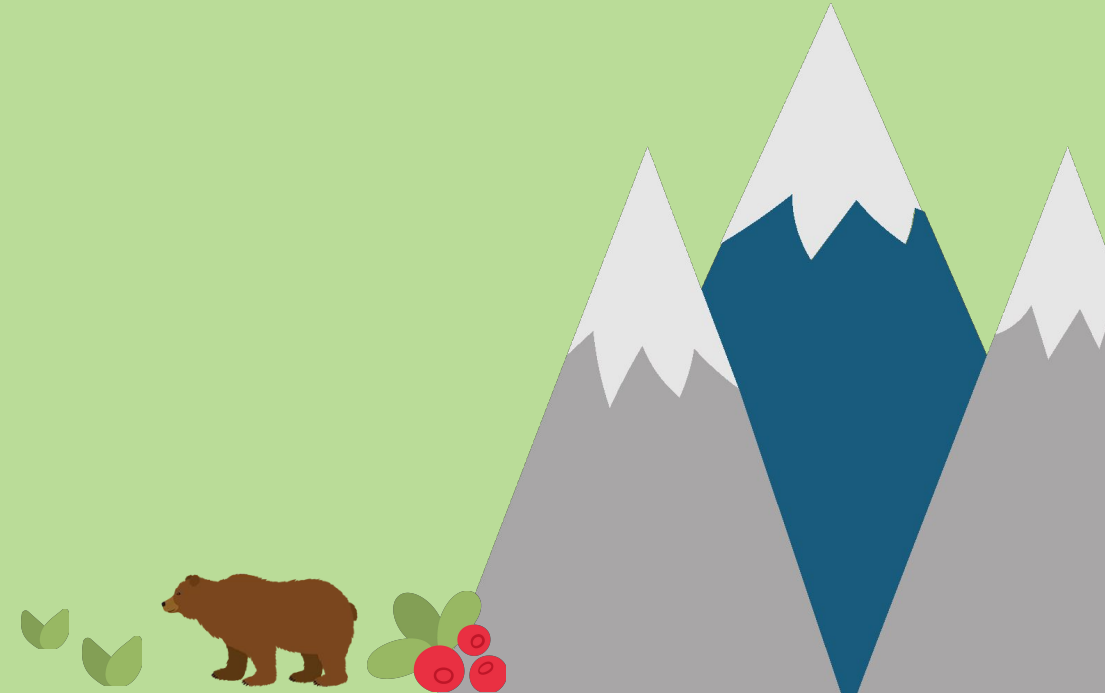




# Core Concepts of Access & Grouping

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](mailto:grouper-guy@virginia.edu) (also [saml-guy@virginia.edu](mailto:saml-guy@virginia.edu))

**Grouper Does Everything**

- Automation ✓
- Attestation ✓
- Folder structure ✓
- Metadata ✓
- API ✓
- Auditing ✓
- Containerized ✓
- Permissions ✓
- Nice UI ✓
- Pluggable Architecture? ✓

**Request new group**

**Quick links**

- My groups
- My folders
- My favorites
- My services
- My activity
- Miscellaneous

**Browse folders**

- UVA
  - Applications
  - Basis Groups
  - Group Configuration
  - Intake
  - MyGroups Attestation
  - Organizational Groups
  - Personal Groups
  - Reference Groups
  - Testing

**Home**

## Grouper

University of Virginia

This website allows you to manage groups associated with your organization and the members of those groups. For a list of answers to frequently asked questions, refer to the [support documentation](#).

### Recent activity

| Recent activity   | Activity Date       |
|---|---------------------|
| Added Cox, Brennan (bhc8t) as a member of the ad-hoc additions (app) group. | 2023/07/17 3:41 PM  |
| Added group foo (app).  | 2023/07/03 11:22 AM |
| Added attribute value to attribute attestationCalculatedDaysLeft.           | 2023/05/26 1:39 PM  |
| Added attribute attestationCalculatedDaysLeft to an attribute assignment.   | 2023/05/26 1:39 PM  |
| Added attestation on group AT_stacs-jira-iam-agents .                       | 2023/05/26 1:39 PM  |
| Added attribute value to attribute attestationHasAttestation.               | 2023/05/26 1:39 PM  |

### My memberships

- authorized
  - Applications : ITS : IAM : Grouper (app)
- eligible
  - Applications : ITS : IAM : Grouper : rules (app)
- staff
  - Basis Groups (basis)
- grouperUIUserData
  - Group Configuration : grouperUI (etc)
- sysadmingroup
  - Group Configuration (etc)
- uvaPrivilegedViewers
  - Group Configuration : uvaViewsConfig (etc)
- AT\_stacs-jira-iam-agents
  - MyGroups Attestation

