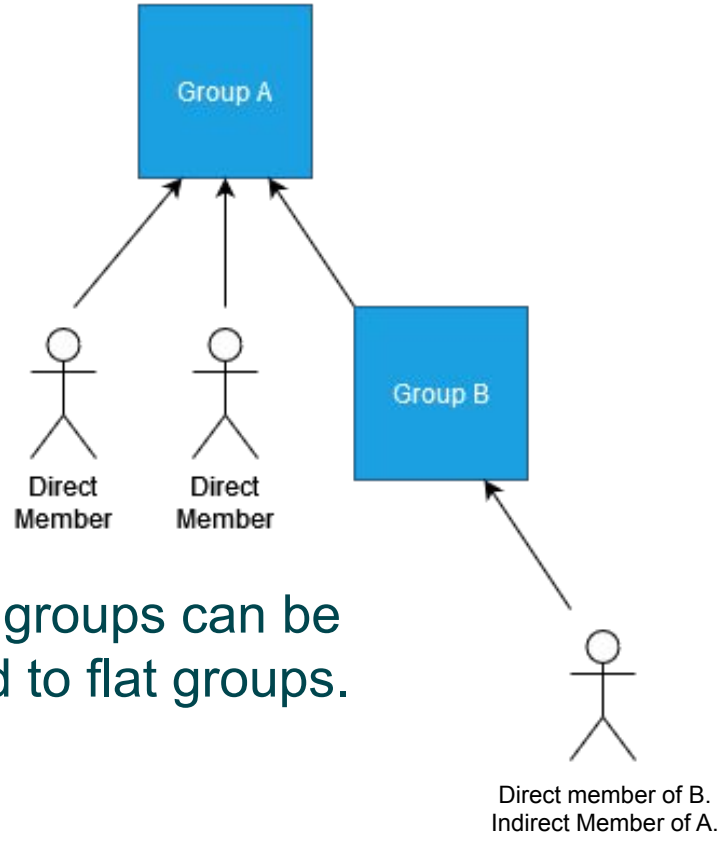
Group Data Structures

Flat



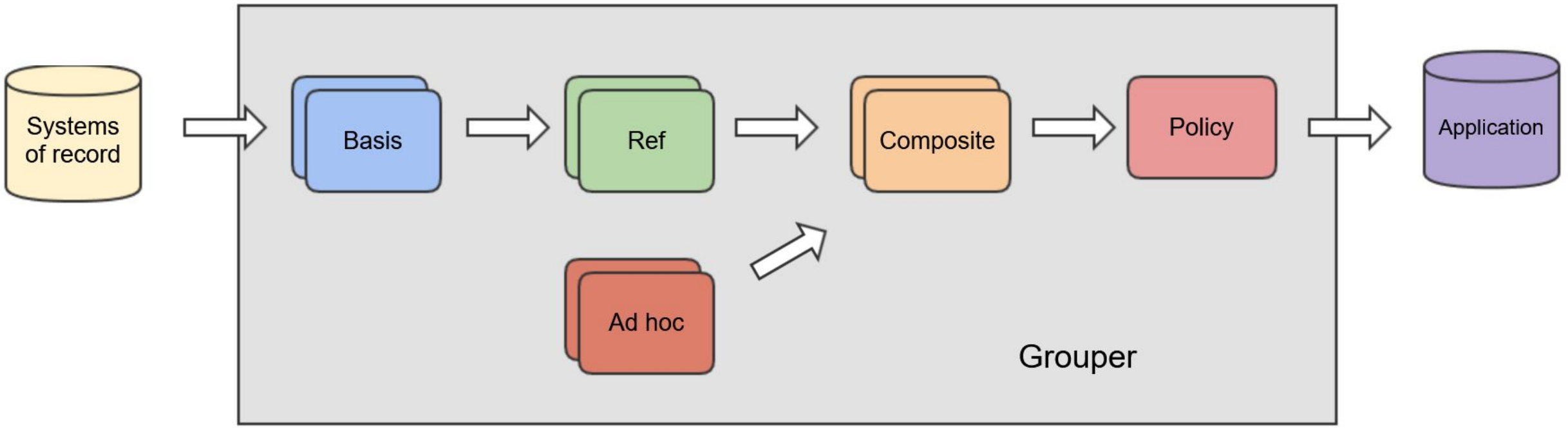
Flat groups tend to predominate in LDAP deployments.

Nested



Nested groups can be mapped to flat groups.

