INTERNET2®

2017 TECHNOLOGY exchange

SAN FRANCISCO CA OCTOBER 15-18

INTERNET2® TIER

TRUST & IDENTITY IN EDUCATION & RESEARCH

Grouper in Action

Access Management Strategies for Higher Education and Research

Chris Hyzer, University of Pennsylvania
Bert Bee-Lingren, Georgia Institute of Technology
Bill Thompson, Lafayette College
Carl Waldbieser, Lafayette College

Agenda

- Grouper – Chris Hyzer
- TIER Grouper Deployment Guide – Bill Thompson

- Morning Break 10:00 – 10:30

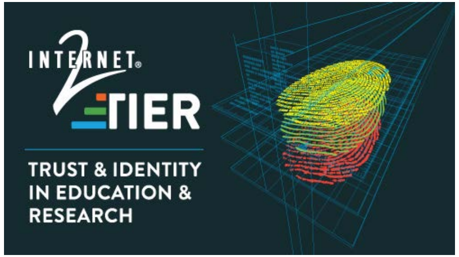
- Grouper in Action: Lafayette College – Carl Waldbieser
- Grouper in Action: Georgia Tech – Bert Bee-Lingren

- TIER Grouper Package – Chris Hubing
- Open Q&A

TIER Grouper Deployment Guide

Bill Thompson

Director Digital Infrastructure, Lafayette College



James Babb
Tom Dopirak
TIER API and Entity Registry WG
Grouper Development Team
Community Contributions

Albert Wu - UCLA
Bert Bee-Lindgren - Georgia Tech
Bill Kaufman - Internet2
Bill Thompson - Lafayette College
Brian Savage - Boston College
Brian Woods - Rice
Carey Black - The Ohio State University
Chris Hyzer - Penn
Dean Lane - Rice
Emily Eisbruch - Internet2
Eric Goodman - UCOP
Ethan Disabb - University of Florida
Ethan Kromhout - UNC Chapel Hill
Gabor Eszes - Old Dominion
Gary Brown- University of Bristol
Harry Samuels - Northwestern
James Babb - UW Madison
Jill Gemmill - Clemson
Jim Fox - University of Washington
Tom Jordan - UW Madison
Tom Zeller
Warren Curry - University of Florida

Jon Finke - RPI
Jon Miner - UW Madison
José Cedeño - Oregon State University
Keith Hazelton - UW Madison
Keith Wessel - University of Illinois
Ken Koch - Washington University
Maarten Kremers - SURFnet
Mark McCahill - Duke
Michael Gettes - Penn State
Michael Hodges - University of Hawaii
Mike Zawacki - Internet2
Paul Caskey - Internet2
Raoul Sevier - Harvard
Rob Carter - Duke
Scott Cantor - The Ohio State University
Shilen Patel - Duke
Steve Carmody - Brown
Steve Moyer - Penn State
Steve Zoppi - Internet2
Tom Barton - University of Chicago
Tom Dopirak - “Retirement”