### Groups I manage

- foo
  - Applications (app)
- authorized
  - Applications : ITS : IAM : Grouper (app)
- ad-hoc additions
  - Applications : ITS : IAM : Grouper : rules : additions (app)
- eligible
  - Applications : ITS : IAM : Grouper : rules (app)
- ad-hoc removals
  - Applications : ITS : IAM : Grouper : rules : removals (app)
- all removals
  - Applications : ITS : IAM : Grouper : rules : removals (app)

### Recently used

- ad-hoc additions
  - Applications : ITS : IAM : Grouper : rules : additions (app)
- foo
  - Applications (app)
- AT\_stacs-jira-iam-agents
  - MyGroups Attestation
- stacs-jira-iam-agents
  - MyGroups Attestation
- Chris Group
  - Personal Groups
- MyGroups Attestation
  - UVA
- ops\_testing\_template\_demo
  - Testing (test)

# 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

Role-based Access Control

## PBAC

Policy-based Access Control

## ABAC

Attribute-based Access Control

- No one 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 → \$\$\$

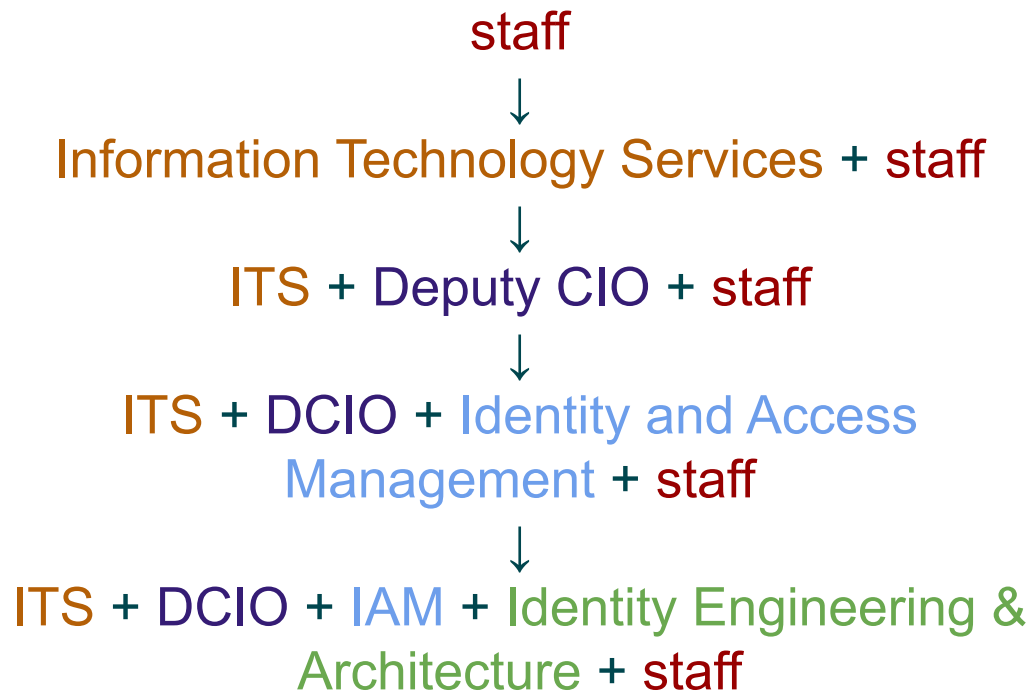
**Question: Where do Groups fit into all of this?**

