



Grouper in Action

Access Management Strategies for Higher Education and Research TIER Grouper Deployment Guide

Bill Thompson, CISSP, CSSLP, GSLC
Director Digital Infrastructure
Lafayette College

NIST Special Publication 800-162

Guide to Attribute Based Access Control (ABAC) Definition and Considerations

Vincent C. Hu
David Ferraiolo
Rick Kuhn
Adam Schnitzer
Kenneth Sandlin
Robert Miller
Karen Scarfone

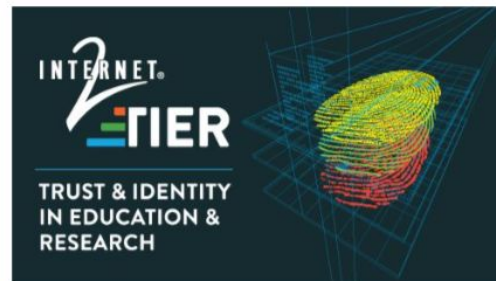
<http://dx.doi.org/10.6028/NIST.SP.800-162>

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

TIER Grouper Deployment Guide

Version 1.0 2017-04-21



Repository ID: TI.25.1

Authors: James Babb
Tom Dopirak
Bill Thompson, Editor
TIER API and Entity Registry WG
Grouper Development Team

Sponsor: Internet2

Superseded documents: (none)

Proposed future review date: April 2018

Subject tags: Grouper, access management, authorization, access control, access control model, access control policy

© 2017 Internet2

This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Why do we need a guide?

- [“Better documentation will make your project more successful”](#) – Daniele Procida
- Four distinct types/purposes:
 - Tutorials – learn by doing, getting started, repeatable, concrete
 - How-to guides – series of steps, specific real goal/problem, some flexibility
 - Reference – technical description, information oriented, accuracy
 - **Discussions – context, explaining why, multiple examples**
- <https://www.divio.com/en/blog/documentation/>

TIER Grouper Deployment Guide

“The goal of this document is to help you come up to speed on Grouper concepts, how they relate to identity and access management, and how they can be deployed to implement effective access control in a wide variety of situations.”

Section 3 Understanding Grouper

Section 4 Installing Grouper

Section 5 TIER Folder and Group Design

Section 6 Access Control Models

Section 7 Provisioning

Section 8 Operational Considerations

Section 9 Conclusion

Appendix A Example policies

Appendix B Acknowledgements

Terminology

- [NIST 800-162 ABAC](#)
- [Grouper glossary](#)
- [Grouper UI terminology](#)

Grouper Specific

- **Direct membership** – subject added directly to a group’s membership list
- **Indirect membership** – subject is a member by virtue of membership in another group
- **Composite group** - combining two other groups to form a third group

TIER Access Management

- **Basis group** – direct subject membership, low level, “raw” groups
- **Reference group** – institutionally meaningful cohorts - aka subject attributes
- **Access/Account policy group** – pre-computed policy decision

