Exploring Internet2 Grouper & NIST RBAC/ABAC
Misagh Moayyed, IAM Architect, Unicon
William G. Thompson, Jr., CISSP, Lafayette College
Exploring Internet2 Grouper & NIST RBAC/ABAC

Introduction to NIST RBAC/ABAC models and standards

- INCITS 359-2012 Role Based Access Control
- INCITS 494-2012 RBAC - Policy-Enhanced
- NIST Special Publication 800-162 Guide to Attribute Based Access Control Definition and Considerations

How do these models and standards apply to Grouper and Grouper based access management systems?
Shout out to Shawn McKinney, symas.

https://www.linkedin.com/in/shawn-mckinney-5238672
https://symas.com/

- OpenLdap
- Apache Fortress
- JavaOne Open Source IAM Expert Panel

“Good artists copy, great artists steal” - Steve Jobs quoting Picasso quoting Igor Stravinsky quoting T.S. Elliot quoting …” - http://quoteinvestigator.com/2013/03/06/artists-steal/
INCITS 359-2012 Role Based Access Control

INCITS 494-2012 RBAC - Policy-Enhanced

NIST Special Publication 800-162 Guide to Attribute Based Access Control Definition and Considerations

Introduction to NIST RBAC/ABAC models and standards
NIST: Role Based Access Control (RBAC) and Role Based Security - [http://csrc.nist.gov/groups/SNS/rbac/](http://csrc.nist.gov/groups/SNS/rbac/)

Formalized by David Ferraiolo and Rick Kuhn in Role-Based Access Controls (1992)

NIST RBAC model (Sundhu, Ferraiolo, and Kuhn, 2000)

Initially released as ANSI INCITS standard in 2004

Updated and expanded in 2012 as
- INCITS 359-2012 Role Based Access Control
- INCITS 359-2012 Role Based Access Control - Policy Enhanced
INCITS 359-2012 Role Based Access Control (RBAC)

“...initiated by National Institute of Standards (NIST) in recognition of a need...for **consistent and uniform definition of role based access control (RBAC) features.**”

“...lack of widely accepted model resulted in uncertainty and confusion about RBAC’s utility and meaning. This standard seeks to resolve this situation by using a **reference model to define RBAC features** and then describing the functional specifications for those features.”

Developed by InterNational Committee for Information Technology Standards (INCITS) and approved by American National Standards Institute (ANSI). INCITS Committee members: Apple, EMC, IBM, IEEE, Intel, NIST, Oracle, Microsoft, Purdue University, US DOD, US DHS, VMWare,...
INCITS 359-2012 Role Based Access Control (RBAC)

RBAC Reference Model & Functional Specification

Reference Model has four model components:

**Core RBAC - Users, Roles, Perms, Session (aka Role Activation)**
Role is a set of permissions
Users assigned to Roles (creates effective permission sets for users)
Users activate one or more Roles in an application Session

**Hierarchical Roles**
Roles can inherit privilege sets

**Static Separation of Duties (SSD)**
Can be assigned a subset of roles in a particular collection

**Dynamic Separation of Duties (DSD)**
Can activate a subset of roles in a particular collection
ANSI INCITS 359 RBAC has three standards interfaces:

1. Administrative - CRUD permission, role, hierarchy assignments, etc.
2. Review - policy interrogation (grouper audit/report/etc)
3. System - policy enforcement (authN/authZ CAS and Spring/Shiro/.Net))

Map RBAC Reference Model to Grouper terminology (users, roles, permissions, operations, and objects) -> (users/groups, roles, permissions, actions, resources)

Map RBAC functional specification to Grouper functions
Figure 1: Core RBAC
Figure 2: Hierarchical RBAC
Figure 3: SSD within Hierarchical RBAC
Figure 4: Dynamic Separation of Duty Relations
Grouper RBAC

- Attributes
- Roles
- Permissions
- Attribute definition
- Permission definition
- Role inheritance
- Delegation model extends that for Groups
<table>
<thead>
<tr>
<th>RBAC</th>
<th>Grouper</th>
<th>uPortal</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Subject</td>
<td>Principal</td>
</tr>
<tr>
<td>Operation</td>
<td>Action</td>
<td>Activity</td>
</tr>
<tr>
<td>Object</td>
<td>Resource</td>
<td>Target</td>
</tr>
</tbody>
</table>
### Groups / roles / local entities

Enter search text to find a group / role / local entity

Applications:uPortal:Roles:Portal Developers

**Edit group / role / local entity** | **New group / role / local entity**

---

### Role

<table>
<thead>
<tr>
<th>Folder</th>
<th>apps: portal: roles:</th>
</tr>
</thead>
<tbody>
<tr>
<td>UUID</td>
<td>7260a1c7cd384fe2948cd2ed49b66897</td>
</tr>
<tr>
<td>ID</td>
<td>12.local.16</td>
</tr>
<tr>
<td>ID Path</td>
<td>apps:portal:roles:12.local.16</td>
</tr>
<tr>
<td>Type</td>
<td>Role</td>
</tr>
<tr>
<td>Name</td>
<td>Portal Developers</td>
</tr>
<tr>
<td>Description</td>
<td>All IT developers</td>
</tr>
</tbody>
</table>

