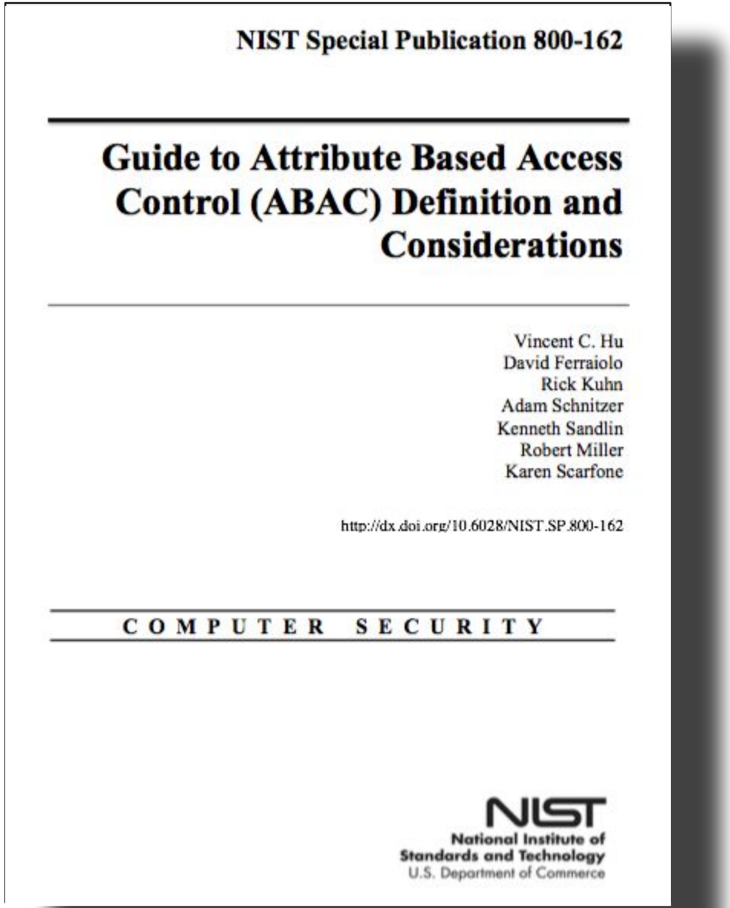
Is Grouper the Answer for Role-based Access? It Sure is for Deprovisioning!

ABAC with Grouper @ Lafayette College

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



NIST Special Publication 800-162

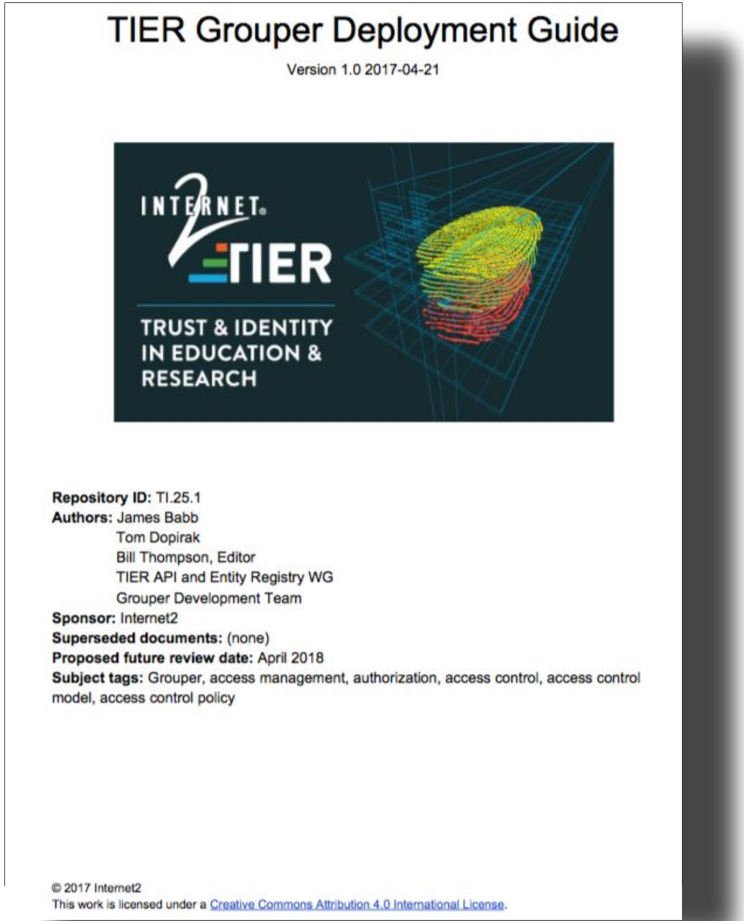
Guide to Attribute Based Access Control (ABAC) Definition and Considerations