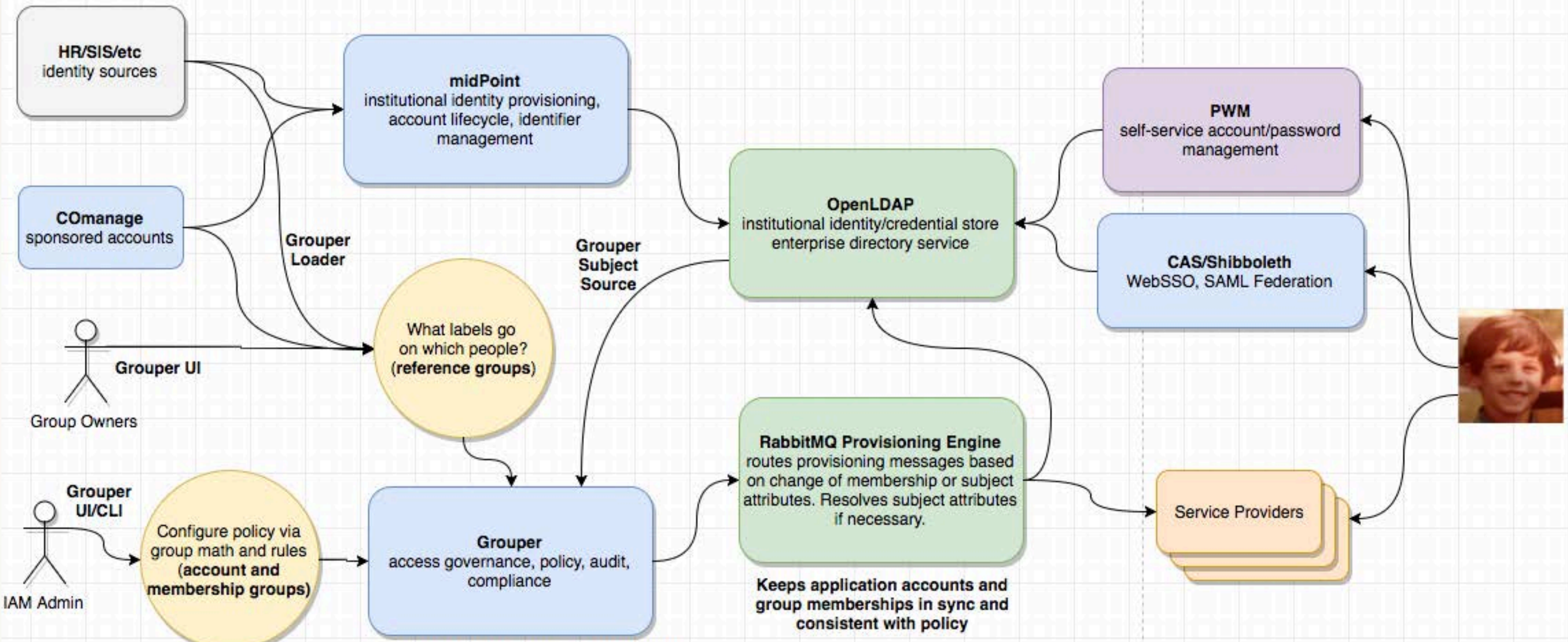
Agenda

- Why do we need a guide?
- Grouper’s place in a TIER-based IAM architecture
- Introduction to the guide
- TIER folder and group design
- Access control models

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/

Lafayette College TIER Campus Success IAM Architecture
2017-08-25



HR/SIS/etc
identity sources

midPoint
institutional identity provisioning, account lifecycle, identifier management

COmanage
sponsored accounts

Grouper Loader

Grouper Subject Source

OpenLDAP
institutional identity/credential store enterprise directory service

PWM
self-service account/password management

CAS/Shibboleth
WebSSO, SAML Federation

Grouper UI

Group Owners

What labels go on which people? (**reference groups**)

Grouper UI/CLI

IAM Admin

Configure policy via group math and rules (**account and membership groups)**

Grouper
access governance, policy, audit, compliance

RabbitMQ Provisioning Engine
routes provisioning messages based on change of membership or subject attributes. Resolves subject attributes if necessary.

Service Providers

Keeps application accounts and group memberships in sync and consistent with policy

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 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

