2018 TECHNOLOGY exchange

ORLANDO FL OCTOBER 15-18

Grouper Birds of a feather

PRESENTER NAME:

Chris Hyzer, Penn
Shilen Patel, Duke
Bill Thompson, Lafayette
Bert Bee-Lindgren, Georgia Tech
John Gasper, Unicon
Chad Redman, UNC

INTERNET2

Grouper BOF

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

Grouper Team (alphabetical) - people who worked on Grouper in last 6mo

- **James Babb** (Internet2) - Trainer
- **Bert Bee-Lindgren** (Georgia Tech) - provisioning
- **Carey Matt Black** (Ohio State) – general support
- **Emily Eisbruch** (Internet2) - work group support
- **John Gasper** (Unicon) - Grouper Training Environment, connectors
- **Chris Hyzer** (Penn) - Grouper lead, API, WS, and UI
- **Shilen Patel** (Duke) – API, loader, UI
- **Chad Redman** (UNC) – Build and dependency management, UI
- **Vivek Sachdeva** (independent) – WS, UI
- **Bill Thompson** (Lafayette) – Grouper Deployment Guide, Training Environment
- **Carl Waldbieser** (Lafayette) - Trainer

What is Grouper?

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

Grouper and TIER

TIER delivers a packaged suite of components (Shibboleth Identity Provider, **Grouper**, COmanage, midPoint) with a set of APIs to provide consistency and flexibility.

TIER provides the Grouper project:

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

Grouper Roadmap

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

- Plan for Grouper 2.5
- Support 2.4
- Continue to do low impact improvement patches in 2.4
- 2.5 release in 2019 Q2

Grouper Roadmap - 2.4 patches (tentative)

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

- Tag TIER objects (ref, basis, policy, etc)
- Performance improvements
- Provisioning managed from UI
- Allow configuration to be stored in database
- Membership reports
- Simple workflow approvals
- Subject source configuration in UI

Grouper Roadmap – 2.5 (tentative)

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

- Group delete dates
- Membership notes
- “Internal” groups
- Better paging in WS
- Continue dependency updates

Grouper Community Contributions recently updated on the Grouper wiki

Carnegie Mellon University **(Updated Nov. 2017)**- Integrating Grouper with Google Apps and using the Grouper Active-MQ Provisioner (GAP) framework.

Cardiff University - Grouper deployment at Cardiff University includes an ESB Interface. (note: last updated in 2011)

Colorado State University - **(Added February 2018) -** Provisioning from Grouper to LDAP.

Columbia University - **(Added June 2016) -** Using Grouper to support email and institutional reference groups and using Grouper with Google Groups for authorization.

Consortium GARR - **(Added Oct. 2014)-** Grouper for a centralized authorization system for multiple virtual organizations.

University of Illinois Urbana-Champaign - **(Added Feb 2018)** Deploying Grouper in Amazon Web Services

University of Maryland Baltimore County - **(Added April 2017) -** groups provisioned to LDAP for access management

University of Maryland College Park - **(Added Fall 2017) -** info coming soon

University of Memphis - **(Brief note added Nov. 2014)** Running Grouper API in production.

University of Michigan - **(Added Feb 2018)** Using containerized Grouper

University of Minnesota - **(2013)** Using Grouper to manage access to BPEL workflows, VPN groups and more.

University of Montreal - **(2013)** Using Grouper for automatic and delegated group and membership management

University of Nebraska **(Updated Feb 2018)** Using Grouper to manage student, employee and residence hall data.

Yale - **(Added February 2018) -** Banner integration, Canvas integration and more

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

Grouper progress in last 6 months

2.4 release

Many bug fixes

Improvements

- Finished up deprovisioning
- Removed admin and lite UIs
- Real-time loader with LDAP
- Real-time loader in SQL can use different databases
- Enable/disable loader jobs
- Grouper templates
- PSPNG improvements
- Updated 3rd party libraries

Deprovisioning

- Register realm in config (e.g. employee, student, IT staff member)
- Identify deprovisioning admins per realm
- Handle optional deprovisioning of loader jobs
- Notify admins of applications where Grouper is read only
- See reports of inactive users

