INTERNET2®

2017 TECHNOLOGY exchange

SAN FRANCISCO CA OCTOBER 15-18

GROUPER BOF

Chris Hyzer, University of Pennsylvania
Shilen Patel, Duke
Bert Bee-Lindgren, Georgia Tech
Bill Thompson, Lafayette College

Grouper BOF

- Welcome
- Agenda Bash
- Core Team
- What is Grouper
- Grouper and TIER
- Progress since Global Summit
- Roadmap and Scheduling
- TIER Grouper Deployment Guide
- Community Contributions
- Discussion

Grouper Core Team

- Chris Hyzer (Penn) - Grouper lead, API, WS, and UI
- Shilen Patel (Duke) - API and everything else
- Bert Bee-Lindgren (Georgia Tech) - provisioning
- Vivek Sachdeva (independent) - WS
- Emily Eisbruch (Internet2) - work group support
- Chad Redman (UNC) – starting with build and dependency management
- Jim Fox (University of Washington) – conference calls
- Bill Thompson

What is Grouper?

- Central authorization
- Groups
- Permissions
- Provisioning
- Auditing
- Delegation and distributed management

Grouper and TIER

TIER provides:

- Requirements for development
- Funding
- Architectural guidance
- Standards to harmonize with other TIER products
- Contributions in areas such as: packaging, security, administrative help, etc

Grouper progress in last 6 months

Note, most or all of these things are in 2.3.0 patches

- GSH(ng)
- Instrumentation on UI
- Real time loader with messaging (works with LDAP)
- Attestation update in UI
- Started on deprovisioning in UI
- Improved grouper daemon logging
- UI accessibility
- Add messaging strategies
- Messaging WS operations
- Messaging to WS connector to run Grouper logic from messaging
- External users migrated from Lite UI to New UI
- PSPNG

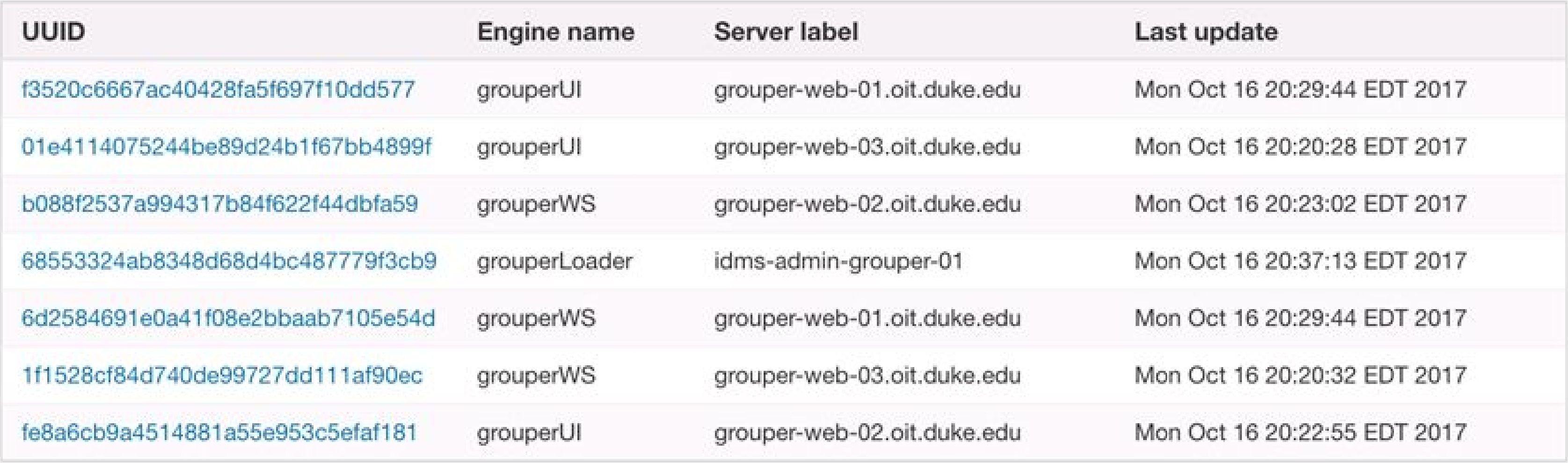
Improve GSH - GSHNG

https://spaces.internet2.edu/display/Grouper/Grouper+Shell+Improvements

- Previously Grouper used BeanShell
  - Not the most user friendly implementation - no history, tab completion, etc.
- Grouper 2.3 patch switches to Groovy as the default shell
  - Backwards compatible (mostly)
  - Built in GSH commands all work as before
  - History, tab completion, etc
  - Custom Groovy scripts/methods.
  - If you have issues, you can revert back to BeanShell by a simple configuration setting