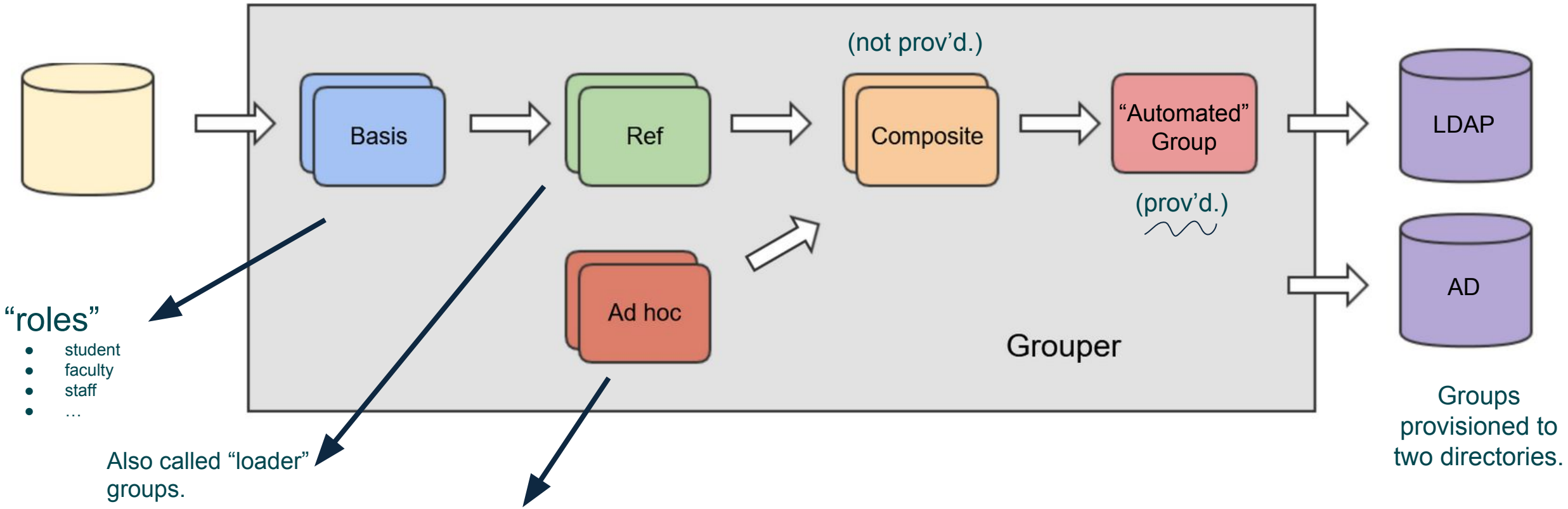
Group Data Structure (Grouper Deployment Guide)



Source: https://spaces.at.internet2.edu/display/Grouper/Folder+and+Group+Design

Any layer of these groups could be provisioned to targets.

Group Data Structure (UVA)



Our users only know that they have either an "automated" or a "person" (manual) group.