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

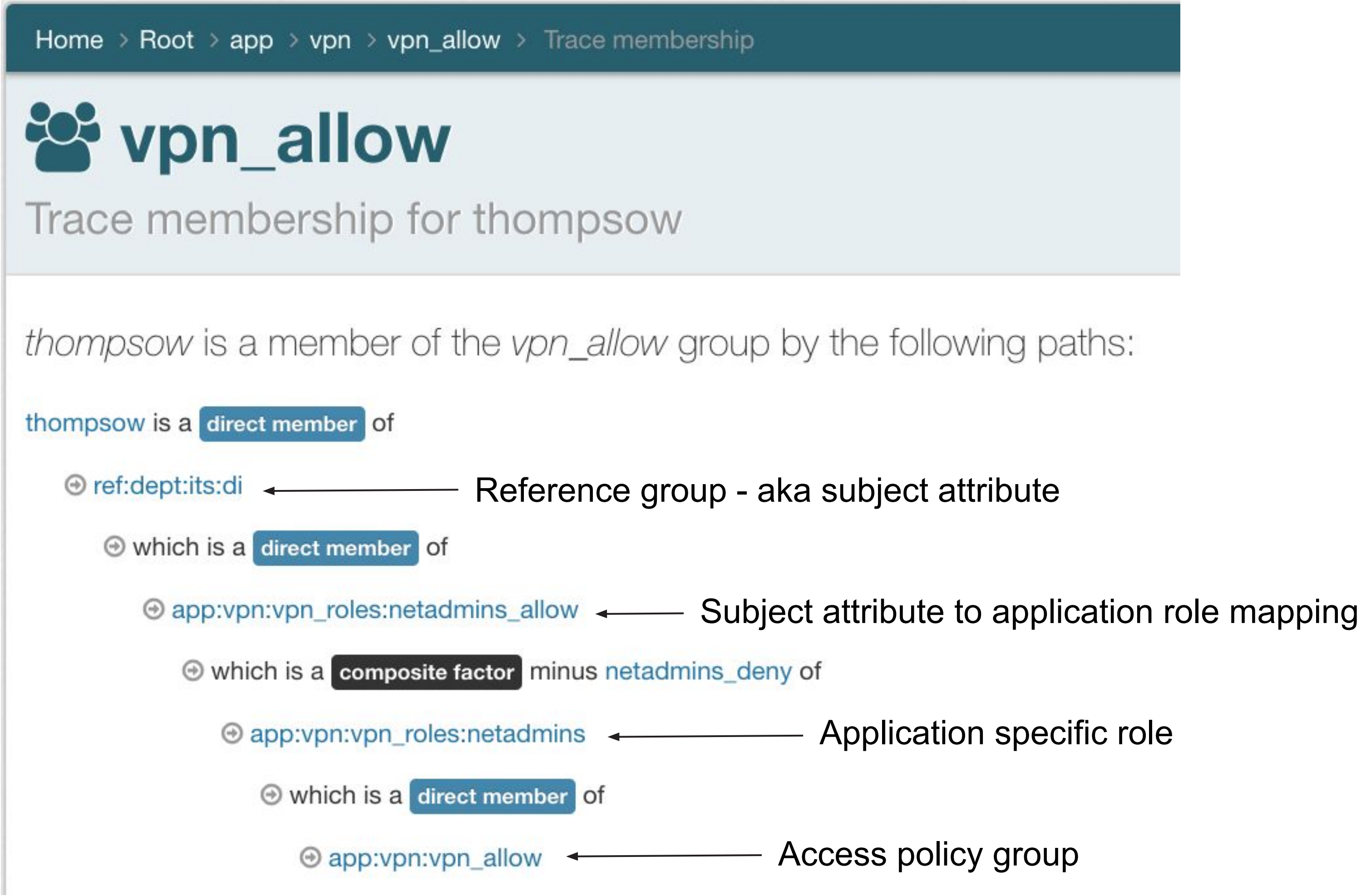
NIST
National Institute of Standards and Technology
U.S. Department of Commerce



