Grouper BOF 17-Oct-2017-at-TechEx

Grouper BoF October 17, 2017 at TechEx in San Francisco

Slides here:

https://meetings.internet2.edu/media/medialibrary/2017/10/25/20171017-hyzer-grouper-bof.pdf

Grouper Product Roadmap

Discussion

Shilen Patel, Duke

- Working to improve GSH - previously Grouper used Beanshell
- GrouperShell (gsh)
- Grouper 2.3 uses Groovy Shell - it's mostly backwards compatible, with previous scripts you may have, let the Grouper Dev team know if you have issues.
- Instrumentation - adding the instrumentation thread to Grouper Web services - Keeps track and reports back to the database

- Real time loader - Grouper loader - each time a loader job runs it gets the relevant data from Grouper and does same in source data (LDAP). Does a comparison of the 2. Could take seconds or longer. Real time loader makes updates happen faster. Integration now added to LDAP loader. Uses messaging not just database triggers.   Process reads from changelog. Notifies message queue there was a change.

- Can filter by date… Group adds and deletes
- Can see the results by hour.
- Instrumentation work is ongoing, as TIER has more requirements   Grouper instrumentation

Chris Hyzer, U Penn

- working on attestation in the new Grouper UI -- Grouper attestation
- Example of how a feature will be developed with Grouper
- Can look at it with attestation specific lens
- Same type of set up.
- Global Screen to see which groups are testable
- Attestation is when you want to be reminded periodically to review the group membership
- Can manage the attestation configuration on folders and groups
- Deprovisioning in the new UI -- get a screen with all the direct assignments in Grouper for that user -- permissions are assigned to roles. Direct permissions are assigned to memberships.

- If Grouper is not system of record for an authorization -- it can email the outside system such as Remedy.
- Accessibility has been improved, thanks U. Colorado
-
- Messaging Strategies - Grouper Messaging System
- RabbitMQ
-
- Migrated External users screen from LITE UI to new UI Grouper new UI
-

Bert Bee Lindgren- Georgia Tech

- working on provisioning
- PSP NG focuses on LDAP provisionin
- M Gettes asks for a notification mechanism
- Include the composite groups and have the overall in there based on a suffix or a prefix
- Can do that in the config -- perhaps should make it global
- Change separator for posix group, it takes group path as the CN, the colons are not friendly with the applications using those groups…
- Bert: you define the template, and you can use Java string manipulation to replace colons.

- Single group in Grouper being published to multiple LDAPs. That is supported

===

- Performance - there was an observation on the Grouper users list that emptying a 50K member group is not efficient… A full sync is more efficient. Will take advantage of that in automatic way
- With real queuing system, won't get stuck as often

- Hope to support more end points.
- Office 365 perhaps. Please talk with Bert if you have thoughts

=====

Chris:

- before we release Grouper 2.4, hope to do deprovisioning, improve UI issues
- Migrate from Vdlap to LDAPtive
- Membership reports where you go to group or folder -- show me all the people not active
- Database DDL work
- Store configuration info in database
- Hope for release by Jan 2018

==

After Grouper 2.4

- More provisioning targets
- More UIs
- Packaging improvements

=====

Bill Thompson - Lafayette

- Thanks to everyone who contributed to the TIER Grouper Deployment Guide
- Link is here: TI.25.1
- Using the community experience
- Better documentation will make your project more successful
- Focus on Sections 5 and 6 if you don't have time to read whole Grouper Deployment Guide
- NIST 800-162 is very helpful - took models from that
- Grouper terminology and layered access management terminology on top
- TIER Folder and Group Design
- Access Control models
- Security program is coming together w Identity and Access management

===

- M. Gettes asks about attestation w rules, where if you don't act on it, something happens .
- Good idea
- Ties into a rules UI
- Right now was have expire dates on memberships but not groups. Should have on groups
- we have rules, that is hard to configure, an admin has to use GSH, Making triggers more manageable with UI
- Overlap in provisioning between Grouper , Midpoint and COmanage . They all have some provisioning capability.
- There is an issue that many people can create groups, they will and do forget about them. Old stuff does not get cleaned up. Have expire dates for Grouper with attestation. Detect when a group is not being used. No membership changes or reads.

Contributing your Campus Deployment Story

Please contact emily@internet2.edu if you have a campus deployment story to contribute here

Community Contributions

Advance CAMP sessions on Grouper

- Grouper Deployment Guide 2.0
- https://docs.google.com/document/d/19I-Phm9PbPJB6RgRk-_WKF0mr-3c4A7B354N_gSCbw0/edit

- Grouper Provisioning Topics
- https://docs.google.com/document/d/1oCfUKYckK-fnfgNcmy5uphsF–tvcxZNa5ZJkaL2dmk/edit#

- Dockeriing Grouper
- https://docs.google.com/document/d/1oUlR3B1Pk6KeGXVQOz-Oh5sZC8FtoZ8qYewE_UW063w/edit

Links to the slides used at the Oct 15, 2017 Grouper in Action Tutorial are here:

- Documents & Presentations