Provisioning to BMC remedy

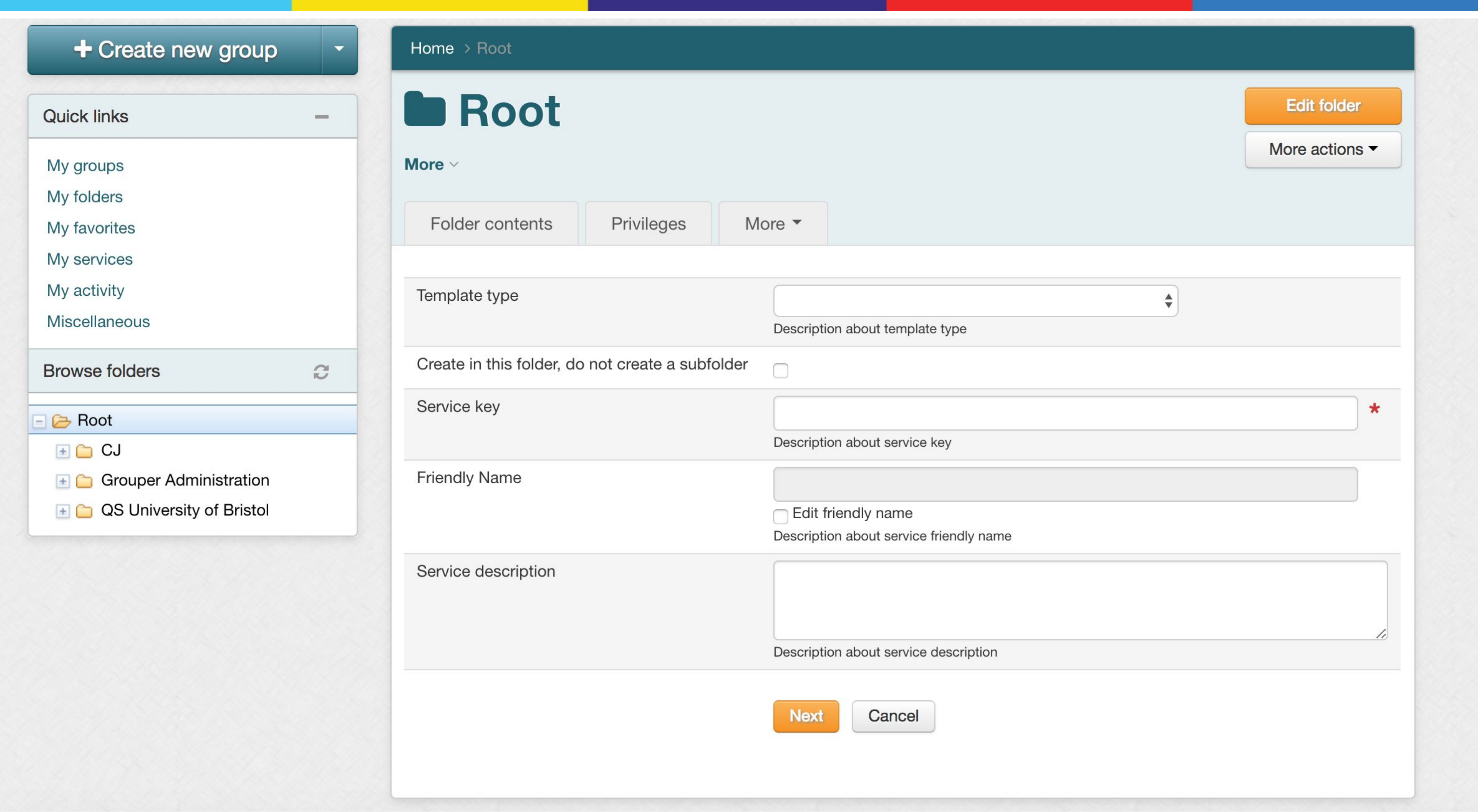
- Provision Grouper to Remedy
- Includes cloud Remedy and Remedy Digital Marketplace
- Can have Grouper groups of people who are allowed to open/view/edit cases in Remedy

Grouper templates

Vivek Sachdeva

Grouper Template Wizard

- Create structure in few clicks
- Two templates provided out of the box
- Open for extension
- Available from every folder including root
- Customizable text