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Superseded documents: (none)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



Home > Root > app > vpn > vpn_allow > Trace membership

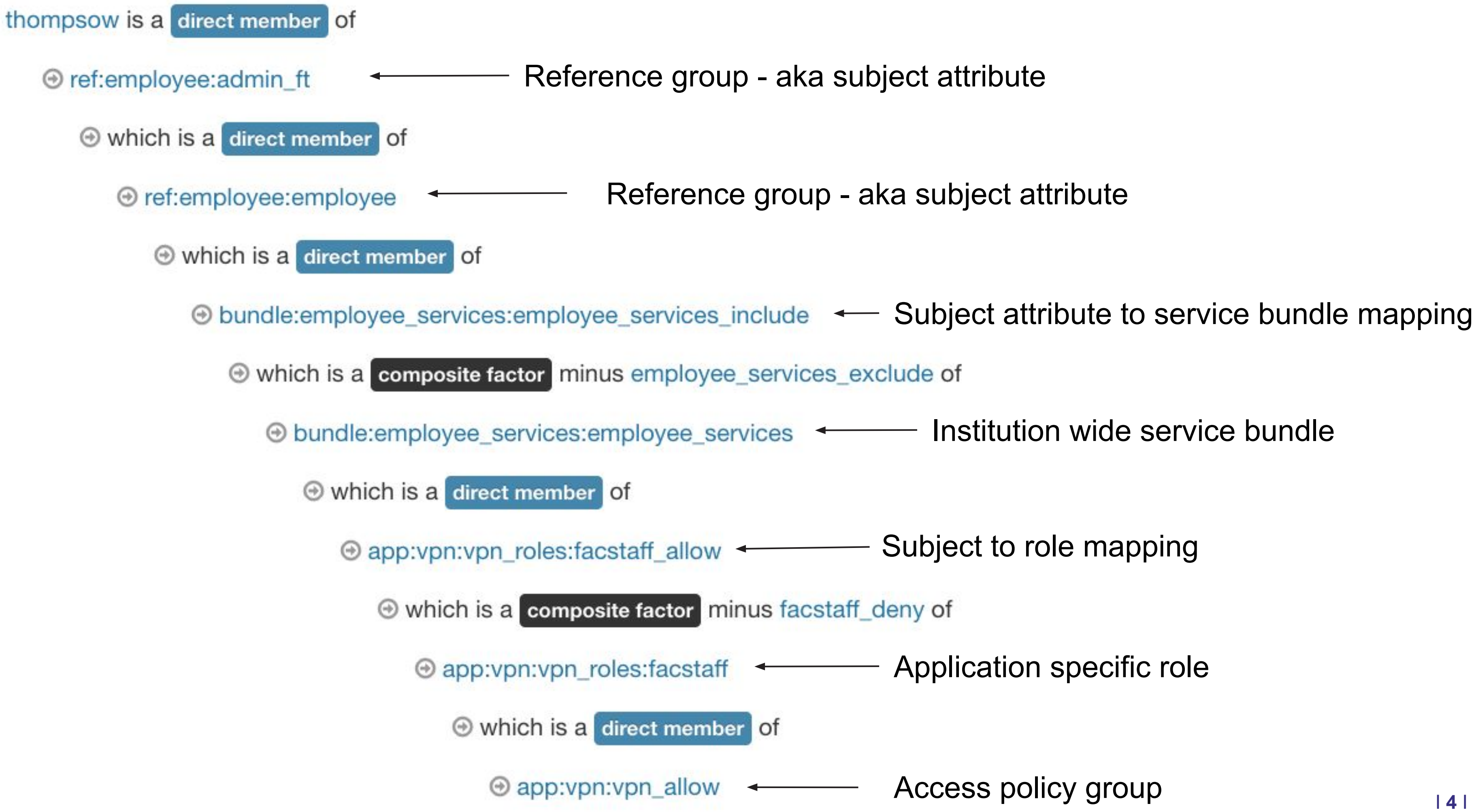
vpn_allow

Trace membership for thompsow