**Assign privileges to everyone**

- [x] read
- [x] view

**Buttons:**
- Delete
- Cancel
- Privileges
- Role inheritance
- Role inheritance graph
- Memberships
- Save
Resource/Object - Error Channel Details

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute definition</td>
<td>apps:portal:permissions:UP_ERROR_CHAN:errorChanPermDef</td>
</tr>
<tr>
<td>Folder</td>
<td>Applications: uPortal: Permissions: Error Channel:</td>
</tr>
<tr>
<td>UUID</td>
<td>075e1829cbfc4a51837b12733f5fb5ac</td>
</tr>
<tr>
<td>ID</td>
<td>DETAILS</td>
</tr>
<tr>
<td>ID Path</td>
<td>apps:portal:permissions:UP_ERROR_CHAN:DETAILS</td>
</tr>
<tr>
<td>Name</td>
<td>DETAILS</td>
</tr>
<tr>
<td>Description</td>
<td>Stack Trace</td>
</tr>
</tbody>
</table>

Options: Delete, Cancel, Inheritance, Inheritance graph, Attribute definition, Save
Database table rows and columns (i.e. target resource/object)

<table>
<thead>
<tr>
<th>ID</th>
<th>PersonID</th>
<th>NetID</th>
<th>First</th>
<th>Last</th>
<th>Email</th>
<th>Work#</th>
<th>Home#</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3</td>
<td>12345</td>
<td>js</td>
<td>John</td>
<td>Smith</td>
<td><a href="mailto:js@a.edu">js@a.edu</a></td>
<td>3-1234</td>
<td>123-4567</td>
</tr>
<tr>
<td>B4</td>
<td>98765</td>
<td>sd</td>
<td>Sara</td>
<td>Davis</td>
<td><a href="mailto:sd@a.edu">sd@a.edu</a></td>
<td>5-2345</td>
<td>234-5678</td>
</tr>
<tr>
<td>C5</td>
<td>54321</td>
<td>rj</td>
<td>Ryan</td>
<td>Jones</td>
<td><a href="mailto:rj@a.edu">rj@a.edu</a></td>
<td>7-4567</td>
<td>345-6789</td>
</tr>
<tr>
<td>T7</td>
<td>56789</td>
<td>jc</td>
<td>Julia</td>
<td>Clark</td>
<td><a href="mailto:jc@a.edu">jc@a.edu</a></td>
<td>9-6789</td>
<td>456-7890</td>
</tr>
</tbody>
</table>

Students

Faculty
Permission definition has configuration and security

Attribute definition

Folder: fgac: apps: secureUserData: permissions:

UUID: 963bd02023bc492a99993c0c81caa219

ID: rowOrColumnPermissionDef

Type: Permission

Description: row or column permission for the Secure User Data application

Multi-assignable: 

Value type: No value

Multi-valued: 

Assign to:
- Attribute definition
- Folder
- Group
- Member
- Membership
- Membership - immediate only

Assign privileges to everyone:
- admin
- update
- read
- view
- optin
- optout

Delete | Cancel | Actions | Privileges | Attribute names | Save
Read/write action for this permission def

Include an “all” which implies read and write

Note: this is specific to this one permission definition, and does not affect other permissions in Grouper
Resource/Object name for each set of columns

<table>
<thead>
<tr>
<th>Attribute definition</th>
<th>fgac:apps:secureUserData:permissions:rowOrColumnPermissionDef</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Folder</strong></td>
<td>fgac: apps: secureUserData: permissions: columns:</td>
</tr>
<tr>
<td><strong>UUID</strong></td>
<td>58e3436a7dbe47ae8d0ec114ce5a6138</td>
</tr>
<tr>
<td><strong>ID</strong></td>
<td>columns_contact</td>
</tr>
<tr>
<td><strong>ID Path</strong></td>
<td>fgac:apps:secureUserData:permissions:columns:columns_contact</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>columns_contact</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Contact information for the user (email, phone, etc)</td>
</tr>
</tbody>
</table>
Column resource inheritance

Attribute name graph

Attribute name: fgac:apps:secureUserData:permissions:columns:columns_all

- columns_all
- columns_name
- columns_contact
- columns_ids
Subjects will get connect as a specific database schema.
## Assign the permissions

**Permission type:** Entity

**Permission definition:**
- fgac:apps:secureUserData:permissions:rowOrColumnPermissionDef

**Permission resource:**

**Role:**

**Entity:**

**Action:**

**Enabled / disabled:** Enabled only

### Assignments

<table>
<thead>
<tr>
<th>Entity</th>
<th>Resource</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>columns_ids</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>columns_name</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>rows_fgacStudents</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>columns_contact</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>columns_ids</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>columns_name</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>rows_fgacFacultyAndStaff</td>
<td>all</td>
</tr>
</tbody>
</table>
attribute: RBAC session attributes as used in this document are a characteristic of a subject, resource, action, or environment that may be referenced in a predicate or target.

constraint: A constraint is a relation among role features that acts as a restriction. This standard describes both static constraints (administratively controlled) and dynamic constraints (run time)

external policy rules: Imported constraints and data values for use in making role-base access control decisions.
INCITS 494-2012 RBAC - Policy-Enhanced

All constraints are determined only by External Policy Rules and External Data.

