TIER Access Governance and Grouper 2.4

IAM Online
Wednesday, September 12, 2018

Michael Gettes, University of Florida
Chris Hyzer, University of Pennsylvania
Bill Thompson, Lafayette College
What is Grouper? A lottery?
What is Grouper?

Packaged?

In a container?

→ yes, that’s Grouper!
And now Grouper 2.4 on Slide 2.4

And here’s Chris….
Grouper 2.4 released

- August 2018
- Two years since previous release
- Dozens of substantial enhancements
- Hundreds of small fixes and improvements
Grouper 2.4 features

Release announcement

- Only New UI (other UIs removed)
- Deprovisioning
- Attestation
- Grouper Deployment Guide
- Packaging
- Messaging
- GSH-ng
- Updates to third party packages
Grouper 2.4 upgrade

- Minor upgrade (quick, easy, low risk)
- Please start planning
- Grouper team will focus on 2.4 support and new features
  - Will still fix major bugs and security issues in previous versions
- Upgrade instructions from 2.3
  - Convert some configs
  - Run upgrader
Grouper roadmap - currently working on

Roadmap
- Supporting 2.4
- Configuration stored in database
- Templates to create services and TIER structure
- Real time LDAP loader
- Provision to BMC Remedy
Grouper roadmap - next priorities

- Tag TIER objects (ref, basis, authz, etc)
- Configure which objects to provision in UI
- Add ability to disable loader jobs
- Subject source configuration wizard
- Permission role hierarchy in UI
- Membership reports

- Please email grouper-core@internet2.edu with Roadmap feedback
Access Management Strategies for Higher Education and Research
TIER Grouper Deployment Guide

Bill Thompson, Director, Digital Infrastructure
Lafayette College
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

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Superseded documents: (none)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.
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

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
“All students, staff, postdocs, and members of the IRB have access to VPN unless their account has been locked by the CISO or is in the closure process.”
"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

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

thompsonow 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
VPN access is granted to all faculty, staff, network administrators, service managers, and...exceptions.
Managed exceptions. Delegated to appropriate people.
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
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 PAP and PDP - eduPersonEntitlement
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 = "targetServiceAccount"
...and other resource attributes

 Resource
Target Service

 Account
uid="Jack"
Access Control Model 3 – RBAC User to Role Mapping

1. Role -> Perms
2. User -> Role
3. PEP -> PDP

Service Provider with RBAC

Shibboleth/SAML

Grouper/LDAP
Access Control Model 4 – WebSSO Short-circuit

1. Grouper/LDAP
   - PDP
   - PIP
   - PAP

2. Shibboleth/SAML
   - PEP
   - 3
   - Unauthorized User

3. Service Provider
   - PEP
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 is consistent, easy, flexible, and can be delegated
• Improved security posture and ability to onboard new services quickly

TIER Access Governance with Grouper and Friends
https://meetings.internet2.edu/2018-technology-exchange/detail/10005135/
2018 Technology Exchange - Monday, September 28, 8am - 5pm
Please evaluate today’s session

https://www.surveymonkey.com/r/IAMOnline-Sept2018
2018 Internet2 Technology Exchange (TechEx)
October 15-19, 2018 - Orlando, Florida
https://meetings.internet2.edu/2018-technology-exchange/

- Two full tracks for Trust and Identity topics
- Advance CAMP (ACAMP)
- Pre-meeting tutorials
InCommon Shibboleth Workshop: Making Federation Easier

Brown University, Providence, Rhode Island
November 13-14, 2018

www.incommon.org/shibtraining