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

thompsow 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



thompsow 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

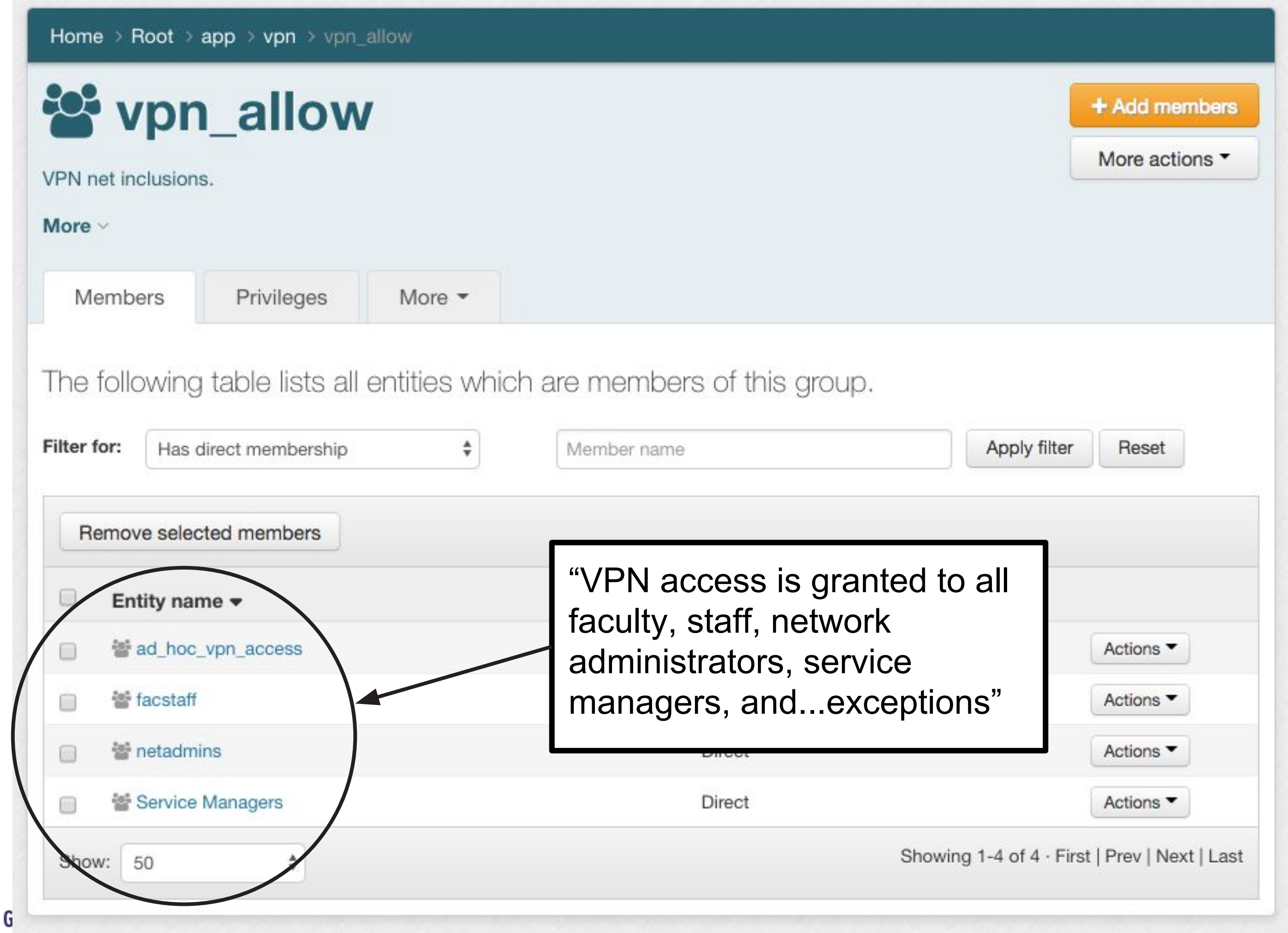
app:vpn:vpn_roles:facstaff_allow ← Subject to role mapping