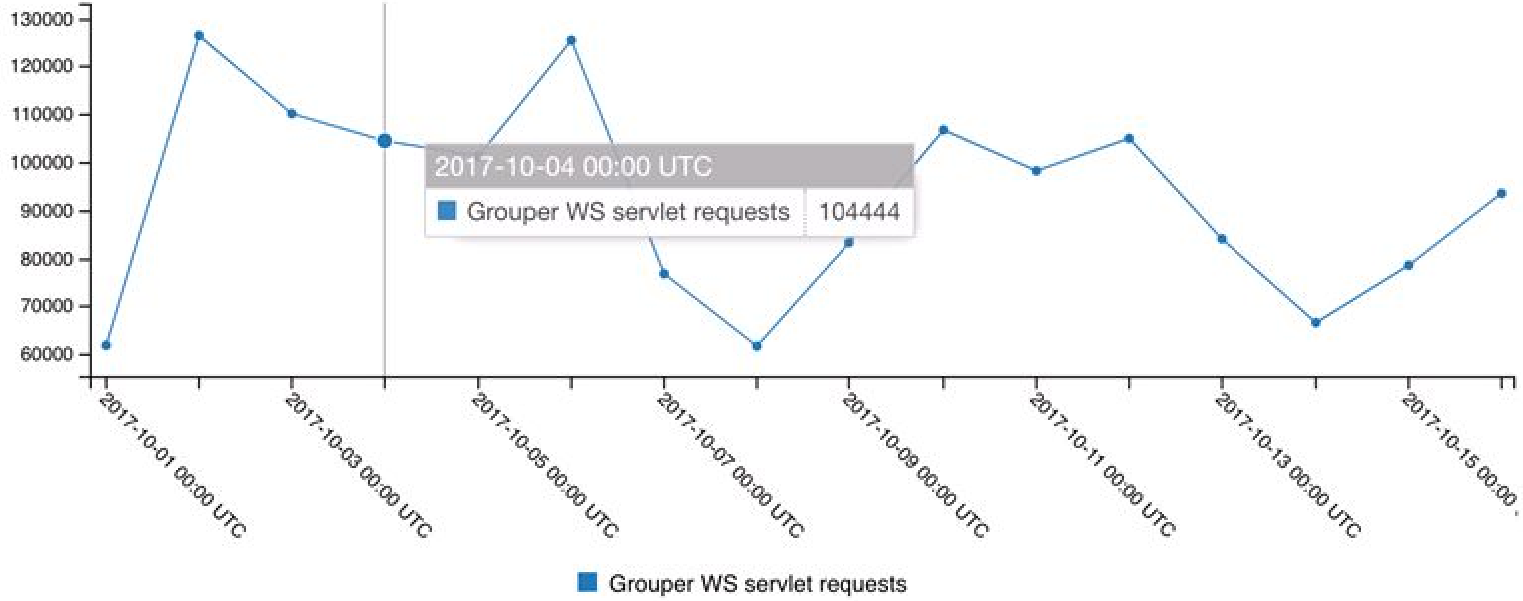
Added instrumentation thread to Grouper WS