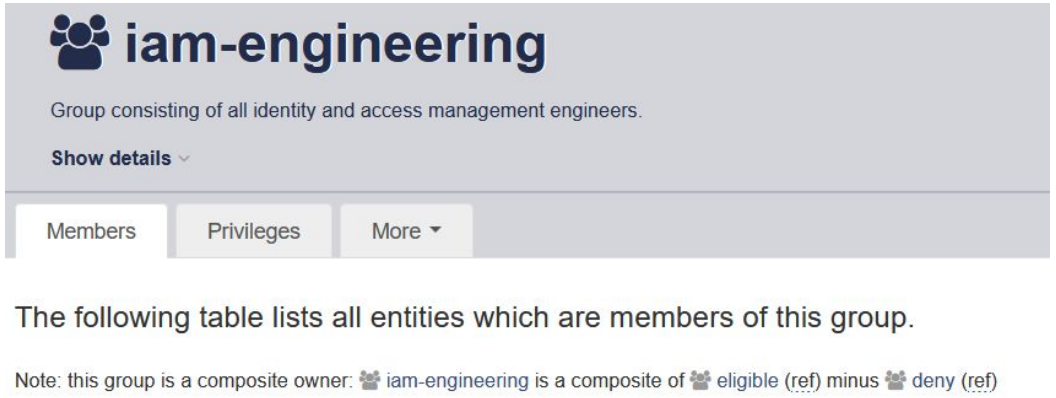
Manual vs Automated Groups

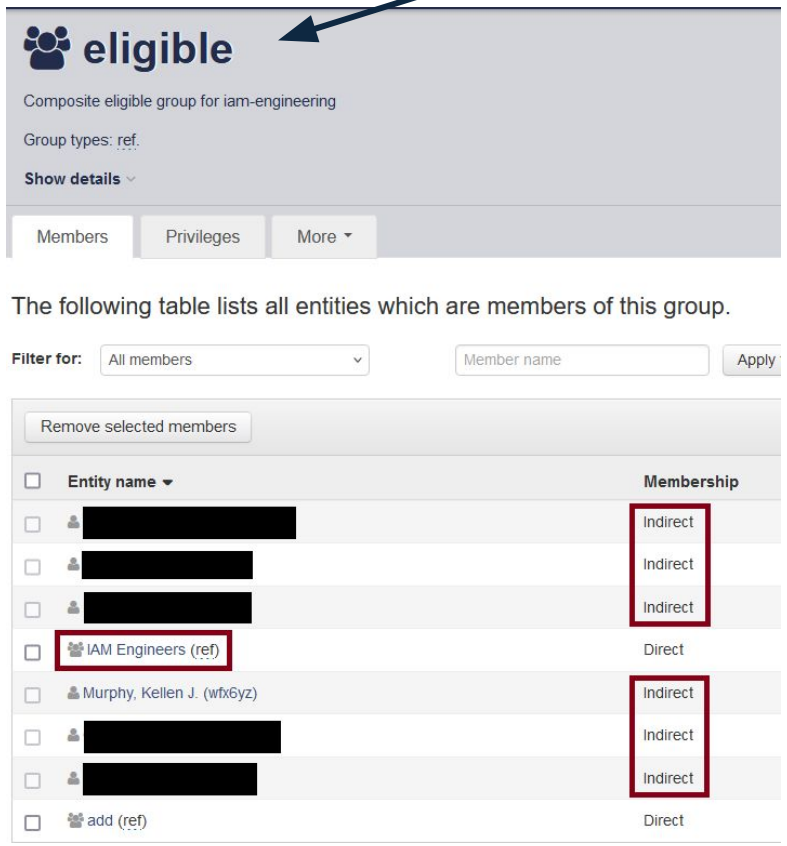
- Fully manual groups are major sources of entropy in the IAM system.
  - What happens when a member leaves the org?
  - What happens when a member joins the org?
  - What happens when an owner/updater leaves the org?

- Automated groups reduce **some** of these challenges… but:
  - What happens when there's no easy rule that captures the population that needs to be in the group?
  - Exceptions are **always** a thing!

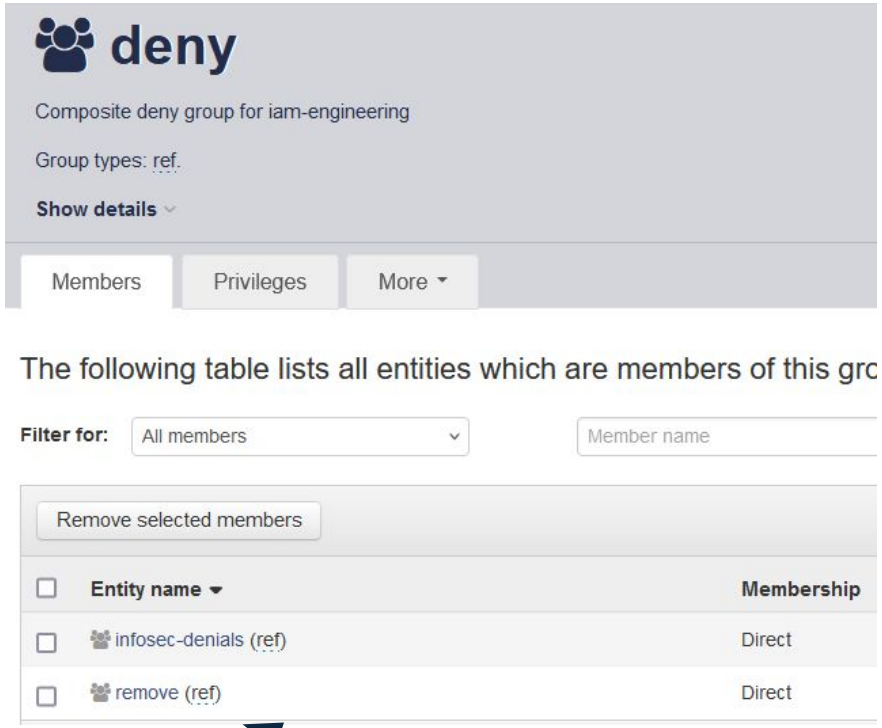
It's just set math!

group = eligible - deny
group = (reference + add) - deny
group = (reference + add) - (infosec-denials + remove)





"Reference Group"



"add" and "remove" are manual (ad-hoc)

Manual vs Automated Groups @ UVA

- Fully manual groups are major sources of entropy in the IAM system… **users demand them!** ☹️
  - What happens when a member leaves the org? **They fall out of Grouper… yay!** ✅
  - What happens when a member joins the org? **That's a group owner's problem, not mine!** ✅😃
  - What happens when an owner/updater leaves the org? **Run a report regularly for "ownerless" groups…** 😐