- **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

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

Understanding Grouper

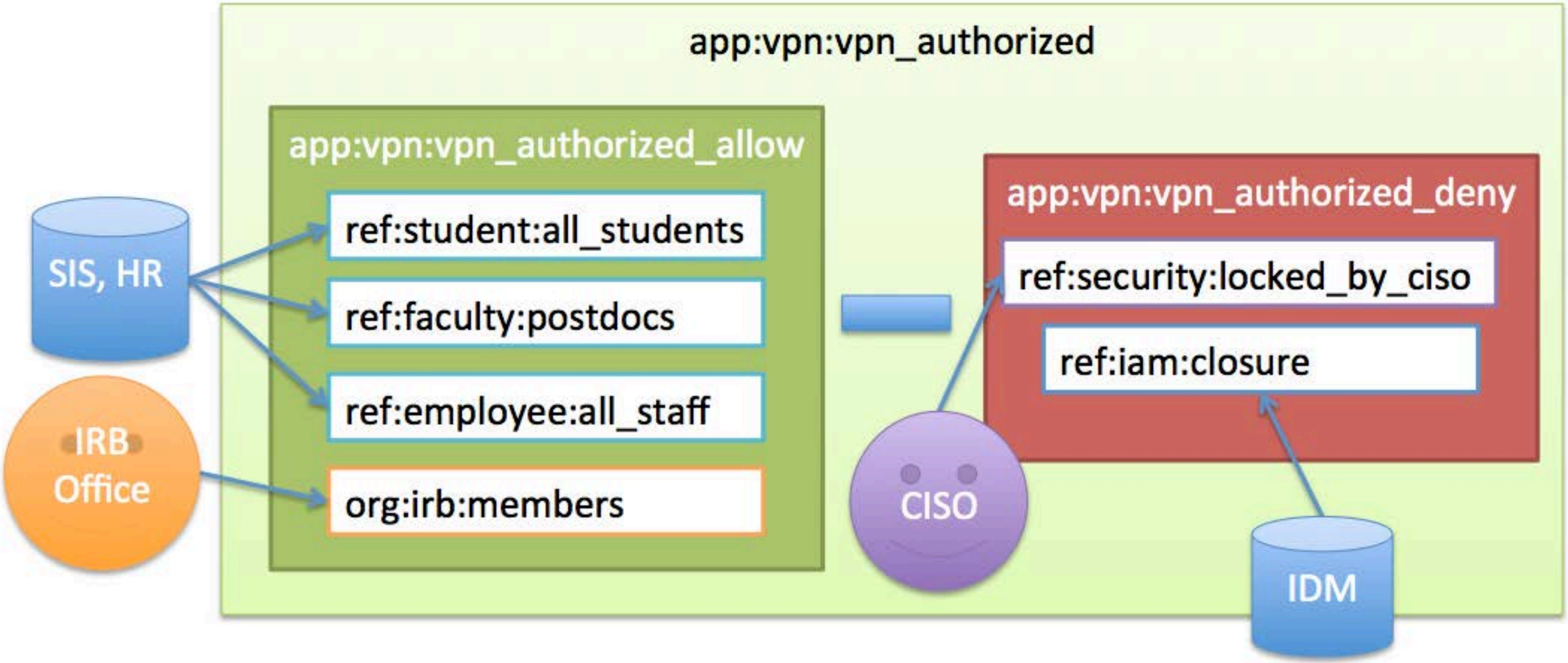
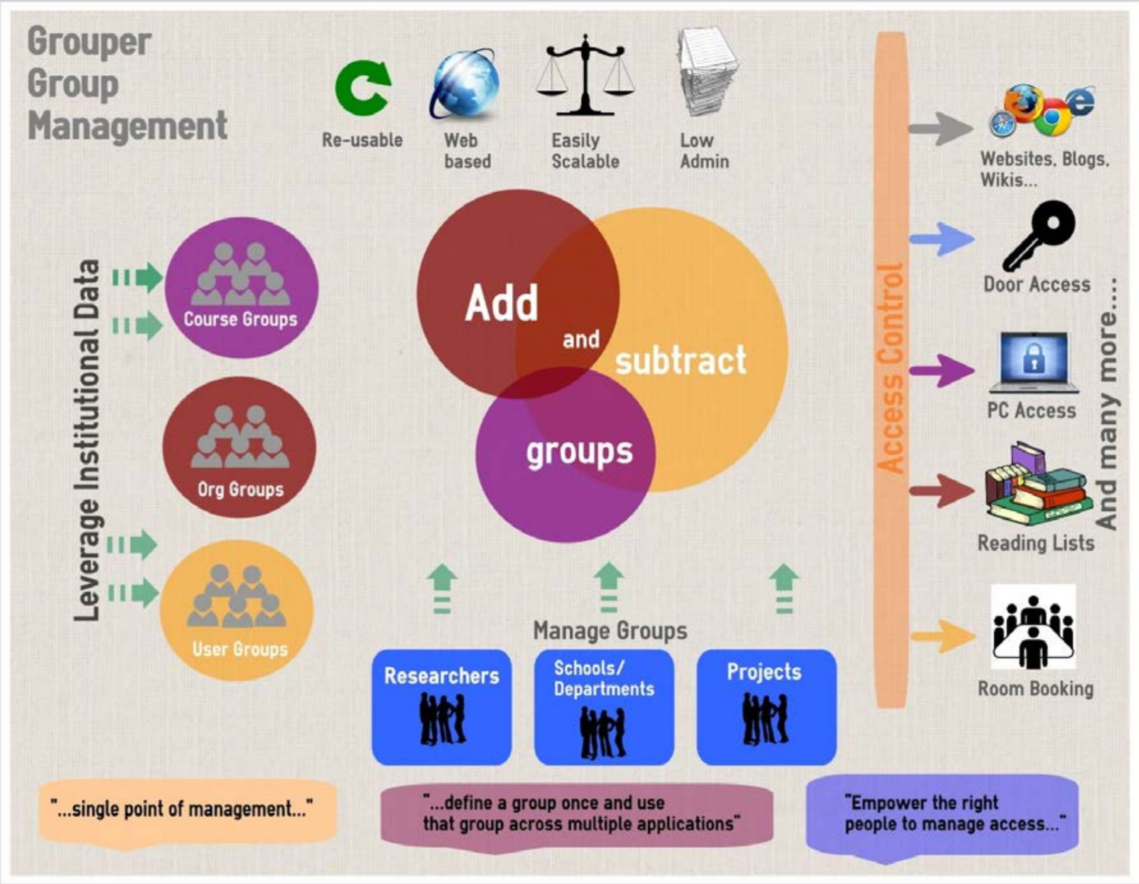