https://spaces.internet2.edu/display/Grouper/Grouper+instrumentation



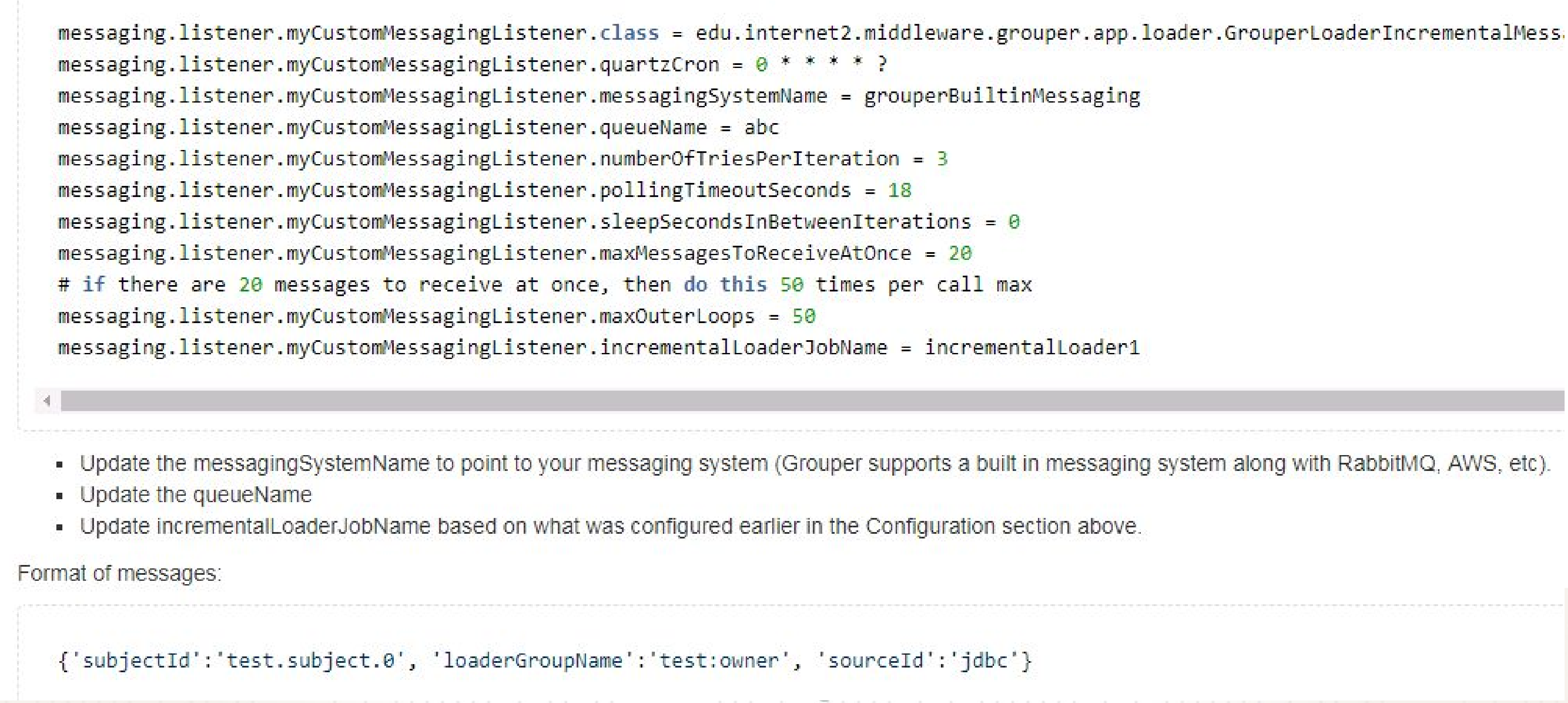
UUID	Engine name	Server label	Last update
f3520c6667ac40428fa5f697f10dd577	grouperUI	grouper-web-01.oit.duke.edu	Mon Oct 16 20:29:44 EDT 2017
01e4114075244be89d24b1f67bb4899f	grouperUI	grouper-web-03.oit.duke.edu	Mon Oct 16 20:20:28 EDT 2017
b088f2537a994317b84f622f44dbfa59	grouperWS	grouper-web-02.oit.duke.edu	Mon Oct 16 20:23:02 EDT 2017
68553324ab8348d68d4bc487779f3cb9	grouperLoader	idms-admin-grouper-01	Mon Oct 16 20:37:13 EDT 2017
6d2584691e0a41f08e2bbaab7105e54d	grouperWS	grouper-web-01.oit.duke.edu	Mon Oct 16 20:29:44 EDT 2017
1f1528cf84d740de99727dd111af90ec	grouperWS	grouper-web-03.oit.duke.edu	Mon Oct 16 20:20:32 EDT 2017
fe8a6cb9a4514881a55e953c5efaf181	grouperUI	grouper-web-02.oit.duke.edu	Mon Oct 16 20:22:55 EDT 2017

Added instrumentation thread to Grouper WS



Real-time loader from message

https://spaces.internet2.edu/display/Grouper/Grouper+loader+real+time+updates



```
messaging.listener.myCustomMessagingListener.class = edu.internet2.middleware.grouper.app.loader.GrouperLoaderIncrementalMess
messaging.listener.myCustomMessagingListener.quartzCron = 0 * * * * ?
messaging.listener.myCustomMessagingListener.messagingSystemName = grouperBuiltinMessaging
messaging.listener.myCustomMessagingListener.queueName = abc
messaging.listener.myCustomMessagingListener.numberOfTriesPerIteration = 3
messaging.listener.myCustomMessagingListener.pollingTimeoutSeconds = 18
messaging.listener.myCustomMessagingListener.sleepSecondsInBetweenIterations = 0
messaging.listener.myCustomMessagingListener.maxMessagesToReceiveAtOnce = 20
# if there are 20 messages to receive at once, then do this 50 times per call max
messaging.listener.myCustomMessagingListener.maxOuterLoops = 50
messaging.listener.myCustomMessagingListener.incrementalLoaderJobName = incrementalLoader1
```

- Update the messagingSystemName to point to your messaging system (Grouper supports a built in messaging system along with RabbitMQ, AWS, etc).
- Update the queueName
- Update incrementalLoaderJobName based on what was configured earlier in the Configuration section above.