Figure 1 – RBAC Policy-Enhanced Reference Model

*The RBAC engine controls all access control decisions
Table 1 – RPE Dynamic Constraints

<table>
<thead>
<tr>
<th>Constraint Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role-role (Dynamic)</td>
<td>Restriction on which roles may be active simultaneously</td>
</tr>
<tr>
<td>User-role (Dynamic)</td>
<td>Restriction on which users may activate a given pair of roles at the same time</td>
</tr>
<tr>
<td>Attribute-sensitive (Dynamic)</td>
<td>Restriction on roles or permissions that depends on the value of an attribute</td>
</tr>
</tbody>
</table>

Table 2 – RPE Static Constraints

<table>
<thead>
<tr>
<th>Constraint Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role-role (Static)</td>
<td>Restriction on which roles may be assigned to a given user</td>
</tr>
<tr>
<td>Permission-permission (Static)</td>
<td>Restriction on which permissions may be assigned to the same role</td>
</tr>
<tr>
<td>Permission-role (Static)</td>
<td>Restriction on which permissions may be assigned to a given role</td>
</tr>
<tr>
<td>User-role (Static)</td>
<td>Restriction on which users may ever be assigned to a given pair of roles</td>
</tr>
</tbody>
</table>
Grouper RPE

Grouper Permission Limit Built-In Implementations are:
● Weekday 9 to 5 limit
● Amount less than limit
● Amount less than or equal limit
● Labels contain limit
● IP address on networks limit
● IP address on network realm limit
● Expression language (EL) limit
Attribute Based Access Control (ABAC): An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment attributes and conditions.

Access Control Mechanism (ACM): The logical component that serves to receive the access request from the subject, to decide, and to enforce the access decision.
Figure 4: Enterprise ABAC Scenario Example
Students that are in a COS state may not quite meet the definition of "student" invented for the portal. ITS policy seems to be to continue services for these accounts unless the Office of Advising indicates the account should be termed. Recently reinstated students may also need student access to the portal prior to taking classes. Those accounts should be added to this group with a definite end date (e.g. start of next semester) in mind.
vpn_roles

- exceptions
- exceptions_exclude
- exceptions_include
- netadmins
- netadmins_exclude
- netadmins_include
- vpn
- vpn_exclude
- vpn_include
Grouper

Support is enabled by including the following dependency in the WAR overlay:

```
<dependency>
  <groupId>org.jasig.cas</groupId>
  <artifactId>cas-server-integration-grouper</artifactId>
  <version>${cas.version}</version>
</dependency>
```

This access strategy attempts to locate Grouper groups for the CAS principal. The groups returned by Grouper are collected as CAS attributes and examined against the list of required attributes for service access.

The following properties are available:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupField</td>
<td>Decides which attribute of the Grouper group should be used when converting the group to a CAS attribute. Possible values are NAME, EXTENSION, DISPLAY_NAME, DISPLAY_EXTENSION.</td>
</tr>
</tbody>
</table>

You will also need to ensure grouper.client.properties is available on the classpath:
- Grouper access strategy based on group's display extension:

```json
{
    "@class": "org.jasig.cas.services.RegexRegisteredService",
    "serviceId": "^https://.+",
    "name": "test",
    "id": 62,
    "accessStrategy": {
        "@class": "org.jasig.cas.grouper.services.GrouperRegisteredServiceAccessStrategy",
        "enabled": true,
        "ssoEnabled": true,
        "requireAllAttributes": true,
        "requiredAttributes": {
            "@class": "java.util.HashMap",
            "memberOf": ["java.util.HashSet", ["admin"]]
        },
        "groupField": "DISPLAY_EXTENSION"
    }
}
```
Policy Enforcement Points

ASP .NET web application with a custom implementation of a RoleProvider that uses Grouper Web Services to determine roles and permissions.

[https://github.com/UniconLabs/cas-spring-security-grouper](https://github.com/UniconLabs/cas-spring-security-grouper)
A proof of concept Spring Security adapter implementation on top of Grouper data store

[https://github.com/UniconLabs/cas-shiro-grouper](https://github.com/UniconLabs/cas-shiro-grouper)
proof of concept Apache Shiro adapter implementation on top of Grouper data store