Template type

Description about template type

Create in this folder, do not create a subfolder □

Service key *

Description about service key

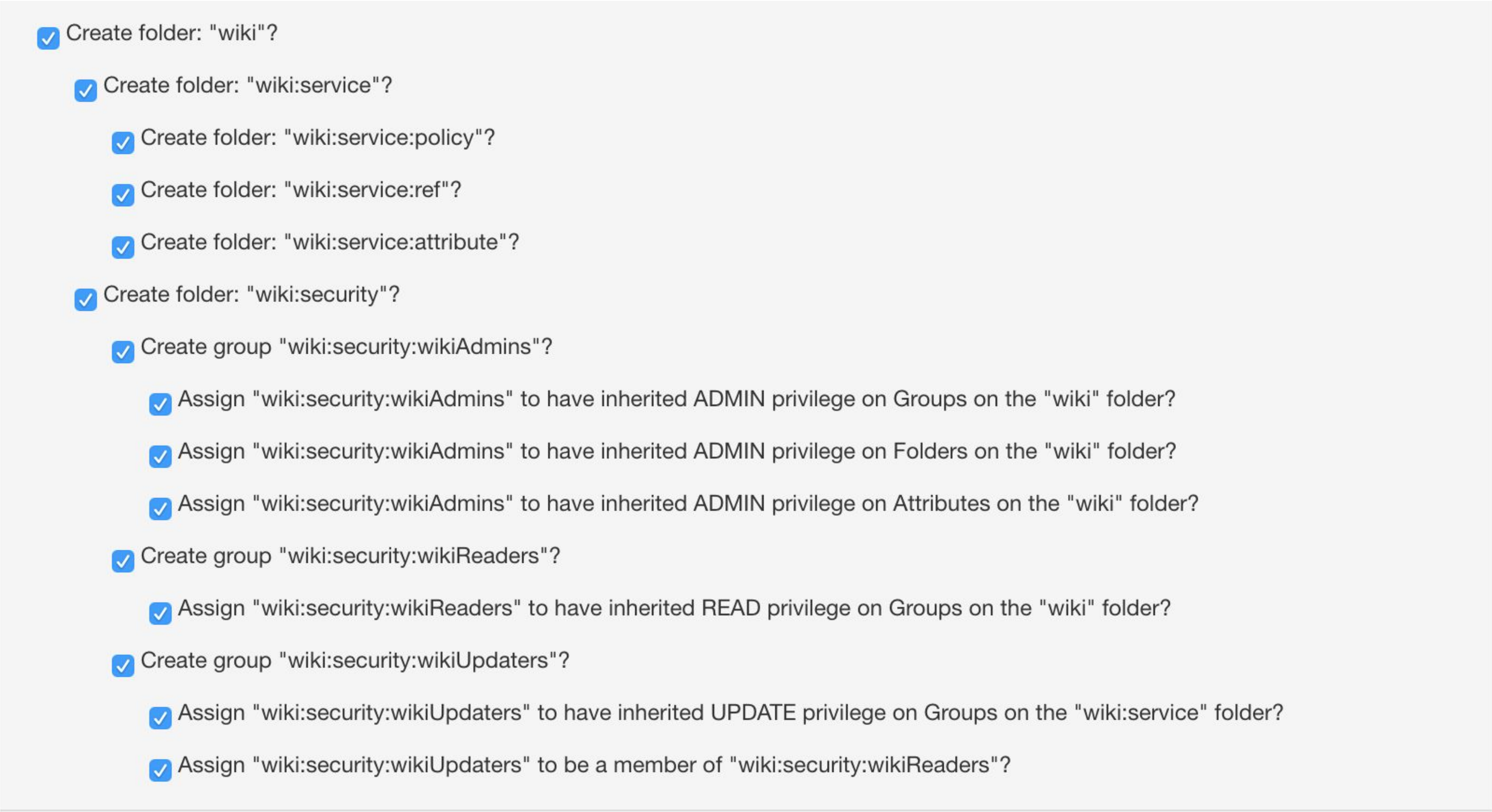
Friendly Name

□ Edit friendly name

Description about service friendly name

Service description

Description about service description



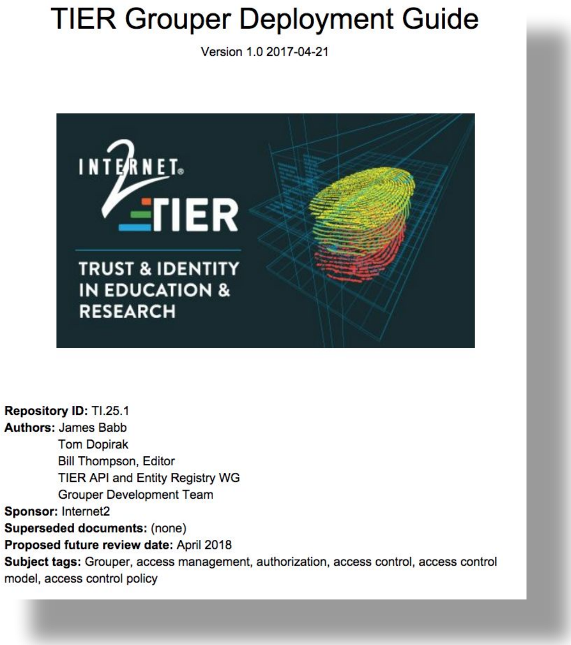
- ☑ Create folder: "wiki"?
  - ☑ Create folder: "wiki:service"?
    - ☑ Create folder: "wiki:service:policy"?
    - ☑ Create folder: "wiki:service:ref"?
    - ☑ Create folder: "wiki:service:attribute"?
  - ☑ Create folder: "wiki:security"?
    - ☑ Create group "wiki:security:wikiAdmins"?
      - ☑ Assign "wiki:security:wikiAdmins" to have inherited ADMIN privilege on Groups on the "wiki" folder?
      - ☑ Assign "wiki:security:wikiAdmins" to have inherited ADMIN privilege on Folders on the "wiki" folder?
      - ☑ Assign "wiki:security:wikiAdmins" to have inherited ADMIN privilege on Attributes on the "wiki" folder?
    - ☑ Create group "wiki:security:wikiReaders"?
      - ☑ Assign "wiki:security:wikiReaders" to have inherited READ privilege on Groups on the "wiki" folder?