Format of messages:

```
{'subjectId':'test.subject.0', 'loaderGroupName':'test:owner', 'sourceId':'jdbc'}
```

Attestation in New UI

https://spaces.internet2.edu/display/Grouper/Grouper+attestation

- Global screen to see attestable groups
- Global screen to see attestation configuration
- Folder level screen to see attestable groups
- Folder level screen to see attestation configuration
- Manage attestation on folders or groups
- See attestation on manage members screen
- See audits
- Demo

Deprovisioning UI

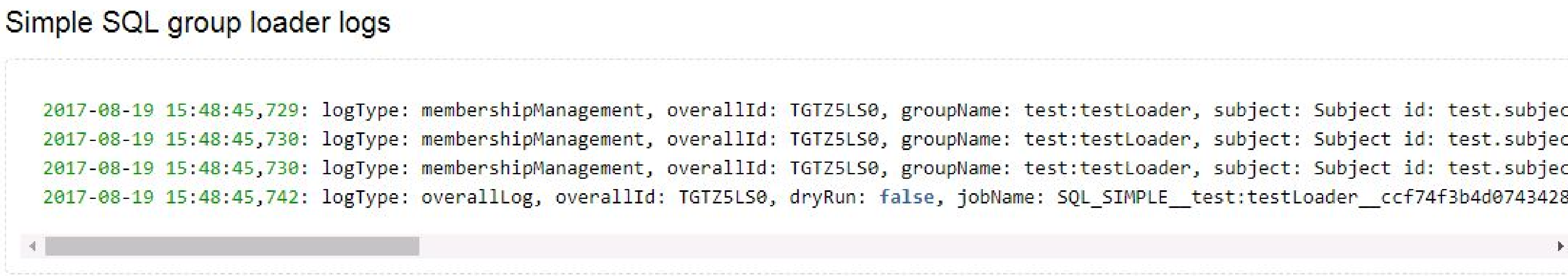
https://spaces.internet2.edu/display/Grouper/Grouper+deprovisioning

- Allow deprovisioning admins (HR?) to deprovision users
- See all direct access assignments (eligible for deprovisioning)
- Notify system admins where Grouper is not the system of record
- Configure deprovisioning on folders or groups
- Audit
- Reprovision the same user or another user
- Restrict users from loader jobs (temporarily)
- See current screens

Improved Grouper Daemon logging

https://spaces.internet2.edu/display/Grouper/Grouper+daemon+log

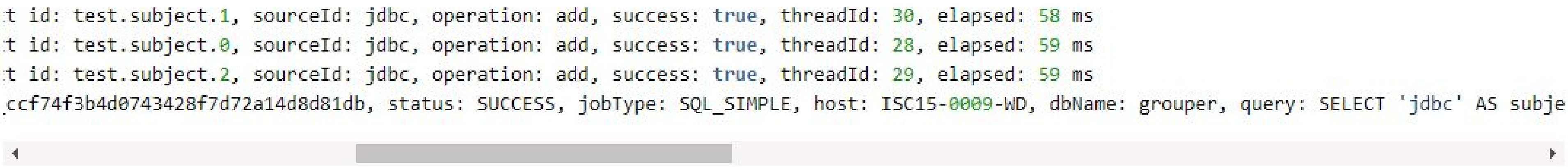
- Logs go to dedicated file (or syslog or whatever configured in log4j.properties)



Simple SQL group loader logs

```
2017-08-19 15:48:45,729: logType: membershipManagement, overallId: TGTZ5LS0, groupName: test:testLoader, subject: Subject id: test.subjec
2017-08-19 15:48:45,730: logType: membershipManagement, overallId: TGTZ5LS0, groupName: test:testLoader, subject: Subject id: test.subjec
2017-08-19 15:48:45,730: logType: membershipManagement, overallId: TGTZ5LS0, groupName: test:testLoader, subject: Subject id: test.subjec
2017-08-19 15:48:45,742: logType: overallLog, overallId: TGTZ5LS0, dryRun: false, jobName: SQL_SIMPLE__test:testLoader__ccf74f3b4d0743428
```

Improved Grouper Daemon logging (continued)



```
t id: test.subject.1, sourceId: jdbc, operation: add, success: true, threadId: 30, elapsed: 58 ms
t id: test.subject.0, sourceId: jdbc, operation: add, success: true, threadId: 28, elapsed: 59 ms
t id: test.subject.2, sourceId: jdbc, operation: add, success: true, threadId: 29, elapsed: 59 ms
ccf74f3b4d0743428f7d72a14d8d81db, status: SUCCESS, jobType: SQL_SIMPLE, host: ISC15-0009-WD, dbName: grouper, query: SELECT 'jdbc' AS subje
```

```
query: SELECT 'jdbc' AS subject_source_id, subjectId AS subject_id FROM SUBJECT WHERE subjectId IN
('test.subject.0', 'test.subject.1', 'test.subject.2'),

rowsFromExternal: 3, rowsFromGrouper: 0,
deleteCount: 0, insertCount: 3, updateCount: 0, totalCount: 3,
millisGetData: 25, millisLoadData: 70, threadId: 1, elapsed: 156 ms
```

UI accessibility improvements

- Report from Colorado
- Fixed the issues, committed to github
- Reviewed by Colorado
- Patched

