Introduction to the GDG

Overview

An InCommon Trusted Access Platform (TAP) based identity and access management program deploys Grouper as a strategic component of its institutional role and access management solution. Grouper is at the center of all group-like management activities, such as institutional roles, access control lists, service eligibility, and email distribution lists.

Grouper can be employed in a variety of flexible access control models, but the underlying approach follows a consistent path:

1. Natural language access management policy drives requirements which help to identify and define institutional cohorts (types of students, types of employees, types of visitors/guests, etc.).
2. Institutional cohorts are then turned into reference groups which are used in the digital access policy definition.
3. Access to systems is then automatically kept in sync with policy as subject attributes change in underlying systems of record (ERP, SIS, etc).

This provides streamlined and automated access for existing and future applications.

In addition to automated access provisioning, Grouper supports user-defined populations. These groups can be self-administered, and attested to, by an authoritative delegate, or, allow members to join or leave as they choose. These ad-hoc populations can then be used in authorization policy as exceptions, self-service, or other forms of populations.

Purpose and Scope

> *"...some additional scaffolding in the form of configurations and conventions based on successful models at other campuses would accelerate an adopting campus's path to rolling out actual services."*
> *- Warren Curry, University of Florida*

This deployment guide aims to make it easier for new deployers to understand Grouper, complete an initial deployment, and implement access management capabilities based on common practice and terminology.

The guide focuses on access management governance using widely deployed Grouper primitives and features. Grouper can also be used to externalize fine-grained application-level permission management. However, that feature has not yet see significant adoption and is mostly out of scope.

Audience

This guide is primarily written for IT architects, technical staff and managers responsible for identity and access management. However, the guide would benefit anyone who is seeking information on an InCommon Trusted Access Platform compatible Grouper deployment.

Readers should be familiar with identity and access management concepts and terminology as defined by NIST Special Publication (SP) 800-162, *Gui de to Attribute Based Access Control (ABAC) Definition and Considerations,* the Grouper glossary, and Grouper UI terminology. Readers completely new to Grouper would also benefit from reviewing the video Intro to Grouper Pt. 1/3: Access Management & Grouper and attending the InCommon Grouper School.

Using the Grouper Deployment Guide

This rest of the deployment guide is organized as follows:

- Understanding Grouper - provides a basic understanding of Grouper and how it relates to the InCommon Trusted Access Platform.
- Folder and Group Design - defines a variety of group types and purposes, and a recommended initial folder and group organization.
- Access Control Models - describes how Trusted Access Platform and Grouper components come together to achieve access management capabilities.
- Provisioning Models - discussion on provisioning models and strategies.
- Operational Considerations - provides pointers and tips on operating Grouper in production.
- Conclusion - concludes the document
- Example Access Policies - provides example access policies.

The guide focuses on high level explanation and discussion. For current technical details and version specific information please refer to the Grouper wiki.

Terminology

This guide builds on and makes use of the terminology defined in NIST Special Publication (SP) 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations,* for IAM level concepts, and borrows Grouper product specific terminology from the Grouper glossary and Grouper UI terminology. When first exposed to Grouper, there is a tendency to view everything as a “group”. This document adopts the following terminology to distinguish Grouper primitives (e.g. “groups”) from IAM level concepts.

Grouper primitives are specific names for features within the product itself. These may be mapped to one or more IAM level concepts that are used to implement various capabilities. A **Grouper group** is a primitive and that can be used in many different ways to implement the desired access control mechanism.

Subjects that have been added directly to a group are said to have a **direct membership assignment**. Subjects that are members of a group by virtue of membership in another group are said to have an **indirect membership assignment**. That is, they are members because of their membership in a subgroup that is itself a member of the parent group. A **composite group** is the result of combining two other groups, typically by relative complement (i.e. Group A minus Group B).

In order to distinguish the intended use of a group this document will qualify the word “group”. For instance, a **reference group** is a named group of subjects that is largely intended to be used by reference within access policy groups. Reference group names can also be thought of as labels or tags that are applied to all the members of the group. In this way, they can also be viewed as subject attributes from an ABAC policy perspective.

Basis groups tend to consist solely of direct subject membership assignments and are often maintained automatically by the Grouper Loader process based on data from a system of record. Basis groups are typically subsets of cohorts that when used together in different combinations form proper reference groups. For instance, an HR system might have different codes for various employees. These cohorts might be loaded separately into basis groups and then combined into an “employee” reference group.

Access policy groups are the digital representation of the natural language requirements for specific access, permissions, or role in a target service. Access policy groups are often implemented as a composite group whose membership is composed of an allow group and a deny group. Effective membership in an access policy group represents a precomputed access policy decision. Membership within an access policy group may be kept in sync directly with a target service or an intermediary like an LDAP based enterprise directory service, and is often incorporated in a SAML authentication response via Shibboleth.

Controlling who has access to objects and actions within Grouper itself is controlled by Grouper Privileges. Grouper Privileges can be assigned to individual Grouper users. However, it is best practice to assign them to specific groups within Grouper. Groups used to assign Grouper Privileges to users are called **security groups.**

Previous: Executive Summary Next: Understanding Grouper

Previous: Executive Summary Next: Understanding Grouper