    - ☑ Create group "wiki:security:wikiUpdaters"?
      - ☑ Assign "wiki:security:wikiUpdaters" to have inherited UPDATE privilege on Groups on the "wiki:service" folder?
      - ☑ Assign "wiki:security:wikiUpdaters" to be a member of "wiki:security:wikiReaders"?

Grouper Deployment Guide and Training Env

Bill Thompson

Grouper Deployment Guide (GDG)

- GDG V1 released @ Summit 2017
  - http://doi.org/10.26869/TI.25.1
- Grouper seminars
  - Tech Exchange 2017 and Summit 2018
- TIER Access Governance with Grouper and Friends
  - Tech Exchange 2018
- GDG V2 Goals
  - Updated for Grouper 2.4, and TIER packaging and architecture
  - Expand some sections – account policy, provisioning
  - New sections – grouper security model, reference group examples,…



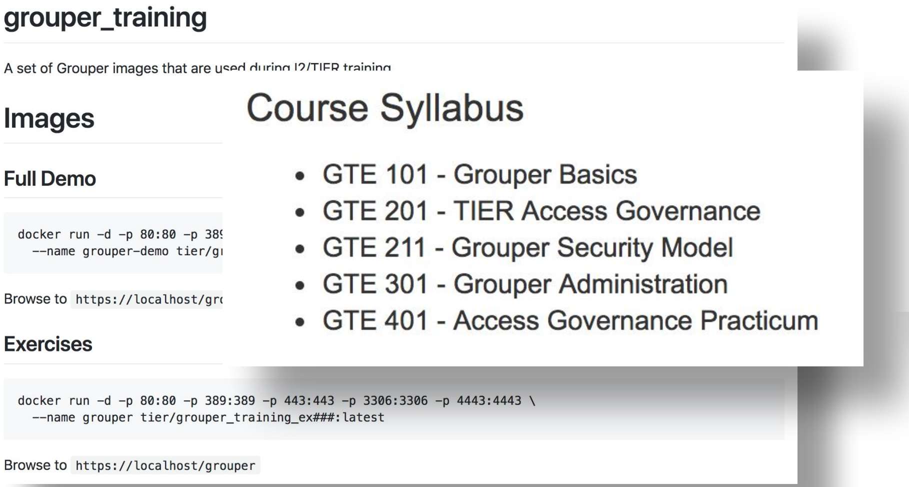
TIER Grouper Deployment Guide

Version 1.0 2017-04-21

Repository ID: TI.25.1
Authors: James Babb
Tom Dopirak
Bill Thompson, Editor
TIER API and Entity Registry WG
Grouper Development Team
Sponsor: Internet2
Superseded documents: (none)
Proposed future review date: April 2018
Subject tags: Grouper, access management, authorization, access control, access control model, access control policy