Messaging strategies

- RabbitMQ (AMQP)

https://spaces.internet2.edu/display/Grouper/Grouper+Messaging+with+RabbitMQ

Note: this is running on the demo server with TLS

- ActiveMQ

https://spaces.internet2.edu/display/Grouper/Grouper+Messaging+with+ActiveMQ

- AWS

https://spaces.internet2.edu/display/Grouper/Grouper+Messaging+with+AWS+SQS

- Of course there is the built-in messaging that uses the Grouper database

Messaging WS operations

- Also included in grouper client
- Send a message

https://spaces.internet2.edu/display/Grouper/Message+Send

- Receive a message

https://spaces.internet2.edu/display/Grouper/Message+Receive

- Mark a message as processed

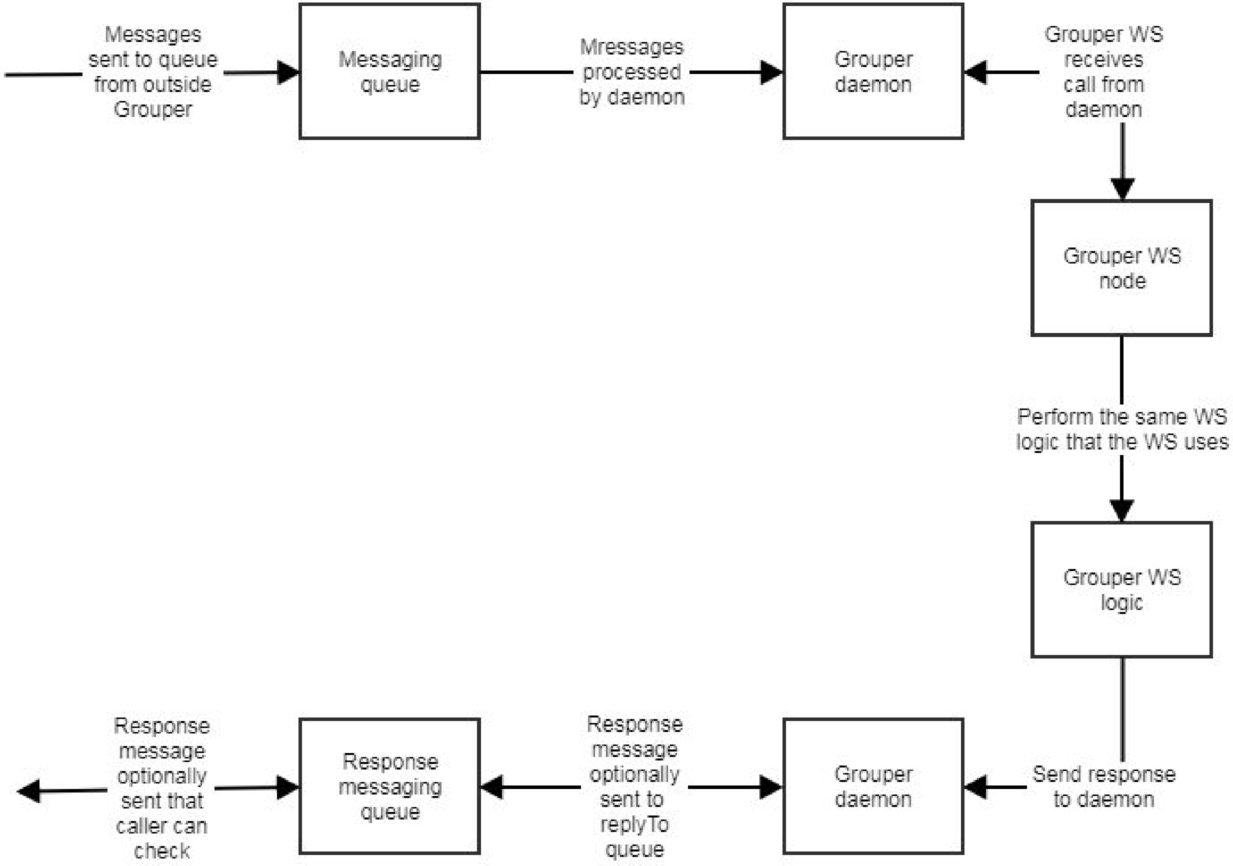
https://spaces.internet2.edu/display/Grouper/Message+Acknowledge

Messaging to WS connector

- Grouper listens on a queue and proxies to WS
- Can add member, remove, view, etc

https://spaces.internet2.edu/display/Grouper/Grouper+messaging+to+web+service+API

Messaging to WS connector



Messages sent to queue from outside Grouper

Messaging queue

Mressages processed by daemon

Grouper daemon

Grouper WS receives call from daemon

Grouper WS node

Perform the same WS logic that the WS uses

Grouper WS logic

Send response to daemon

Grouper daemon

Response message optionally sent to replyTo queue

Response messaging queue

Response message optionally sent that caller can check

External users migrated to New UI

- This work is in git will be in a patch soon (default to off)