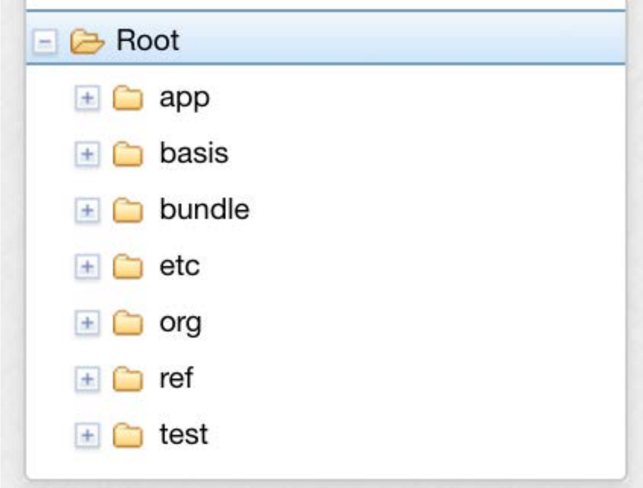
Figure 1: University of Chicago VPN Access Policy



Newcastle University May 2013 Grouper InfoGraphic

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

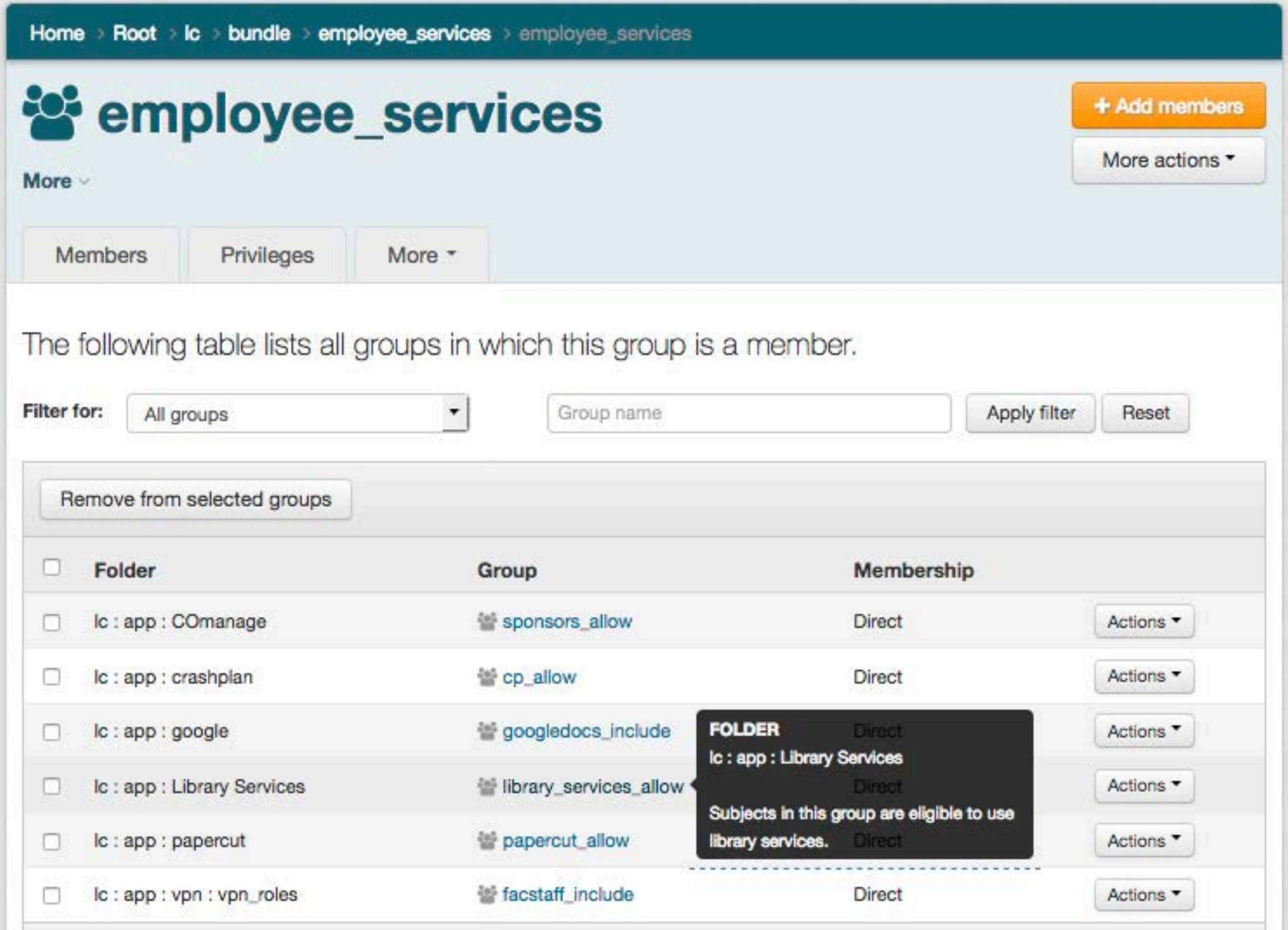
TIER Folder and Grouper Design

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

- **basis:hris:{employee_codes}** - types of employees
- **basis:sis:{student_codes}** - types of students

Reference Groups - Institutionally meaningful cohorts – “truth”

- **ref:role:** - institutional scope roles (e.g. president, provost, chaplain...)
- **ref:employee:** - types of employees (faculty, staff, part-time, full-time...)
- **ref:non-employee:** - types of non-employees eligible for services
- **ref:student:** - types of students (class year, on-track-grad, incoming-class...)
- **ref:alum:** - types of alumni
- **ref:course:** - course rosters including instructors, TAs, etc
- **ref:dept:** - organization hierarchies


Home › Root › lc › bundle › employee_services › employee_services
employee_services
More
+ Add members
More actions
Members
Privileges
More
Remove from selected groups
Apply filter
Reset

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

Filter for: All groups ▾ Group name

□	Folder	Group	Membership	
□	lc : app : COmanage	sponsors_allow	Direct	Actions
□	lc : app : crashplan	cp_allow	Direct	Actions
□	lc : app : google	googledocs_include	Direct	Actions
□	lc : app : Library Services	library_services_allow	Direct	Actions
□	lc : app : papercut	papercut_allow	Direct	Actions
□	lc : app : vpn : vpn_roles	facstaff_include	Direct	Actions

FOLDER
lc : app : Library Services

Subjects in this group are eligible to use library services.