Grouper/TIER Training Environment

- Grouper/TIER Training Environment (GTE)
  - lesson plans
  - training exercises
  - supporting Docker modules



grouper_training

A set of Grouper images that are used during I2/TIER training

Images

Full Demo

```
docker run -d -p 80:80 -p 389
  --name grouper-demo tier/gr
```

Browse to `https://localhost/gro`

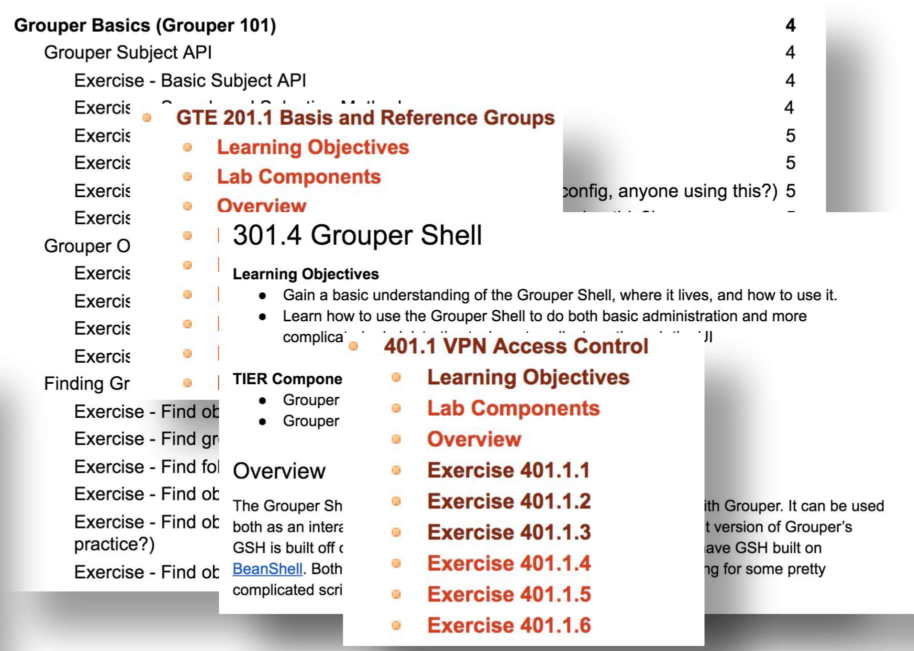
Exercises

```
docker run -d -p 80:80 -p 389:389 -p 443:443 -p 3306:3306 -p 4443:4443 \
  --name grouper tier/grouper_training_ex###:latest
```

Browse to `https://localhost/grouper`

Course Syllabus

- GTE 101 - Grouper Basics
- GTE 201 - TIER Access Governance
- GTE 211 - Grouper Security Model
- GTE 301 - Grouper Administration
- GTE 401 - Access Governance Practicum



- GTE 201.1 Basis and Reference Groups
  - Learning Objectives
  - Lab Components
  - Overview

301.4 Grouper Shell

Learning Objectives

- Gain a basic understanding of the Grouper Shell, where it lives, and how to use it.
- Learn how to use the Grouper Shell to do both basic administration and more complica

TIER Compone

- Grouper
- Grouper

Overview

The Grouper Sh ith Grouper. It can be used both as an intera t version of Grouper's GSH is built off c ave GSH built on BeanShell. Both ng for some pretty complicated scri

- 401.1 VPN Access Control
  - Learning Objectives
  - Lab Components
  - Overview
  - Exercise 401.1.1
  - Exercise 401.1.2
  - Exercise 401.1.3
  - Exercise 401.1.4
  - Exercise 401.1.5
  - Exercise 401.1.6

Real-time loader improvements

GSH improvements

Show and manage daemon jobs in UI

Shilen Patel

Real-time loader improvements

- Previously supported SQL jobs only
- Recently added support for LDAP jobs - this is available as a 2.4 patch
- You can allow changes in your LDAP to trigger messages to Grouper that would trigger all LDAP jobs for the impacted user.
- Also fixed a couple of bugs
- https://spaces.at.internet2.edu/display/Grouper/Grouper+loader+real+time+updates

GSH improvements

- Previously, GSH always returned an exit code of 0 even during failures. That's been fixed to return the exit code from Groovy.
- Also, previously if you were running a GSH script, if any line in the script failed, it would continue to the next line. Now there's an option to immediately exit (with a non-zero return code) if that happens.
- Also, previously if you were starting GSH and there was a problem with your subject source configuration, it would still start up. Now there's an option to also exit immediately (with a non-zero return code).
- This is also available as a 2.4 patch (currently as a test patch).