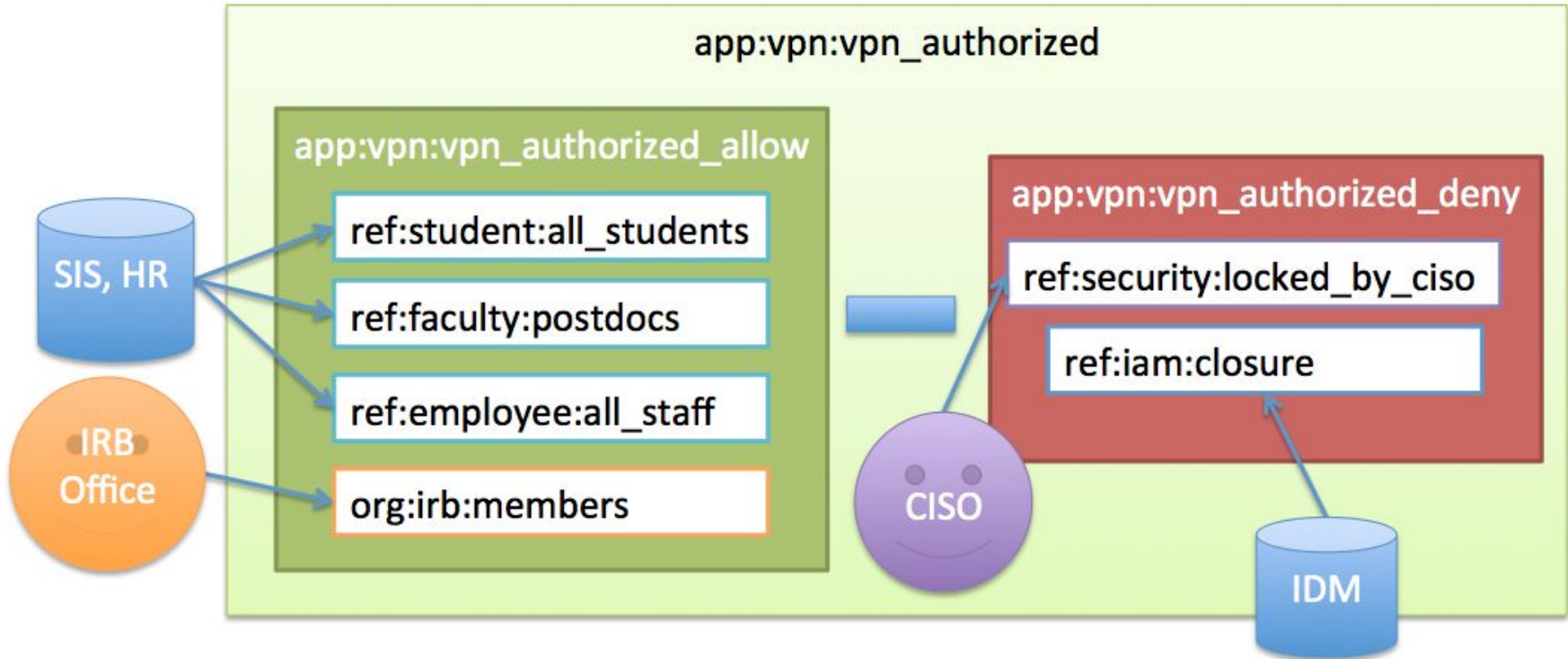
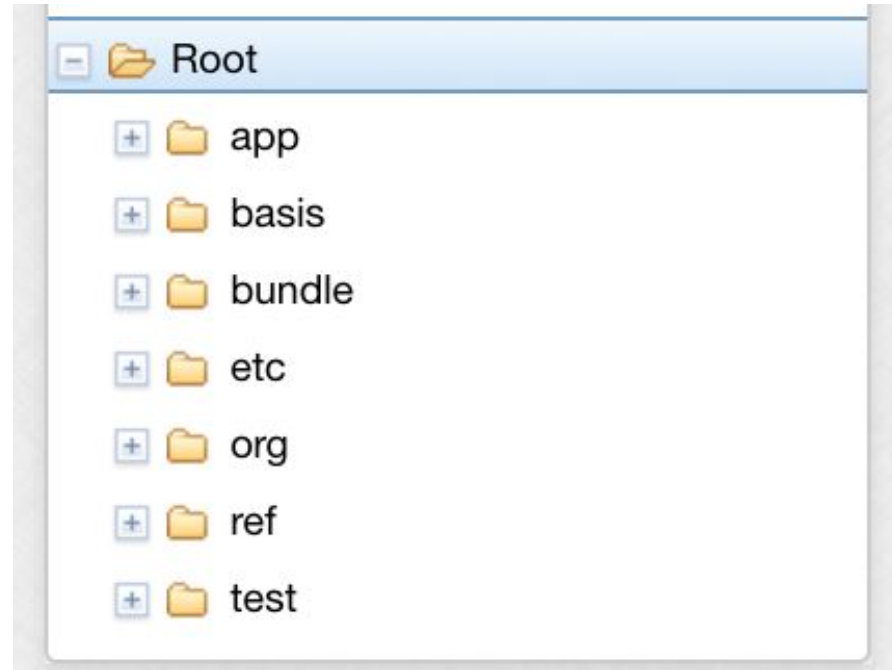


Figure 1: University of Chicago VPN Access Policy

TIER Folder and Group Design

"Just having a plan or standard has been quite helpful, as it allows implementers to get on with real work without having to stumble on how to name things or where to stick them."

- Tom Barton



TIER Folder and Group Design

- **etc:** - Grouper configuration, administrative access control groups, and loader jobs
- **basis:** - groups used exclusively by the IAM team to build reference groups
- **ref:** - reference groups, institutional meaningful cohorts - “truth”
- **bundle:** - sets of reference groups used in policy for many services
- **app:** - enterprise applications access control policy - specific policy for a service
- **org:** - delegated authority, ad-hoc groups, org “owned” apps or reference groups
- **test:** - test folder for system verification

TIER Folder and Group Design

Basis Groups - Systems of record codes (hidden away from access policy)

- **basis:hris:{employee_codes}**
- **basis:sis:{student_codes}**

Reference Groups - Institutionally meaningful cohorts – “truth” (aka subject attributes)

- **ref:role:** - institutional scope roles (e.g. president, provost, chaplain...)
- **ref:employee:** - types of employees (faculty, staff, part-time, full-time...)
- **ref:student:** - types of students