Authorization and Account Groups

- app:vpn: - root folder for the “vpn” application

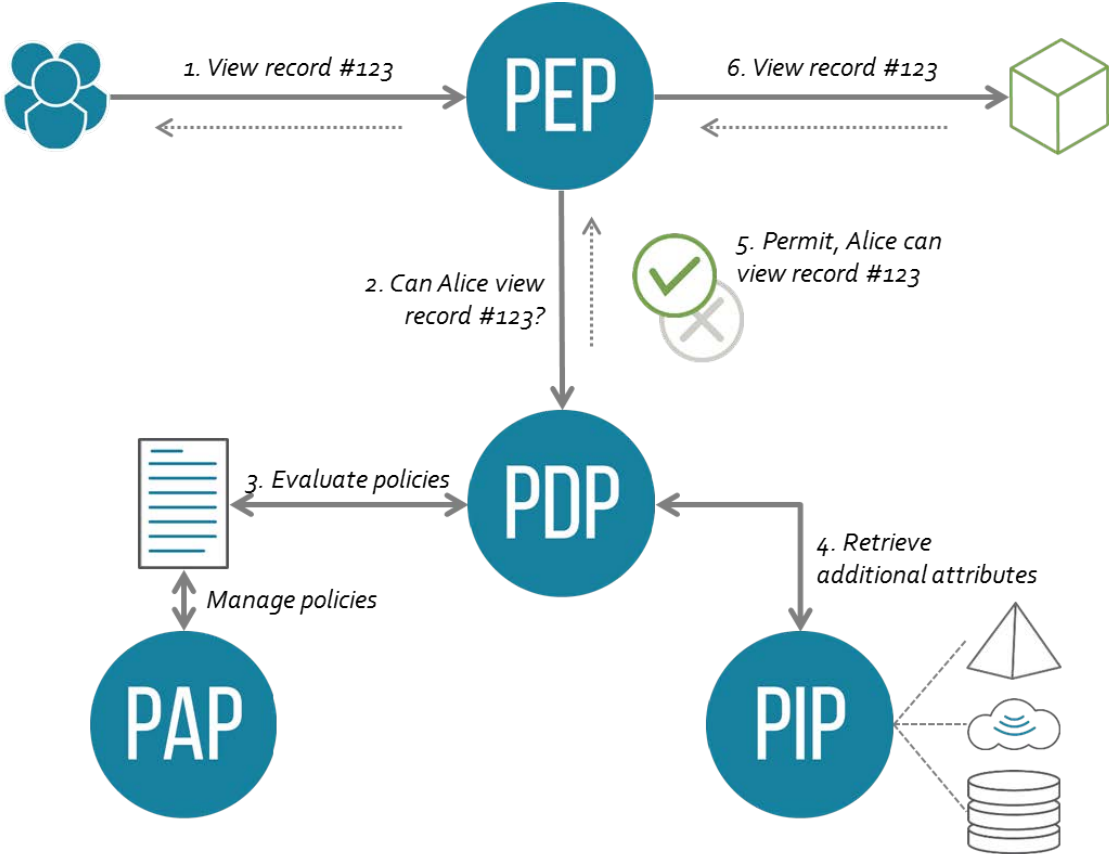
- app:vpn:etc: - folder for administrative security groups
- app:vpn:etc:vpn_admin - members have root-like privileges for the app:vpn:

- app:vpn:ref: - folder for “vpn” application specific reference group if needed

- app:vpn:vpn_user - access policy group (vpn_users_allow - vpn_users_deny)
- app:vpn:vpn_user_allow - only direct members are reference groups
- app:vpn:vpn_user_deny - may include ref:iam:global_deny

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

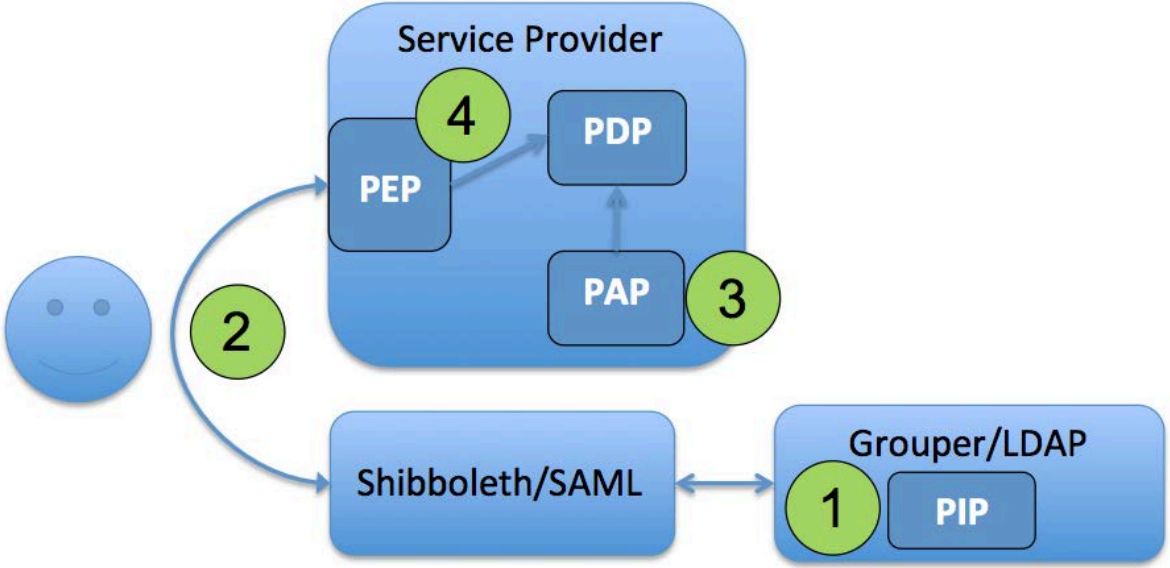

1. View record #123
PEP
6. View record #123
2. Can Alice view record #123?
5. Permit, Alice can view record #123
3. Evaluate policies
PDP
4. Retrieve additional attributes
Manage policies
PAP
PIP