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



Home > Root > app > vpn > vpn_allow

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

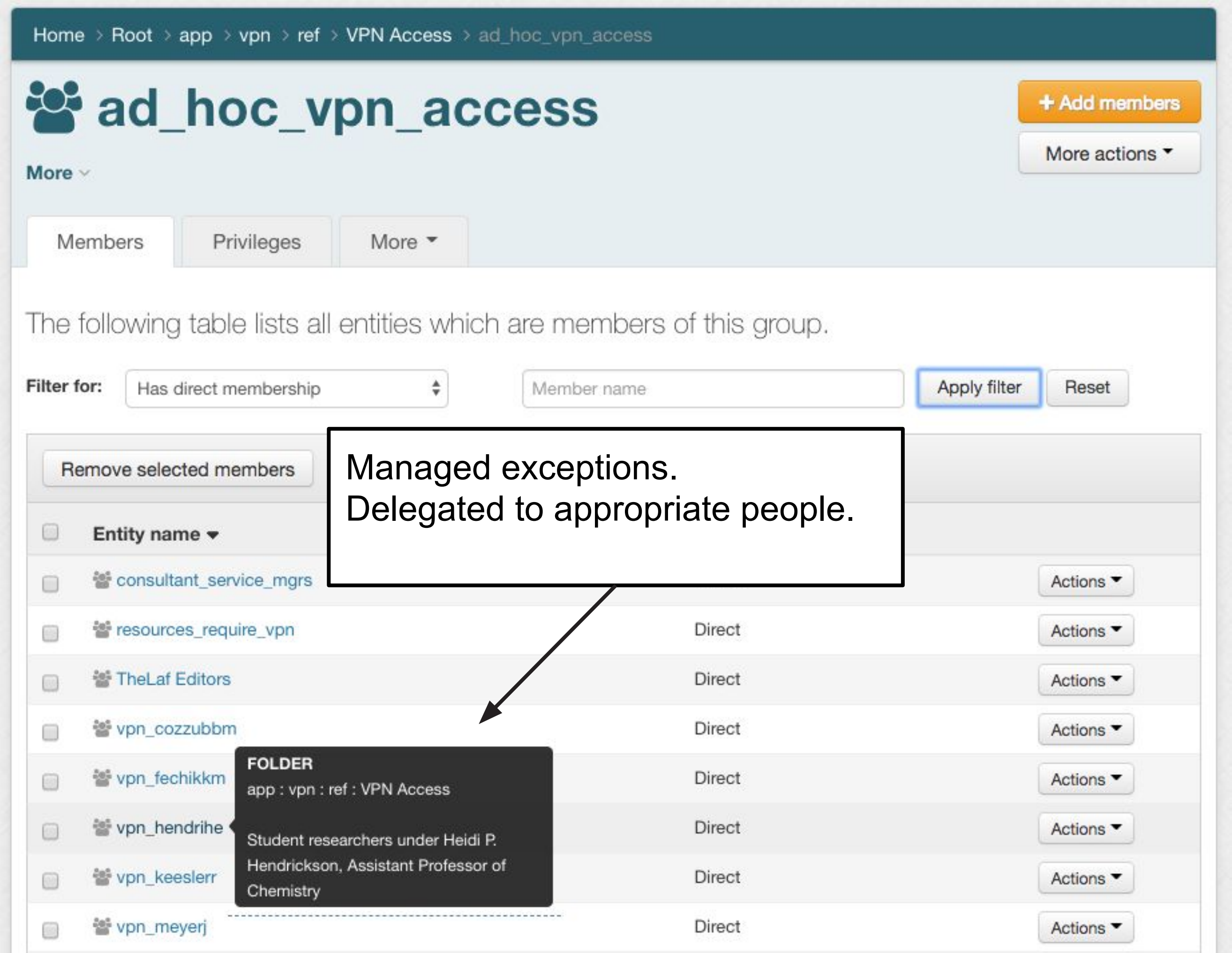
Remove selected members

□	Entity name ▾		
□	ad_hoc_vpn_access		Actions ▾
□	facstaff		Actions ▾
□	netadmins	Direct	Actions ▾
□	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"