Access Policy Groups - digital policy based on subject attributes

- **app:vpn:vpn_allow** - allow policy for vpn access

Bundle Groups - Sets of reference groups (cohorts) used to drive access policy

- **bundle:employee_services** - cohorts that get employee-like access

vpn_allow

Trace membership for thompsov

thompsov is a member of the *vpn_allow* group by the following paths:

thompsov is a **direct member** of

- ⊕ [ref:dept:its:di](#) ← Reference group - aka subject attribute
 - ⊕ which is a **direct member** of
 - ⊕ [app:vpn:vpn_roles:netadmins_allow](#) ← Subject attribute to application role mapping
 - ⊕ which is a **composite factor** minus [netadmins_deny](#) of
 - ⊕ [app:vpn:vpn_roles:netadmins](#) ← Application specific role
 - ⊕ which is a **direct member** of
 - ⊕ [app:vpn:vpn_allow](#) ← Access policy group

thompson is a **direct member** of

⊕ `ref:employee:admin_ft` ← Reference group - aka subject attribute

⊕ which is a **direct member** of

⊕ `ref:employee:employee` ← Reference group - aka subject attribute

⊕ which is a **direct member** of

⊕ `bundle:employee_services:employee_services_include` ← Subject attribute to service bundle mapping

⊕ which is a **composite factor** minus `employee_services_exclude` of

⊕ `bundle:employee_services:employee_services` ← Institution wide service bundle

⊕ which is a **direct member** of

⊕ `app:vpn:vpn_roles:facstaff_allow` ← Subject to role mapping

⊕ which is a **composite factor** minus `facstaff_deny` of

⊕ `app:vpn:vpn_roles:facstaff` ← Application specific role

⊕ which is a **direct member** of

⊕ `app:vpn:vpn_allow` ← Access policy group

vpn_allow

+ Add members

More actions ▾

VPN net inclusions.

More ▾

Members

Privileges

More ▾

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

Filter for: Has direct membership ▾

Member name

Apply filter

Reset

Remove selected members

<input type="checkbox"/> Entity name ▾	Membership	
<input type="checkbox"/>  ad_hoc_vpn_access	Direct	Actions ▾
<input type="checkbox"/>  facstaff	Direct	Actions ▾
<input type="checkbox"/>  netadmins	Direct	Actions ▾
<input type="checkbox"/>  Service Managers	Direct	Actions ▾

Show: 50 ▾

Showing 1-4 of 4 · First | Prev | Next | Last

VPN access is granted to all faculty, staff, network administrators, service managers, and...exceptions.

ad_hoc_vpn_access

+ Add members

More actions ▾

More ▾

Members

Privileges

More ▾

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

Filter for:

Remove selected members

<input type="checkbox"/> Entity name ▾	Membership	
<input type="checkbox"/> consultant_service_mgrs	Direct	<input type="button" value="Actions ▾"/>
<input type="checkbox"/> resources_require_vpn	Direct	<input type="button" value="Actions ▾"/>
<input type="checkbox"/> TheLaf Editors	Direct	<input type="button" value="Actions ▾"/>
<input type="checkbox"/> vpn_cozzubbm	Direct	<input type="button" value="Actions ▾"/>
<input type="checkbox"/> vpn_fechikkm	Direct	<input type="button" value="Actions ▾"/>
<input type="checkbox"/> vpn_hendrihe	Direct	<input type="button" value="Actions ▾"/>
<input type="checkbox"/> vpn_keeslerr	Direct	<input type="button" value="Actions ▾"/>
<input type="checkbox"/> vpn_meyerj	Direct	<input type="button" value="Actions ▾"/>

FOLDER
app : vpn : ref : VPN Access
Student researchers under Heidi P. Hendrickson, Assistant Professor of Chemistry

← Managed exceptions.
Delegated to appropriate people.

employee_services

+ Add members

More actions ▾

More ▾

Members

Privileges

More ▾

The following table lists all groups in which this group is a member.