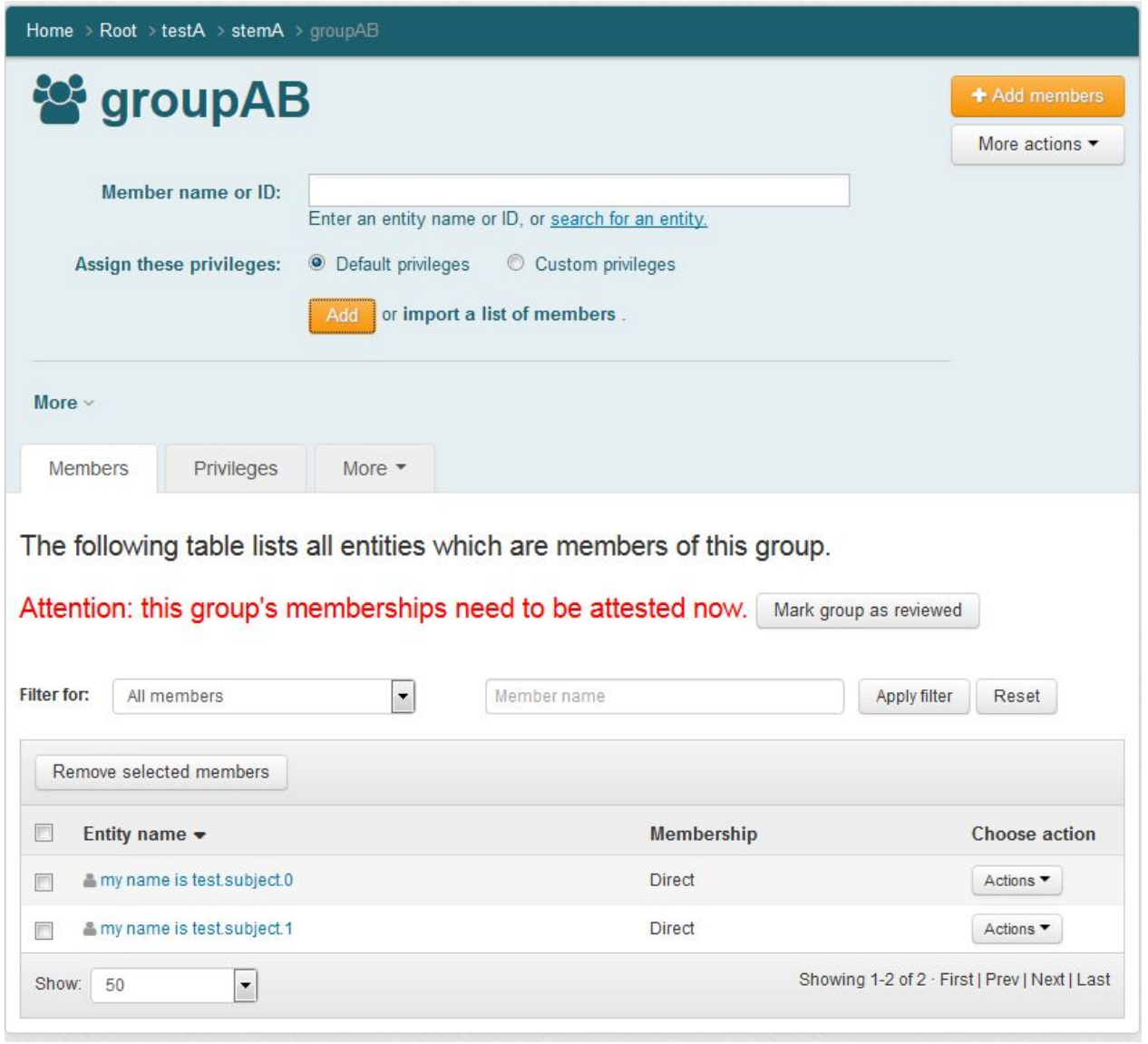
- Automated groups reduce **some** of these challenges… but:
  - What happens when there's no easy rule that captures the population that needs to be in the group?
  - Exceptions are **always** a thing!

Grouper lets us have arbitrary complexity by having multiple reference groups, composite factors, etc.

Attestation

- Requires group “owners” to declare that the group has the correct membership.

- What to do with that information?
  - Delete the group?
  - Deprovision the group?
  - Do nothing / just gathering data for later action?



Example: Using Attestation for Data Cleanup

Trigger that leads to managing the group in Grouper (enable provisioning)

Trigger that leads to purging group from target systems and deleting the group in Grouper.

Questions?

Comments?

Ready for a duck race?