Home > Root > app > vpn > ref > VPN Access > ad_hoc_vpn_access

ad_hoc_vpn_access

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

Filter for: Has direct membership | Member name

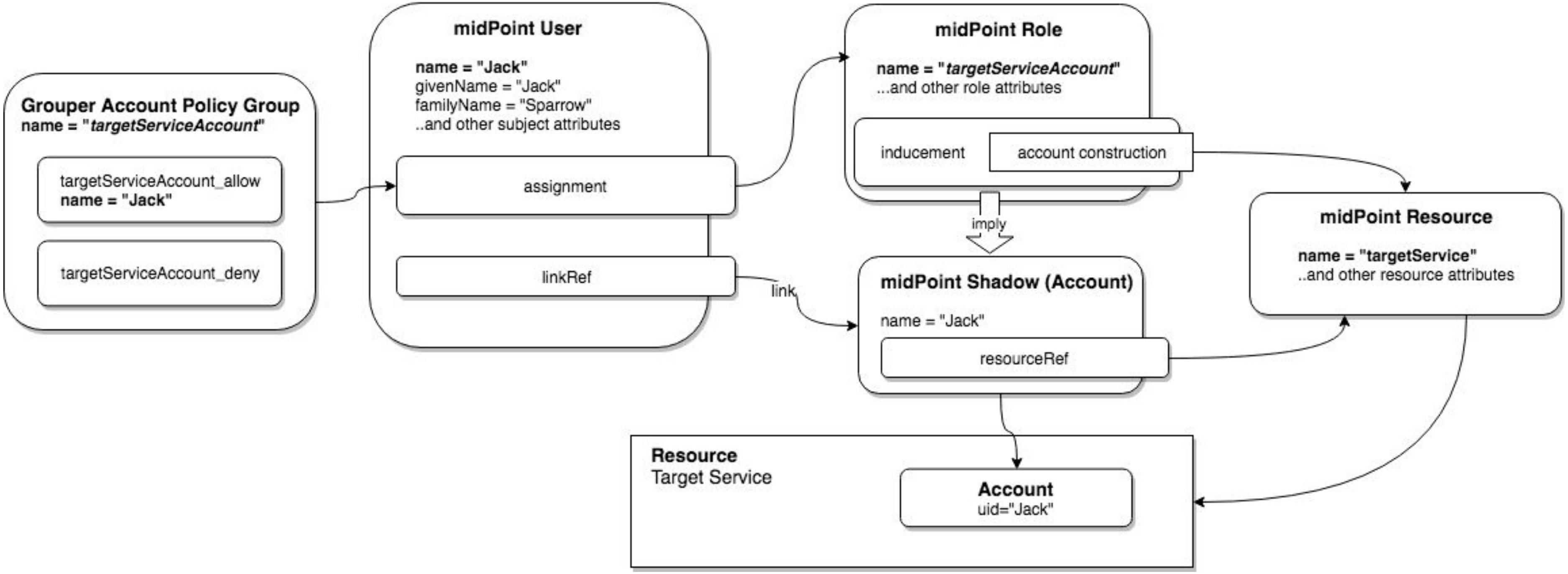
□	Entity name		
□	consultant_service_mgrs		Actions
□	resources_require_vpn	Direct	Actions
□	TheLaf Editors	Direct	Actions
□	vpn_cozzubbm	Direct	Actions
□	vpn_fechikkm	Direct	Actions
□	vpn_hendrihe	Direct	Actions
□	vpn_keeslerr	Direct	Actions
□	vpn_meyerj	Direct	Actions

FOLDER
app : vpn : ref : VPN Access

Student researchers under Heidi P. Hendrickson, Assistant Professor of Chemistry

Managed exceptions.
Delegated to appropriate people.

