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

Vincent C. Hu
David Femiaolo
Ric Kuhn
Adam Schnitzer
Kenneth Sandlin
Robert Miller
Karen Scarfone

https://doi.org/10.6028/NIST.SP.800-162

COMPUTER SECURITY

NIST Special Publication 800-162

TIER Grouper Deployment Guide
Version 1.0 2017-04-21

INTERNET2
TRUST & IDENTITY IN EDUCATION & RESEARCH

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Superseded documents: (none)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

• 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 attribtues
- Access/Account policy group – pre-computed policy decision
Figure 1: University of Chicago VPN Access Policy
"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
thompson is a member of the vpn_allow group by the following paths:

thompson 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

  which is a **direct member** of

- ref:employee:employee

  which is a **direct member** of

- bundle:employee_services:employee_services_include

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

- bundle:employee_services:employee_services

  which is a **direct member** of

- app:vpn:vpn_roles:facstaff_allow

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

- app:vpn:vpn_roles:facstaff

  which is a **direct member** of

- app:vpn:vpn_allow

Reference group - aka subject attribute

Subject attribute to service bundle mapping

Institution wide service bundle

Subject to role mapping

Application specific role

Access policy group
VPN access is granted to all faculty, staff, network administrators, service managers, and...exceptions.
Managed exceptions.
Delegated to appropriate people.
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
1. View record #123
2. Can Alice view record #123?
3. Evaluate policies
4. Retrieve additional attributes
5. Permit, Alice can view record #123
6. View record #123

PAP - Policy Administration Point
PDP - Policy Decision Point
PEP - Policy Enforcement Point
PIP - Policy Information Point

By Axiomatics (Axiomatics) [CC BY 3.0 (http://creativecommons.org/licenses/by/3.0)], via Wikimedia Commons
Access Control Model 1 – Grouper Subject Attributes - eduPersonAffiliation
Access Control Model 2 – Grouper as PAP and PDP - eduPersonEntitlement
Subjects in this group are eligible to use library services.

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

<table>
<thead>
<tr>
<th>Entity name</th>
<th>Membership</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ad_hoc_library_services</td>
<td>Direct</td>
<td>A manually maintained cohort of ad-hoc members who should have access to library services.</td>
</tr>
<tr>
<td>employee_services</td>
<td>Direct</td>
<td></td>
</tr>
<tr>
<td>service_accounts</td>
<td>Direct</td>
<td></td>
</tr>
<tr>
<td>students</td>
<td>Direct</td>
<td></td>
</tr>
</tbody>
</table>

Filter for: Has direct membership

| Member name | Apply filter | Reset |

Show: 50

Showing 1-4 of 4 - First | Prev | Next | Last
TIER Account Provisioning via Grouper and midPoint

Grouper Account Policy Group
- name = "targetServiceAccount"
  - allow
    - 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
<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up one folder</td>
</tr>
<tr>
<td>advising_fullstaff</td>
</tr>
<tr>
<td>adv_career_services</td>
</tr>
<tr>
<td>athletics_fullstaff</td>
</tr>
<tr>
<td>rort_tools_ods_analytics_user</td>
</tr>
<tr>
<td>abroad_fullstaff</td>
</tr>
<tr>
<td>access_fullstaff</td>
</tr>
<tr>
<td>adm_report_manager</td>
</tr>
<tr>
<td>adm_tools_ods_analytics_user</td>
</tr>
<tr>
<td>adv_alum_relations</td>
</tr>
<tr>
<td>adv_annual_fund</td>
</tr>
</tbody>
</table>
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.

HR/SIS/etc identity sources

midPoint institutional identity provisioning, account lifecycle, identifier management

OpenLDAP institutional identity/credential store enterprise directory service

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

What labels go on which people? (reference groups)

COmanage sponsored accounts

Grouper Loader

Grouper Subject Source

PWM self-service account/password management

CAS/Shibboleth WebSSO, SAML Federation

Service Providers

Keep application accounts and group memberships in sync and consistent with policy
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
thompson@lafayette.edu
Director Digital Infrastructure
Lafayette College