Provisioning - PSPNG Background

- Definition: Grouper Provisioning
  - Reflecting Group Memberships in remote systems
    - LDAP, Office 365, Wiki, Duo, LMS, Active Directory, G-Suite, ….
  - Data: Memberships & Group Information
- History of Grouper Provisioning
  - Lots of point solutions, added by sites
  - < 2.3: Grouper PSP - Very Flexible, Complicated and Slow
  - **2.3: Grouper PSPNG - Less Flexible, but simple and fast**
- Goals for PSPNG
  - Simple to configure
  - Just enough flexibility and controls
  - Growing list of targets
  - Fast

Provisioning - PSPNG Current

Current Functionality: (v2.3)

- LDAP Targets
  - LDAP Groups
    - Both member-required and member-optional schemas
  - LDAP Attributes
  - Active Directory Groups
- Incremental Provisioning with periodic Full Syncs
- Messaging: On-demand full syncs
- Automated QA - Integration Tests (docker)
- Password encryption
- Improvements to Bushy Group Folders
- FullSync Improvements: Status feedback
- Updating (non-membership) group attributes [Coming Soon]

Provisioning - PSPNG Roadmap

Ongoing (v2.3 patches)

- Bugs & Gaps
  - Total control of provisioned attribute (prefix=*)
  - Multi-schema groups (multiple membership attributes)
  - Cleaning up empty OUs
- Provisioning & UI:
  - Easier group/folder selection
  - Initiate full-sync from UI
  - See last/current full-sync status/progress
  - Last full-sync summary (adds/removes/correct)
  - Deprovisioning SafetyNets: Alerts & Overrides
  - DN, Attribute, etc of provisioned destination
- Performance: Perform FullSyncs under heavy change

V2.4

- Message-driven provisioning - especially error recovery
- New Endpoints, possibly:
  - Azure / Office 365: Feedback?
  - G-Suite
  - Dropbox

Grouper Roadmap - to do for 2.4

https://spaces.internet2.edu/display/Grouper/Grouper+Product+Roadmap

- Deprovisioning in UI
- Replace Admin and Lite UI with “New UI”
- Provisioning in UI
- Migrate from vt-ldap to ldaptive
- Membership reports first pass?
- Add columns for group expiry, membership notes?
- Allow ability to store configuration in the database
- Release Jan 2018 hopefully

Grouper Roadmap - after 2.4

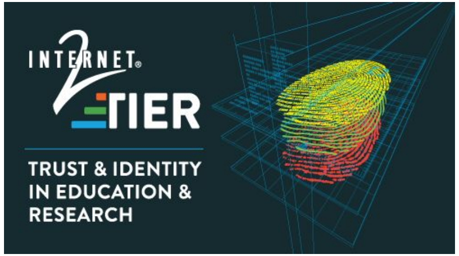
https://spaces.internet2.edu/display/Grouper/Grouper+Product+Roadmap

- Provisioning
  - Improvements
  - More targets
- Add more WS operations
- Add more TIER API operations
- Get more institutions to use the TIER API and packaging
- More UIs for:
  - Attributes
  - Configuration
  - Rules
- Group expire dates
- <Add your item here>

TIER Grouper Deployment Guide

Bill Thompson

Director Digital Infrastructure, Lafayette College



James Babb
Tom Dopirak
TIER API and Entity Registry WG
Grouper Development Team
Community Contributions

Albert Wu - UCLA
Bert Bee-Lindgren - Georgia Tech
Bill Kaufman - Internet2
Bill Thompson - Lafayette College
Brian Savage - Boston College
Brian Woods - Rice
Carey Black - The Ohio State University
Chris Hyzer - Penn
Dean Lane - Rice
Emily Eisbruch - Internet2
Eric Goodman - UCOP
Ethan Disabb - University of Florida
Ethan Kromhout - UNC Chapel Hill
Gabor Eszes - Old Dominion
Gary Brown- University of Bristol
Harry Samuels - Northwestern
James Babb - UW Madison
Jill Gemmill - Clemson
Jim Fox - University of Washington
Tom Jordan - UW Madison
Tom Zeller
Warren Curry - University of Florida
Jon Finke - RPI
Jon Miner - UW Madison
José Cedeño - Oregon State University
Keith Hazelton - UW Madison
Keith Wessel - University of Illinois
Ken Koch - Washington University
Maarten Kremers - SURFnet
Mark McCahill - Duke
Michael Gettes - Penn State
Michael Hodges - University of Hawaii
Mike Zawacki - Internet2
Paul Caskey - Internet2
Raoul Sevier - Harvard
Rob Carter - Duke
Scott Cantor - The Ohio State University
Shilen Patel - Duke
Steve Carmody - Brown
Steve Moyer - Penn State
Steve Zoppi - Internet2
Tom Barton - University of Chicago
Tom Dopirak - “Retirement”