TIER Account Provisioning via Grouper and midPoint



Grouper Account Policy Group
name = "*targetServiceAccount*"

targetServiceAccount_allow
name = "Jack"

targetServiceAccount_deny

midPoint User

name = "Jack"
givenName = "Jack"
familyName = "Sparrow"
..and other subject attributes

assignment

linkRef

midPoint Role

name = "*targetServiceAccount*"
...and other role attributes

inducement

account construction

midPoint Shadow (Account)

name = "Jack"

resourceRef

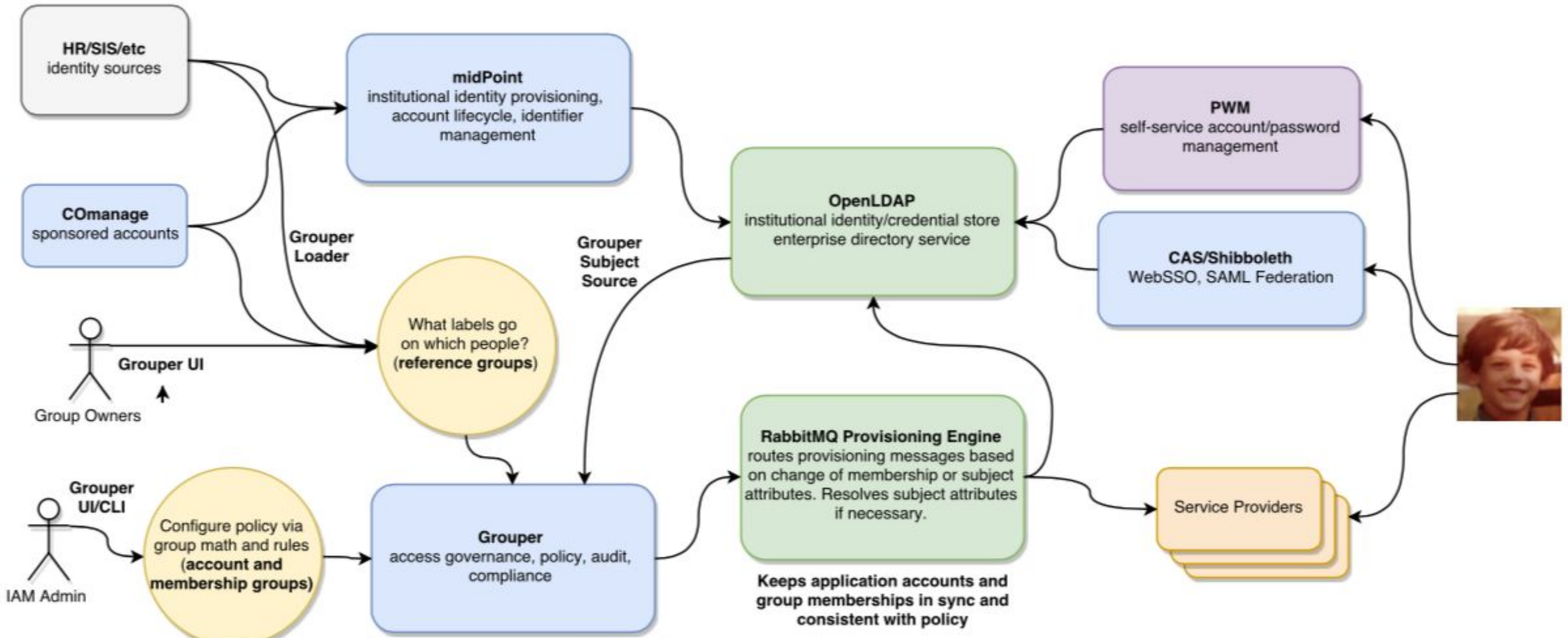
midPoint Resource

name = "targetService"
..and other resource attributes

Resource
Target Service

Account
uid="Jack"

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

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

Grouper UI

Group Owners

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.

Is Grouper the Answer for Role-based Access? It Sure is for Deprovisioning!

ABAC with Grouper @ Lafayette College

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