Filter for: All groups ▾

Group name

Apply filter

Reset

Remove from selected groups

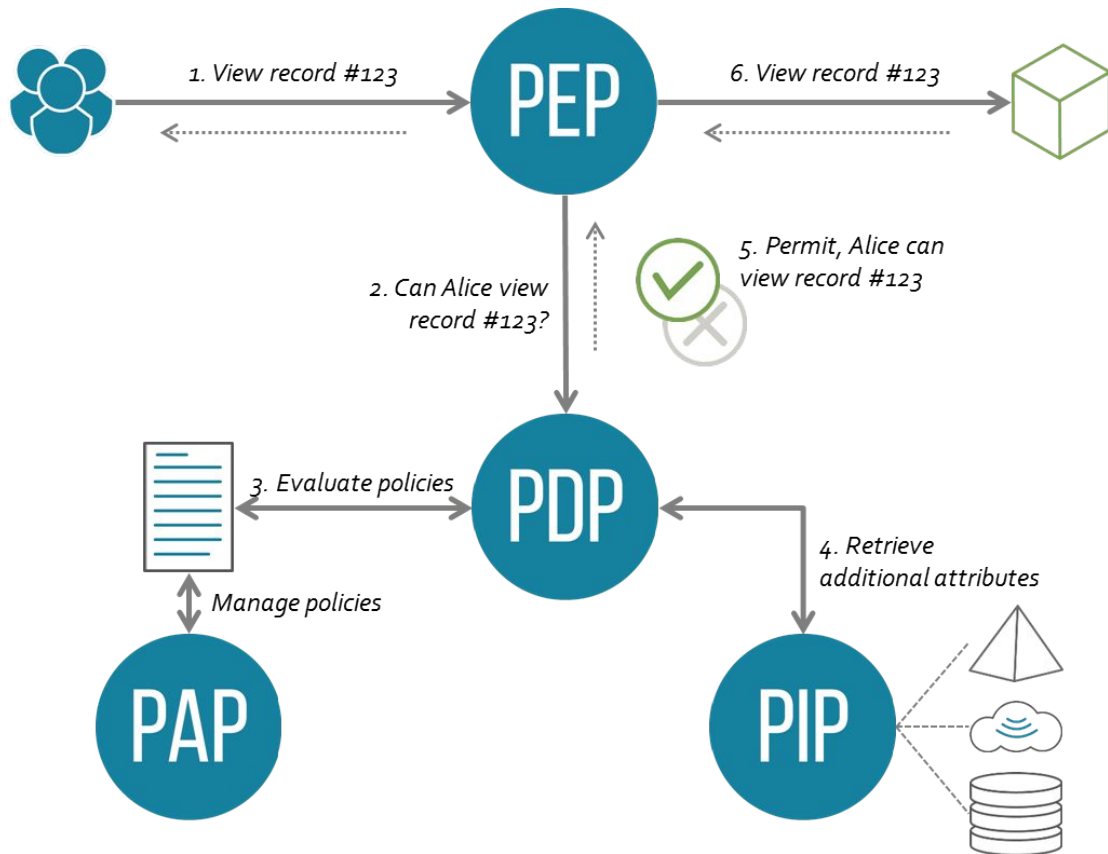
<input type="checkbox"/>	Folder	Group	Membership	
<input type="checkbox"/>	lc : app : COmanage	 sponsors_allow	Direct	Actions ▾
<input type="checkbox"/>	lc : app : crashplan	 cp_allow	Direct	Actions ▾
<input type="checkbox"/>	lc : app : google	 googledocs_include	Direct	Actions ▾
<input type="checkbox"/>	lc : app : Library Services	 library_services_allow	Direct	Actions ▾
<input type="checkbox"/>	lc : app : papercut	 papercut_allow	Direct	Actions ▾
<input type="checkbox"/>	lc : app : vpn : vpn_roles	 facstaff_include	Direct	Actions ▾

FOLDER
lc : app : Library Services
Subjects in this group are eligible to use library services.

Bundle group provides a mechanism to manage employee-like access.

TIER Access Control Models

- Access Control Model 1 – Grouper Subject Attributes
- Access Control Model 2 – Grouper as PAP and PDP
- Access Control Model 3 – Application RBAC User to Role Mapping
- Access Control Model 4 – WebSSO Short-circuit