# 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**.



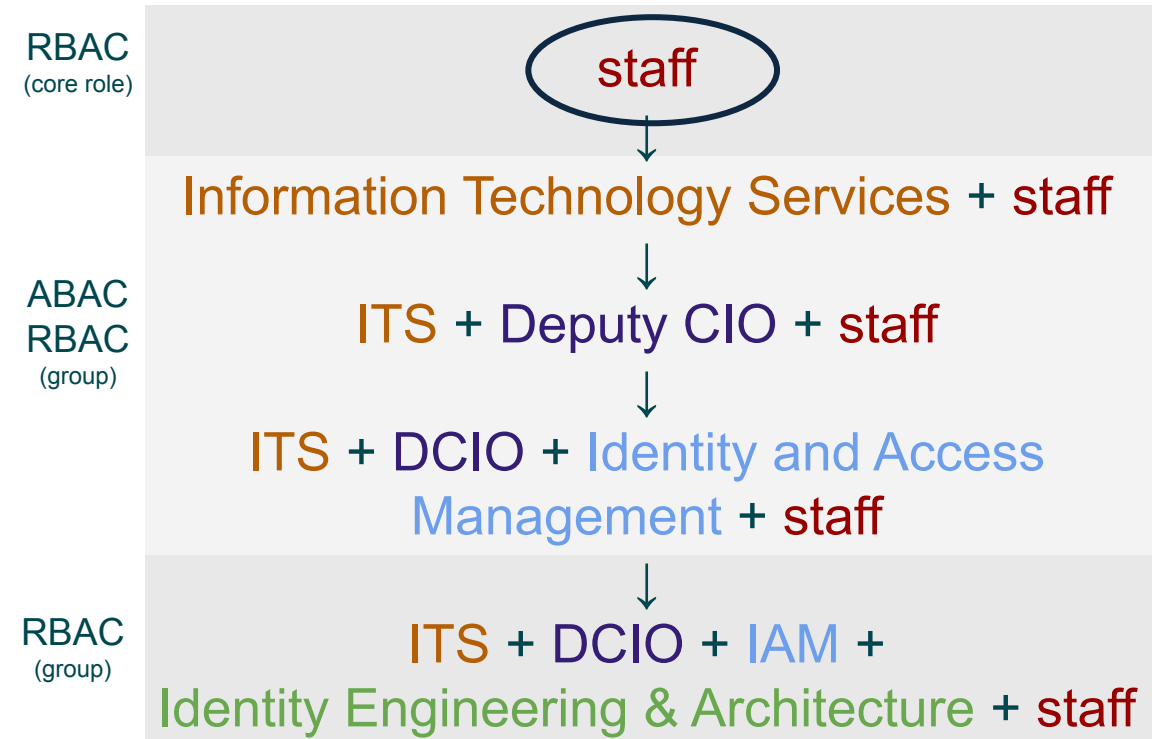
|                             |  |
|-----------------------------|--|
| description                 | Staff  |
| displayName                 | Kellen J. Murphy   |
| eduPersonAffiliation        | employee   |
| eduPersonAffiliation        | member   |
| eduPersonAffiliation        | staff  |
| eduPersonOrgDN              | 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



# 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**.



|                             |  |
|-----------------------------|--|
| 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   |