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

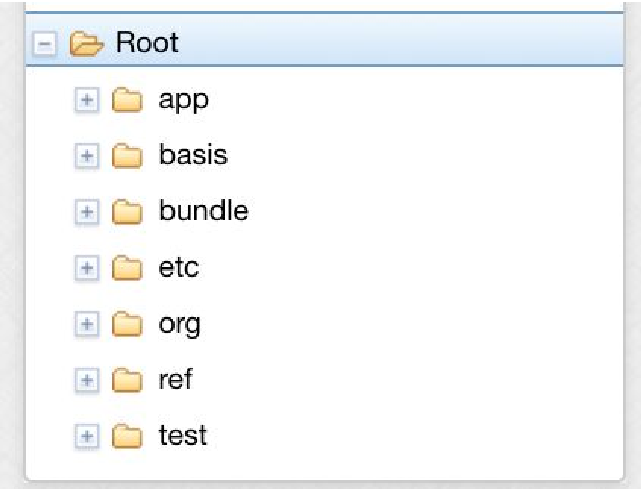
- NIST 800-162 ABAC
- Grouper glossary
- Grouper UI terminology

- **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

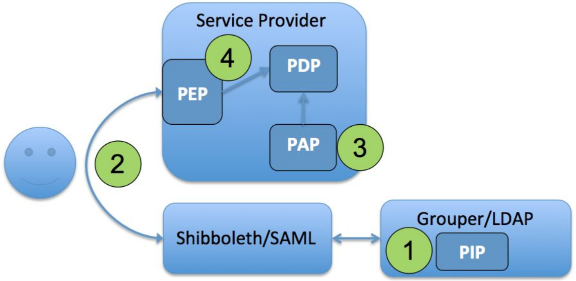
- **Basis group** – direct subject membership, low level, "raw" groups
- **Reference group** – institutionally meaningful cohorts
- **Access/Account policy group** – pre-computed policy decision

TIER Folder and Group Design

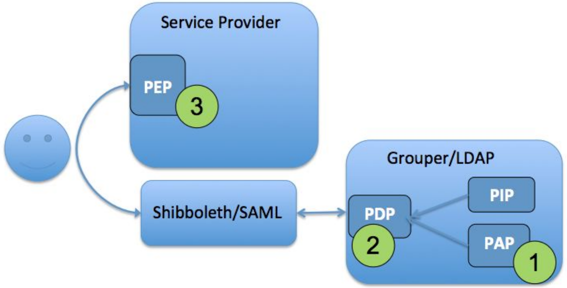
"Just having a plan or standard has been quite helpful, as it allows implementers to get on with real work without having to stumble on how to name things or where to stick them." - Tom Barton