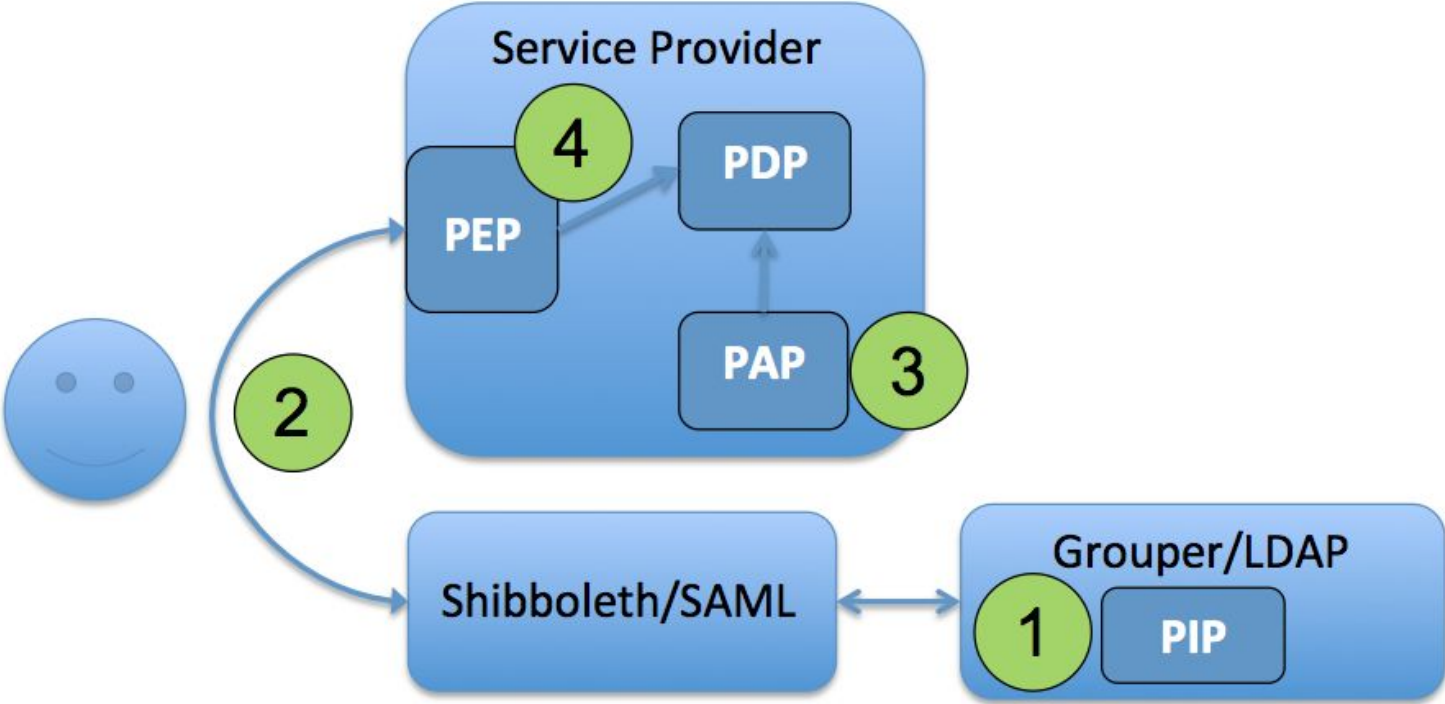


By Axiomatics (Axiomatics) [CC BY 3.0 (<http://creativecommons.org/licenses/by/3.0/>)], via Wikimedia Commons

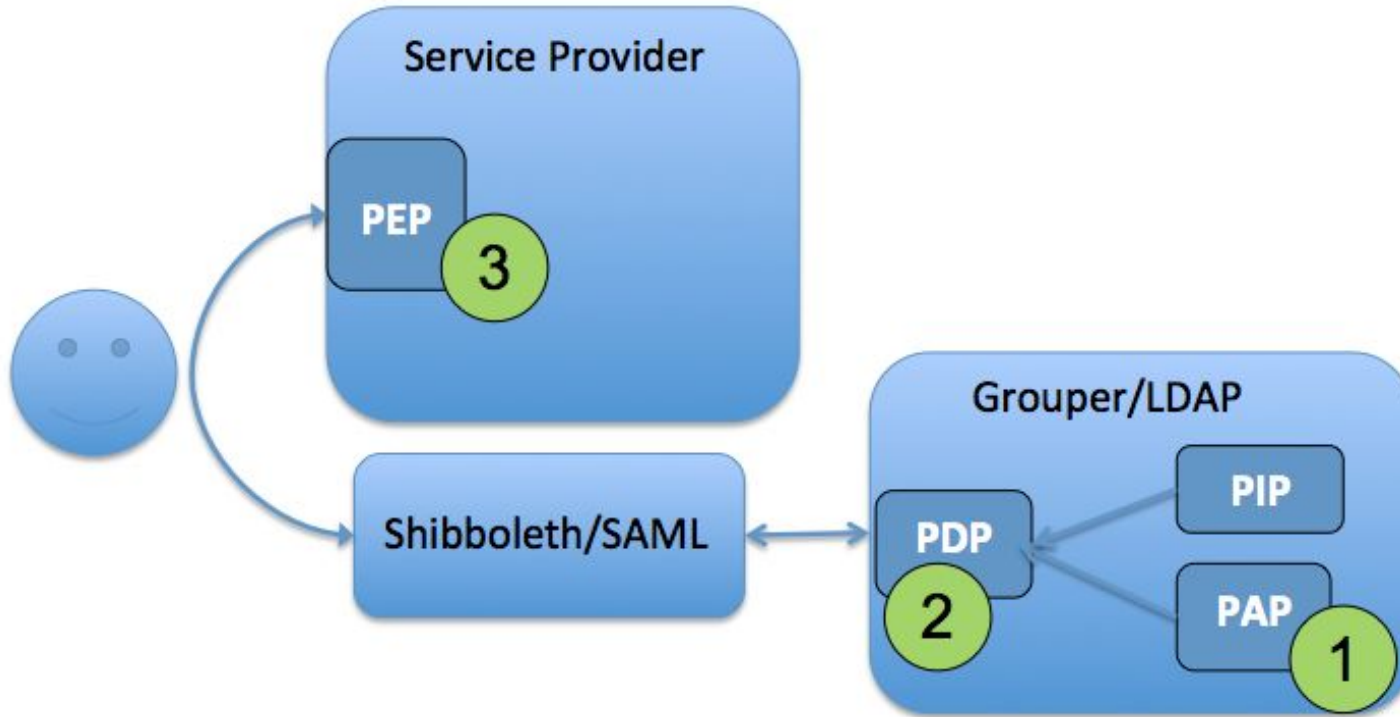
PAP - Policy Administration Point
 PDP - Policy Decision Point

PEP - Policy Enforcement Point
 PIP - Policy Information Point

Access Control Model 1 – Grouper Subject Attributes - eduPersonAffiliation



Access Control Model 2 – Grouper as PDP and PIP - eduPersonEntitlement



library_services_allow

+ Add members

More actions ▾

Subjects in this group are eligible to use library services.