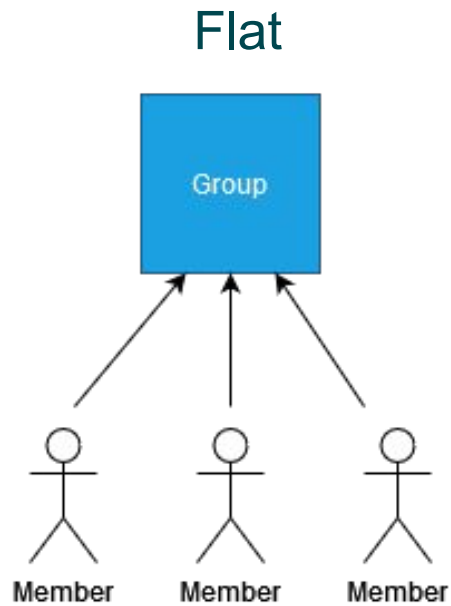
LDAP attributes



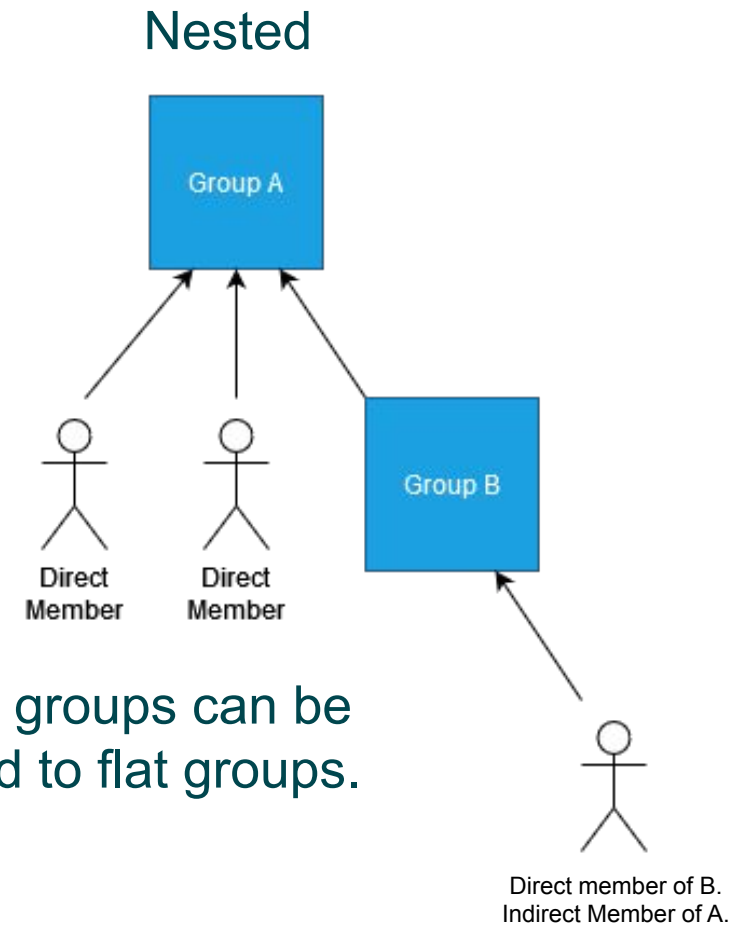
Group consisting of all identity and access management engineers.

|          |   |
|----------|---|
| 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                     |
| memberOf | cn=iam-cc0634,ou=automated,ou=groups,o=university of virginia,c=us                  |

# Group Data Structures

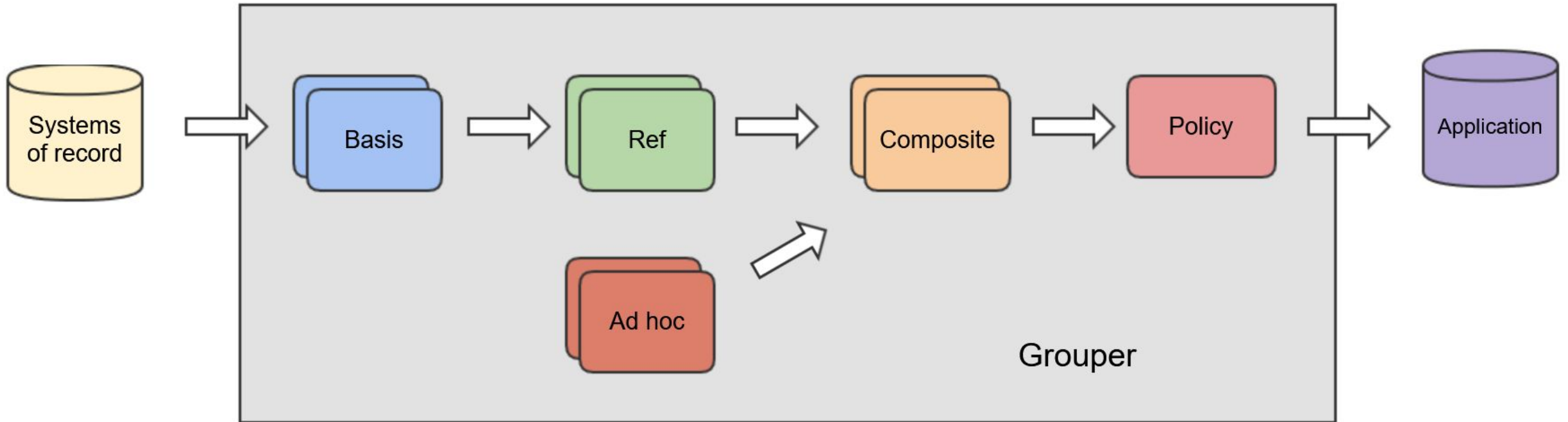


Flat groups tend to predominate in LDAP deployments.



Nested groups can be mapped to flat groups.