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

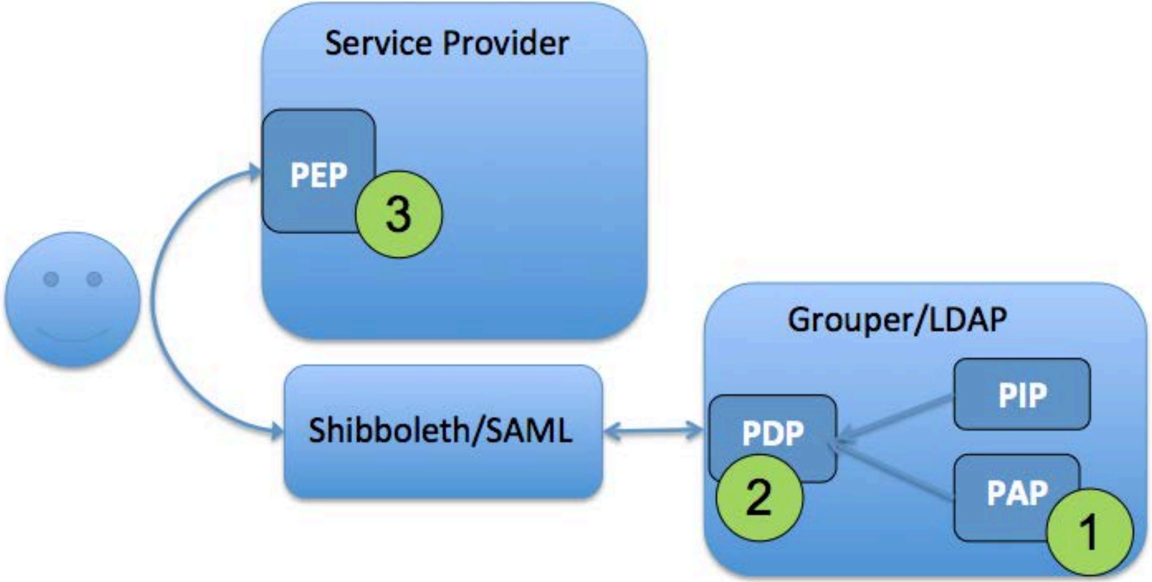
PAP - Policy Administration Point
PDP - Policy Decision Point

PEP - Policy Enforcement Point
PIP - Policy Information Point

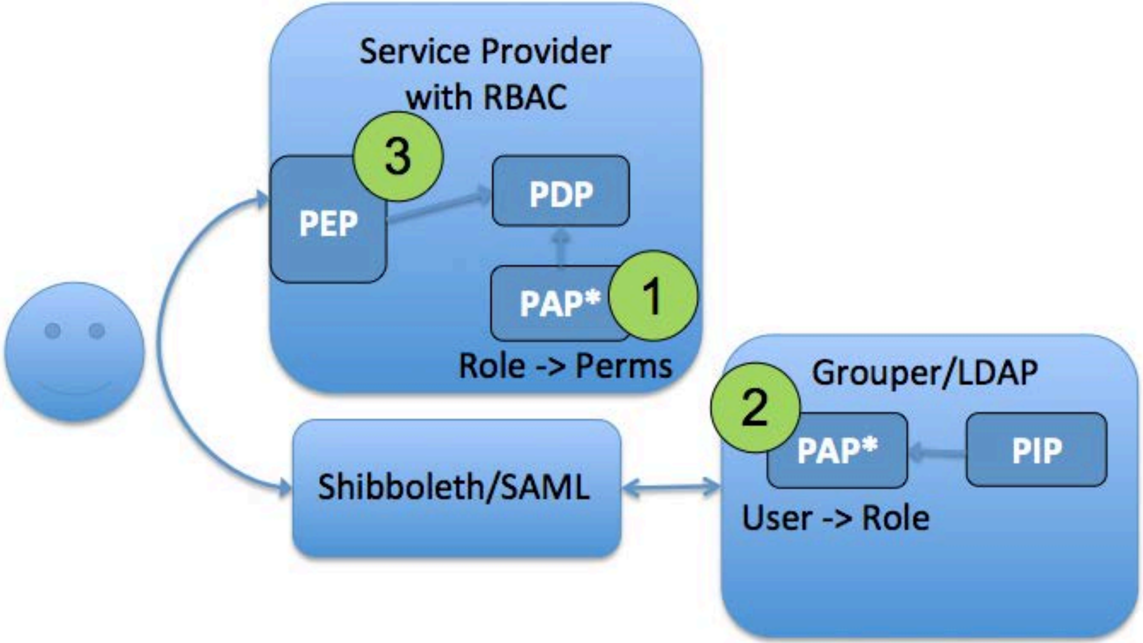
Access Control Model 1 – Grouper Subject Attributes