More ▾

Members

Privileges

More ▾

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

Filter for:

Has direct membership ▾

Member name

Apply filter

Reset

Remove selected members

Entity name ▾

 ad_hoc_library_services

 employee_services

 service_accounts

 students

FOLDER

app : Library Services : ref

A manually maintained cohort of ad-hoc members who should have access to library services.

Membership

Direct

Actions ▾

Direct

Actions ▾

Direct

Actions ▾

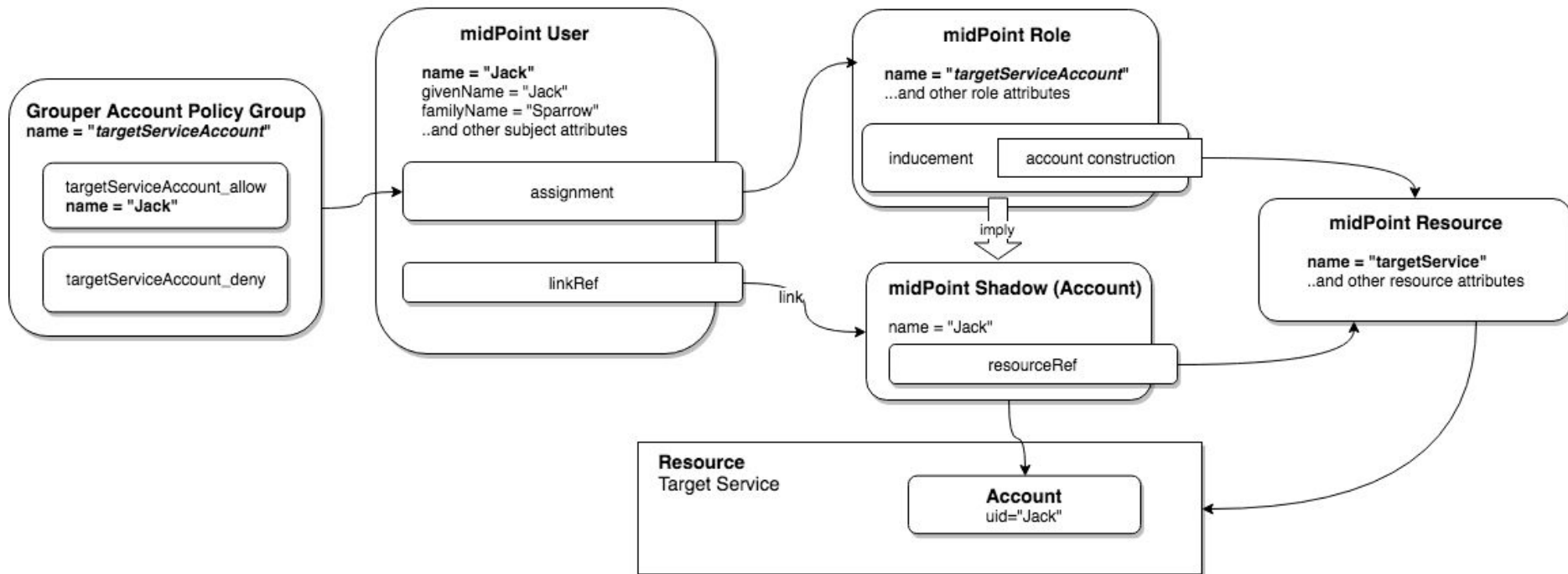
Direct

Actions ▾

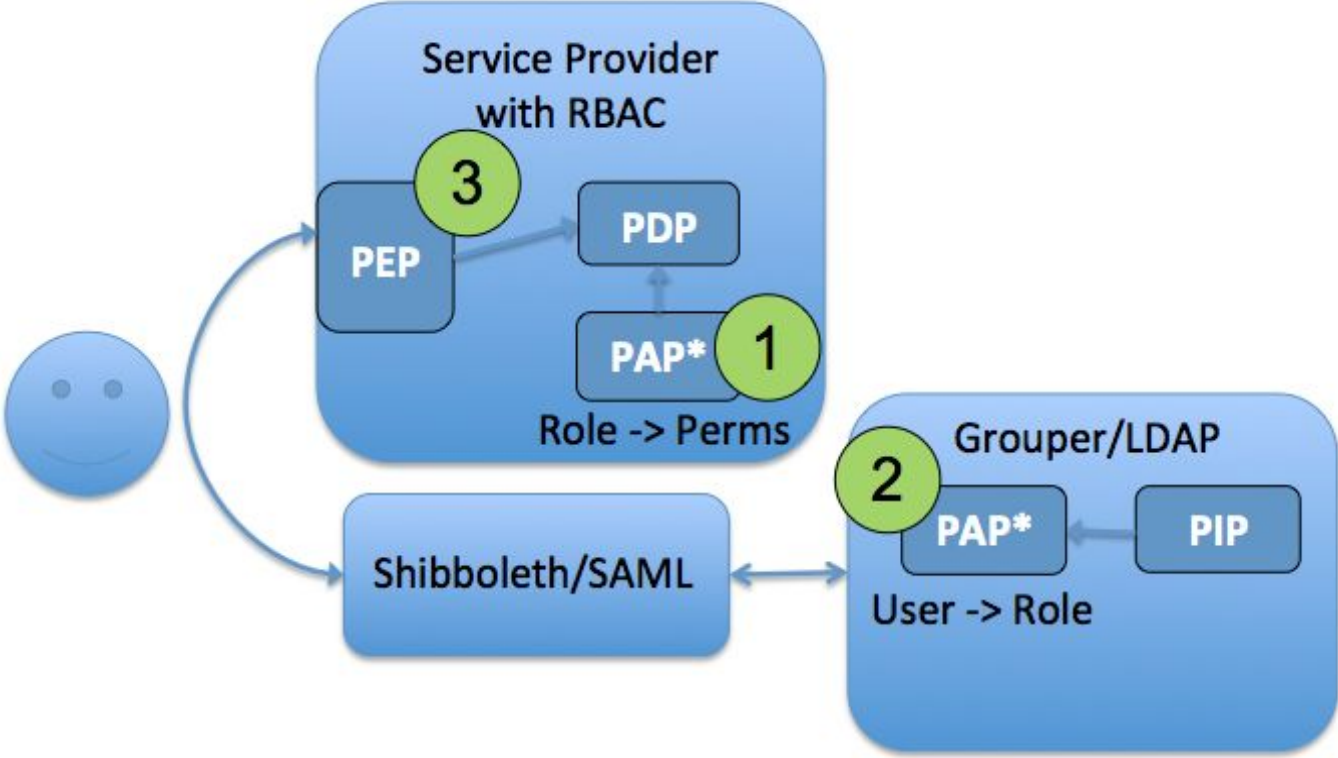
Show: 50 ▾

Showing 1-4 of 4 · First | Prev | Next | Last

TIER Account Provisioning via Grouper and midPoint



Access Control Model 3 – RBAC User to Role Mapping



exports

Edit folder

More actions ▾

More ▾

Folder contents

Privileges

Filter for:

Apply filter

Reset

Name ▾

^ Up one folder

advising_fullstaff

adv_career_services

athletics_fullstaff

rct_tools_ods_analytics_user

abroad_fullstaff

access_fullstaff

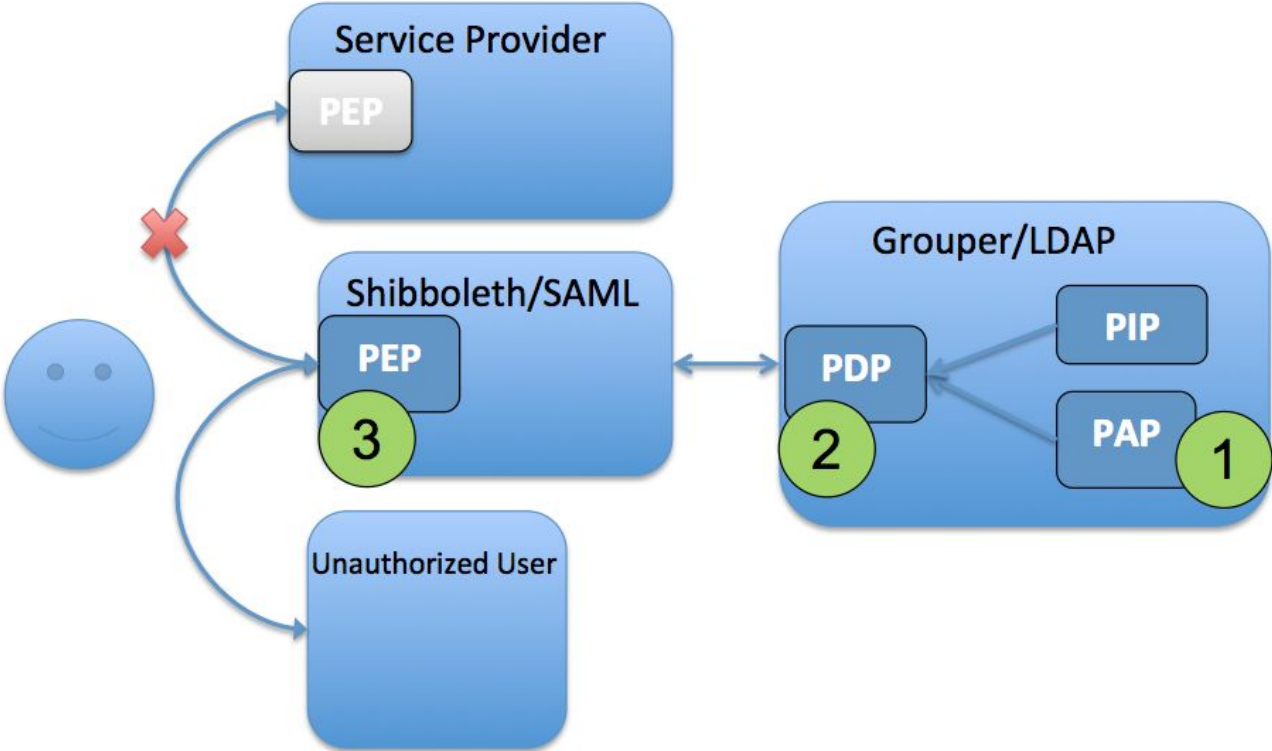
adm_report_manager

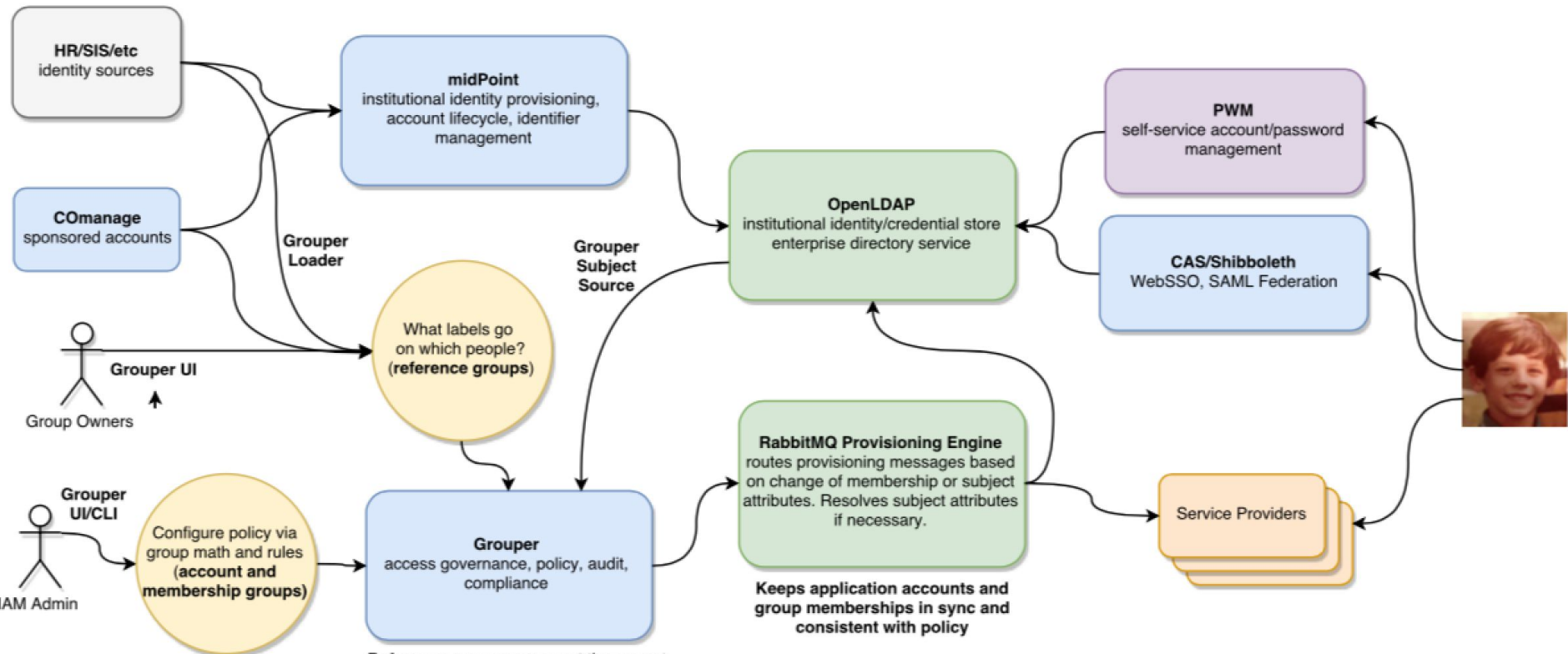
adm_tools_ods_analytics_user

adv_alum_relations

adv_annual_fund

Access Control Model 4 – WebSSO Short-circuit





Account and membership groups represent authorization policy. Effective membership configured via group math or rules generates change notifications.

Reference groups represent the current state of membership for all subjects as known to the enterprise. They are used to configure access management policy and provide the means for automated provisioning of groups and accounts as well as audit and compliance.

TIER Subject Attribute Management and Access Governance

- Consistent model and terminology
 - Basis → reference → policy
 - Reference groups = subject attributes (institutionally meaningful cohorts)
 - Policy groups can implement ABAC, RBAC, and ACLs
- Strategy applies to all four access control models
- Policy is more organized, discoverable, manageable, and auditable
- Management of policy easy, flexible, and can be delegated
- Improved security posture and ability to onboard new services quickly



Thanks!

Bill Thompson, CISSP, CSSLP, GSLC
thompso@lafayette.edu
Director Digital Infrastructure
Lafayette College