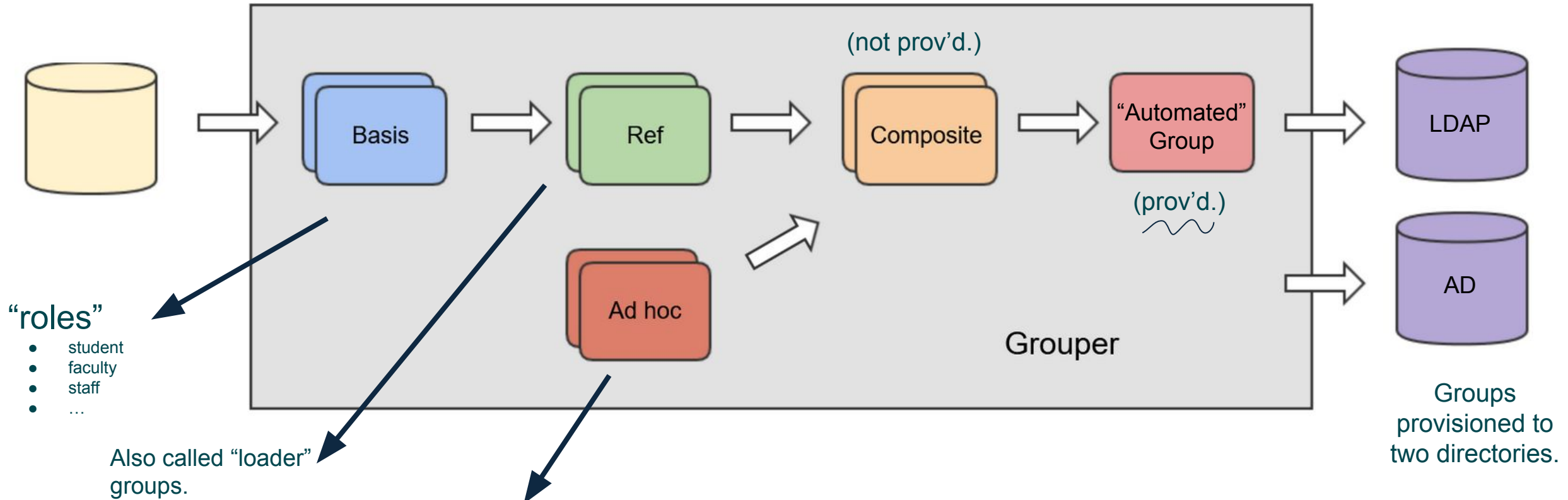
# Group Data Structure (Grouper Deployment Guide)



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!

# iam-engineering

Group consisting of all identity and access management engineers.

Show details

Members Privileges More

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

Note: this group is a composite owner: iam-engineering is a composite of eligible (ref) minus deny (ref)

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

Filter for: All members Member name Apply

Remove selected members

| Entity name                | Membership |
|----------------------------|------------|
| [redacted]                 | Indirect   |
| [redacted]                 | Indirect   |
| [redacted]                 | Indirect   |
| IAM Engineers (ref)        | Direct     |
| Murphy, Kellen J. (wfxGyz) | Indirect   |
| [redacted]                 | Indirect   |
| [redacted]                 | Indirect   |
| add (ref)                  | Direct     |

“Reference Group”

## It's just set math!

$$\text{group} = \text{eligible} - \text{deny}$$

$$\text{group} = (\text{reference} + \text{add}) - \text{deny}$$

$$\text{group} = (\text{reference} + \text{add}) - (\text{infosec-denials} + \text{remove})$$

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

Filter for: All members Member name

Remove selected members

| Entity name           | Membership |
|-----------------------|------------|
| infosec-denials (ref) | Direct     |
| remove (ref)          | Direct     |

“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?

Home > Root > testA > stemA > groupAB

**groupAB** + Add members More actions ▾

Member name or ID:   
Enter an entity name or ID, or [search for an entity](#).

Assign these privileges:  Default privileges  Custom privileges

Add or import a list of members .

More ▾

Members Privileges More ▾

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

**Attention: this group's memberships need to be attested now.** Mark group as reviewed

Filter for:   Apply filter Reset

Remove selected members

| <input type="checkbox"/> Entity name ▾             | Membership | Choose action          |
|--|------------|------------------------|
| <input type="checkbox"/> my name is test.subject.0 | Direct     | <span>Actions ▾</span> |
| <input type="checkbox"/> my name is test.subject.1 | Direct     | <span>Actions ▾</span> |


Show:  Showing 1-2 of 2 · First | Prev | Next | Last

# Example: Using Attestation for Data Cleanup

Home > UVA > Nonprovisioned MyGroups (Attestation Due June 6) > EA-Fall-Patching-2017 > EA-Fall-Patching-2017

## EA-Fall-Patching-2017

Enterprise Applications Fall Patching 2017

This group is managed by loader group  MyGroups Members Loader Group. It was last fully loaded on Mon Sep 16 19:09:39 EDT 2024. Summary is: total: 18, inserted: 0, deleted: 0, updated: 0

Show details ▾

Members

Privileges

More ▾

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

**ATTESTATION - This group's status needs to be confirmed:**

Active (Keep)

Inactive (Delete)

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?