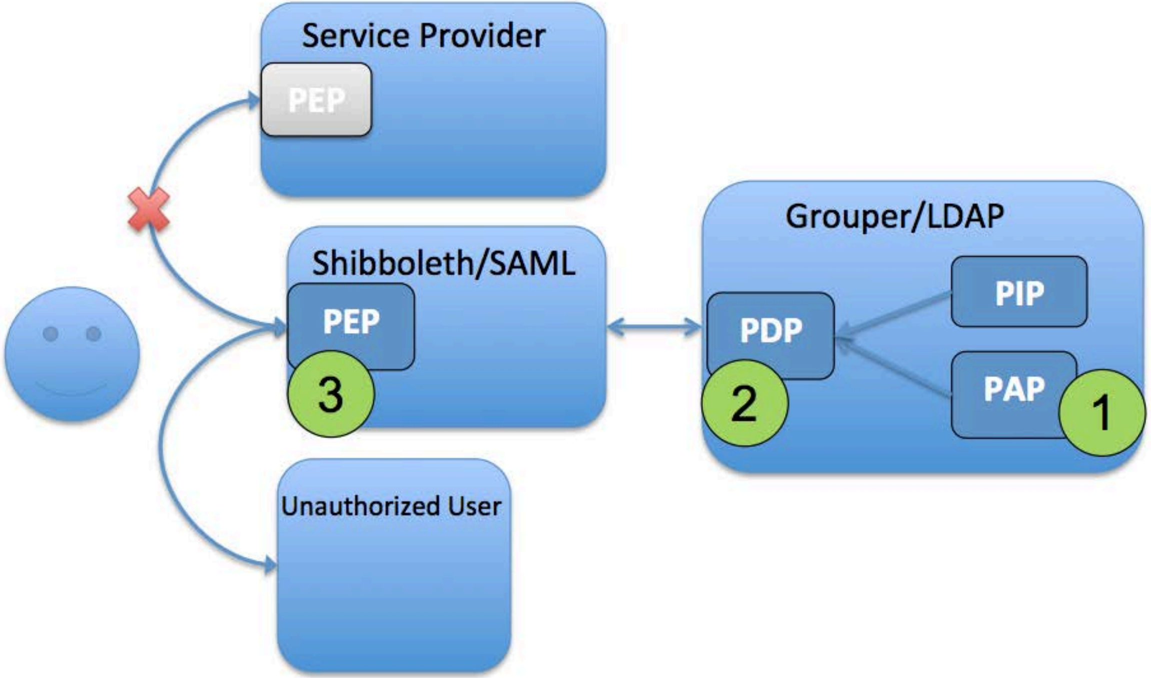
Access Control Model 2 – Grouper as PAP and PDP



Access Control Model 3 – RBAC User to Role Mapping



Access Control Model 4 – WebSSO Short-circuit



Conclusion

- Model and Terminology
  - Basis –> reference –> policy
  - Reference groups = subject attributes (institutionally meaningful cohorts)
  - 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

INTERNET2®

2017 TECHNOLOGY exchange

SAN FRANCISCO CA OCTOBER 15-18

INTERNET2® TIER

TRUST & IDENTITY IN EDUCATION & RESEARCH

Grouper in Action

Access Management Strategies for Higher Education and Research

Chris Hyzer, University of Pennsylvania
Bert Bee-Lingren, Georgia Institute of Technology
Bill Thompson, Lafayette College
Carl Waldbieser, Lafayette College