Access Management Workstream Fit Gap Review

Overview

The Access Management subcommittee has noted that existing projects with substantial capabilities and adoption already exist in the HE community, namely Gouper and KIM, and that there is already substantial agreement among many projects regarding the core objects (data) of access management; groups, permission, roles, etc leveraging much of the work developed by MACE-Paccman.

Rather than produce a fit gap the subcommittee has focused on common ground between Grouper and KIM and provided two recommendations:

1. Use the KIM service interfaces as the starting point for defining how core access management objects (data) are shared among the O4 suite
2. Create a mechanism to increase on-going collaboration between KIM and Grouper

Deliverables

The subcommittee's identified deliverables are essentially an evolution of Grouper and KIM as new use cases are identified and work on API harmonization progresses:

- Identification and documentation of new use cases not covered by current functionality
- Harmonization of APIs and data between KIM and Grouper
- Adoption of APIs within community projects (uPortal uMobile, Kuali, Sakai,...)
- Implementation of PEP plug-ins for common platforms (Spring Security, Apache Shiro, .NET, PHP,...)

Components

- Grouper
- KIM

Potential Components

- KEW

Capabilities

- Central and distributed group and permissions management
- Ad-hoc and institutional data driven groups/permissions
- Externalized permissions/groups/roles
- Access Attestation/Certification - ability to review who has/had access to what/when
- Set of PEP integration plug-ins for Atlassian, Oracle RDBMS Security VPDB, uPortal, Unix permissions.

Note

Workflow tools to support access request and approval was deemed out of scope for the Access Management workstream. This critical capability was deemed the purview of the Shared Services workstream.

Grouper's audit capabilities already meets many need in the area of Access Certification and Risk Assessment. However further definition of these requirements are needed before it could be included in a roadmap. Perhaps a standalone app that can integrate with either KIM or grouper would be useful.

References

- https://spaces.at.internet2.edu/display/OSIdM4HEteam/Access+Management+Subcommittee+Deliverables
- https://spaces.at.internet2.edu/display/macepaccman/MACE-paccman-glossary
- https://spaces.at.internet2.edu/display/macepaccman/Permissions+API+suggestion+based+on+Grouper+permissions
- https://spaces.at.internet2.edu/display/macepaccman/Penn+authorization+system
- https://spaces.at.internet2.edu/display/macepaccman/Another+Glossary+Page
- https://spaces.at.internet2.edu/download/attachments/1540598/Kuali+Service+Summaries.pdf

Comments & Questions

The Access Management subcommittee notes that Grouper and KIM are complimentary and composable. Would it be helpful to further elaborate on this in terms of the XACML model (PEP, PAP, PDP, etc)?

The Provisioning subcommittee has identified the following deliverables for their workstream:
1. Recipes for implementing provisioning in HE
2. Toolkit of existing and to be built open source tools
3. Collection of implementation stories based on 1 & 2
Does it makes sense for Access Management to adopt a similar approach?
Could the recipes build on the work already in progress in MACE-Paccman?https://spaces.at.internet2.edu/display/macepaccman/Access+Management+Recipe++V2

It appears that Policy Enforcements Points are a big gap in the current Grouper/KIM capabilities. Should PEPs for common HE applications (uPortal, Sakai, Kuali,...) and common infrastructure (CAS, Shib, etc) be added to the roadmap?

> *Tom: Grouper has specific integration components for some of these (uPortal, Kuali, shib), though they enable rather than replace the intrinsic PEP capabilities of those products. Which is generally Grouper's mission: enable really good management of access-related info and enable its integration into many application contexts with good provisioning, multiple APIs, and app-specific integration when that makes sense.*
>
> *There has not yet been a use case expressed by the community for building an actual app-specific PEP external to any specific app. And the integrative approach seems to obviate the need for one, which in any case would duplicate existing functionality within apps.*
>
> *But perhaps we're saying the same thing with different terms.*

Externalizing PDP/PEP functionality overtime will tend to put significant load on Grouper/KIM. Are the scaling characteristics of each well known? Should this be a deliverable on the roadmap?

> *Tom: Grouper currently includes a PDP capability. It's true that we do not currently profile its performance as we do with many other aspects of grouper's operation. We should add that to the profiling rig.*

What does it mean to drive federation deep into the IAM architecture from an access management perspective?

Would it be helpful to show how features and components of Grouper/KIM (in conjunction with Provisioning) satisfy various use cases described by MACE-Paccman?https://spaces.at.internet2.edu/display/CAMPJune2009/Access+Management+Use+Cases+Organized+by+Area+of+Interesthttp://www.educause.edu/sites/default/files/library/presentations/CAMP092/GS03/categorizing%2Buse%2Bcases_02.ppt

> *Tom: This was done for 6 benchmark use cases identified by the paccman group. Some of those should probably be updated in light of grouper capabilities developed since then.*
>
> *Grouper has deep support for federation and access management in a federated context. Its Subjects are not constrained to local Subject Sources and there is a UI to invite or conscript external Subjects into a grouper instance. Multiple grouper instances can themselves be federated to cooperatively manage common groups between them. Grouper is the access management layer in several production VO platforms, which demonstrates its viability for that environment.*

What does API/data harmonization provide potential adopters beyond the current robust set of capabilities already present in Grouper/KIM?

> *Tom: The idea here, like the rest of OSIdM, is to recognize that different adopters will have different circumstances and different needs, and hence to let them choose the components that best fit both. If a site starts out with KIM then wants to add grouper capabilities, or vice versa, we'd like the two to integrate as simply as possible, and eventually to integrate as simply as possible with other wares under the CIFER umbrella.*

Regarding recommendation #1, should O4 consider leveraging open standards such as SCIM rather rather than building system specific API?http://www.simplecloud.info/specs/draft-scim-rest-api-01.html

> *Tom: IMO, SCIM isn't designed to enable rich access management capabilities - I look at it more as a simple synchronization paradigm, closer to provisioning than access management. There are good reasons why grouper's and KIM's interfaces have so many methods and objects, and there are good reasons why SCIM has so few. This indicates that they are attacking very different problems.*

Where does the creation of accounts for access to VPN, Windows desktop, various web applications applications fall? Provisioning, Access Management, or both?

Tom: Provisioning, in conjunction with PersonReg & access mgmt. Ie, the identities to be given credentials and credential management capabilities reside in PersonReg. Provisioning might be constrained by access management (eg, which actors have which provisioning permissions), and provisioned artifacts might include attributes/groups/roles/perms in addition to credentials.