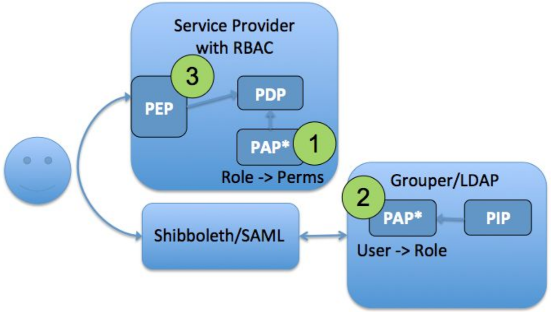
Access Control Models



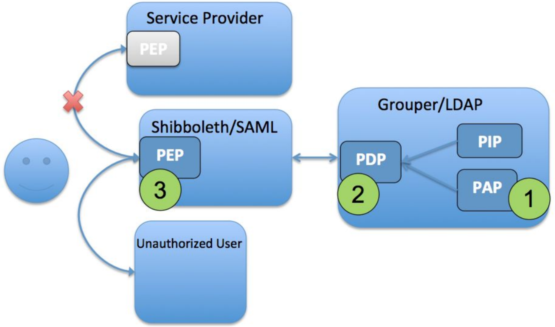
ACM1 - eduPersonAffiliation



ACM2 - eduPersonEntitlement



ACM3 - Application RBAC



ACM4 - WebSSO short-circuit

Grouper Deployment Guide Outcomes

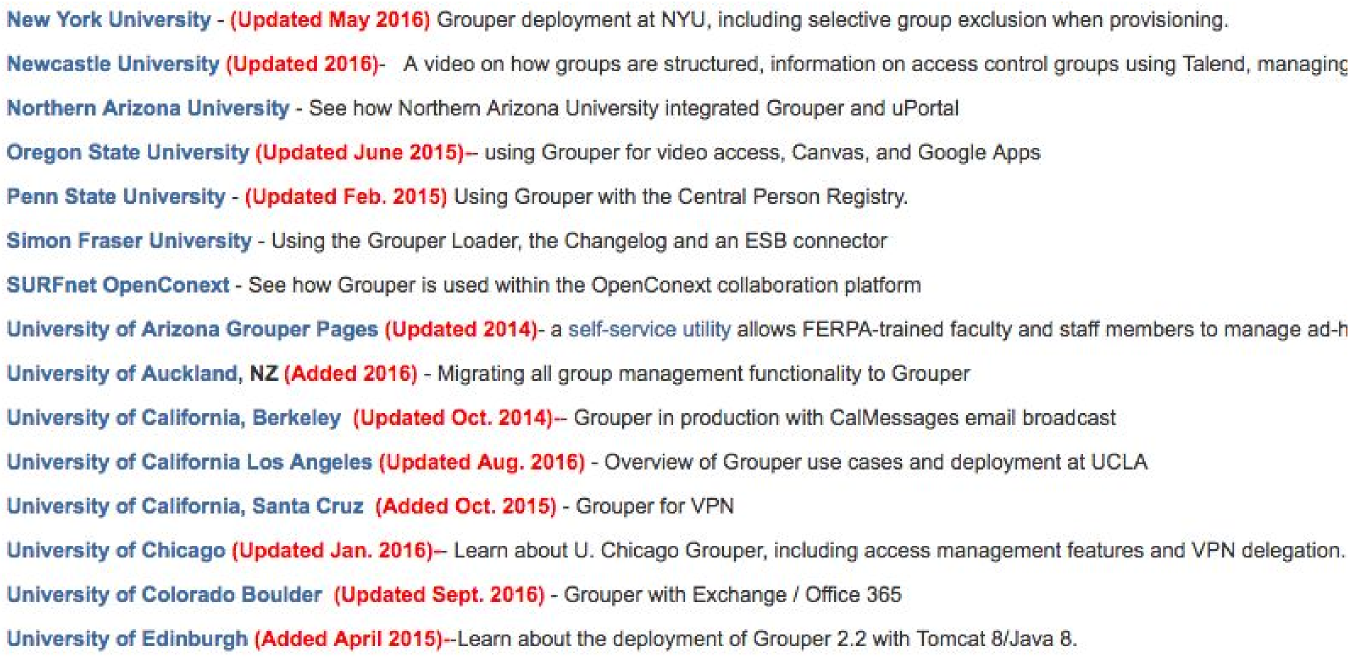
- Model and Terminology
  - Basis –> reference –> policy
  - Reference groups = subject attributes (institutionally meaningful cohorts)
  - Strategy applies to all four access control models

- 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

ACAMP Ideas

- Deep dive into basis and reference groups
- Deep dive into TIER provisioning models
  - pspng, rabbitmq, midpoint, comanage
- TIER Grouper Deployment Guide next steps
  - TIER component integration
  - More operational guidance
  - Real world config examples, How-tos
- Grouper product vision and design goals
  - TIER based capabilities
  - Grouper/folder UI hints
  - Rules/Attributes UI

Grouper Community Contributions on the Grouper wiki



New York University - (Updated May 2016) Grouper deployment at NYU, including selective group exclusion when provisioning.

Newcastle University (Updated 2016)- A video on how groups are structured, information on access control groups using Talend, managing

Northern Arizona University - See how Northern Arizona University integrated Grouper and uPortal

Oregon State University (Updated June 2015)– using Grouper for video access, Canvas, and Google Apps

Penn State University - (Updated Feb. 2015) Using Grouper with the Central Person Registry.

Simon Fraser University - Using the Grouper Loader, the Changelog and an ESB connector

SURFnet OpenConext - See how Grouper is used within the OpenConext collaboration platform

University of Arizona Grouper Pages (Updated 2014)- a self-service utility allows FERPA-trained faculty and staff members to manage ad-h

University of Auckland, NZ (Added 2016) - Migrating all group management functionality to Grouper

University of California, Berkeley (Updated Oct. 2014)-- Grouper in production with CalMessages email broadcast

University of California Los Angeles (Updated Aug. 2016) - Overview of Grouper use cases and deployment at UCLA

University of California, Santa Cruz (Added Oct. 2015) - Grouper for VPN

University of Chicago (Updated Jan. 2016)– Learn about U. Chicago Grouper, including access management features and VPN delegation.

University of Colorado Boulder (Updated Sept. 2016) - Grouper with Exchange / Office 365

University of Edinburgh (Added April 2015)--Learn about the deployment of Grouper 2.2 with Tomcat 8/Java 8.

Grouper Community Contributions

Share your Grouper experience on the Grouper wiki

- Update it from time to time
- https://spaces.internet2.edu/display/Grouper/Community+Contributions
- See or email Emily Eisbruch (emily@internet2.edu) for help setting up your Grouper contributions page

Thanks to all those who have recently updated their Grouper Contrib page!

Staying Informed/Get Involved with Grouper

- Join the Grouper-Users email list
  - To subscribe:

    Email pubsympa@internet2.edu with the subject (case insensitive):

    subscribe grouper-users

INTERNET2®

2017 TECHNOLOGY exchange

SAN FRANCISCO CA OCTOBER 15-18

THANK YOU FOR ATTENDING THE GROUPER BOF

Subtitle (if any)