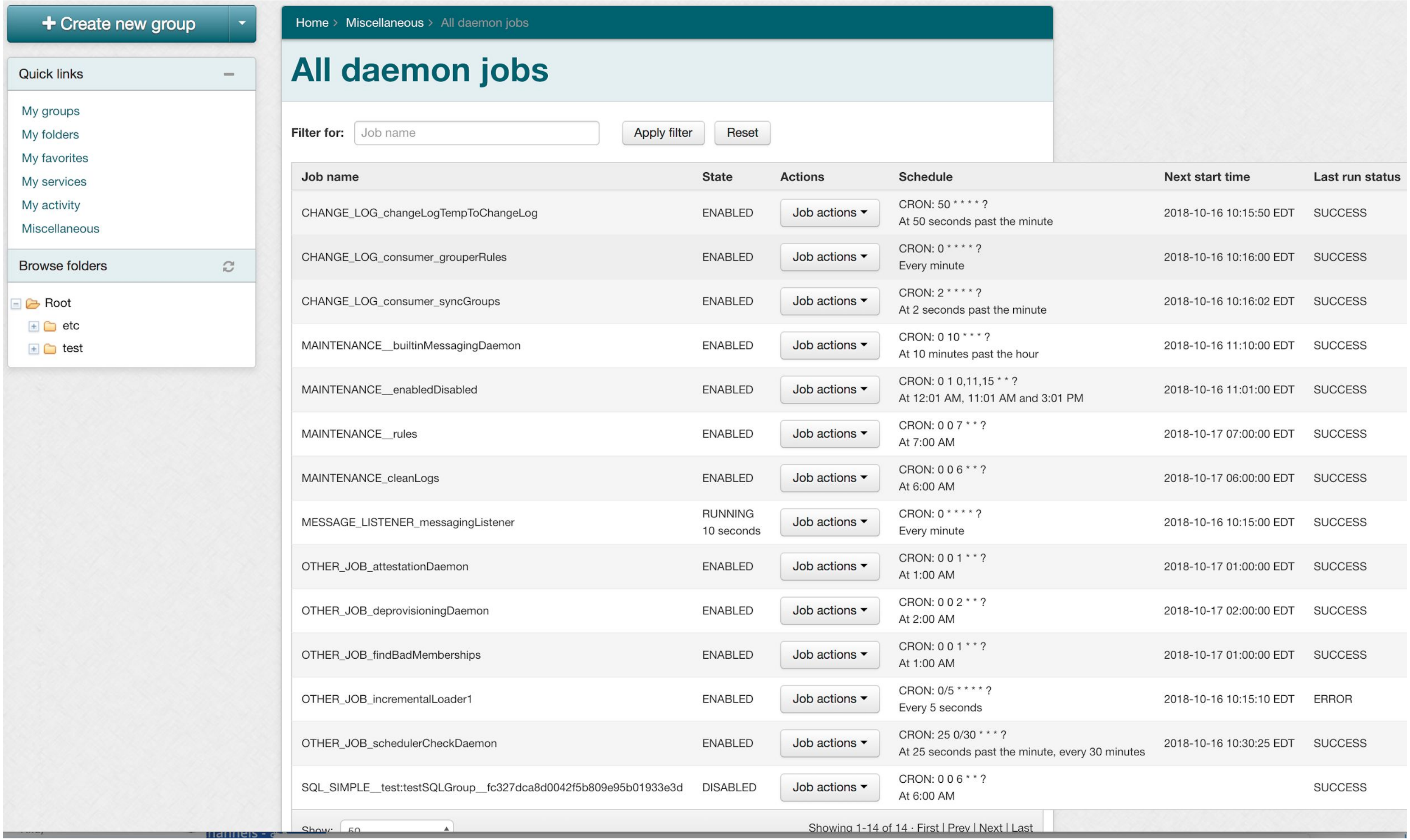
Show and manage daemon jobs in UI

- Working on a page in the Grouper UI to show all daemon jobs and information about each. This not only includes loader jobs, but also includes all other jobs that run in the Grouper Daemon.

- You can also now enable and disable jobs.

- You can also run jobs now.

- This is available as a 2.4 patch as well (currently as a test patch).



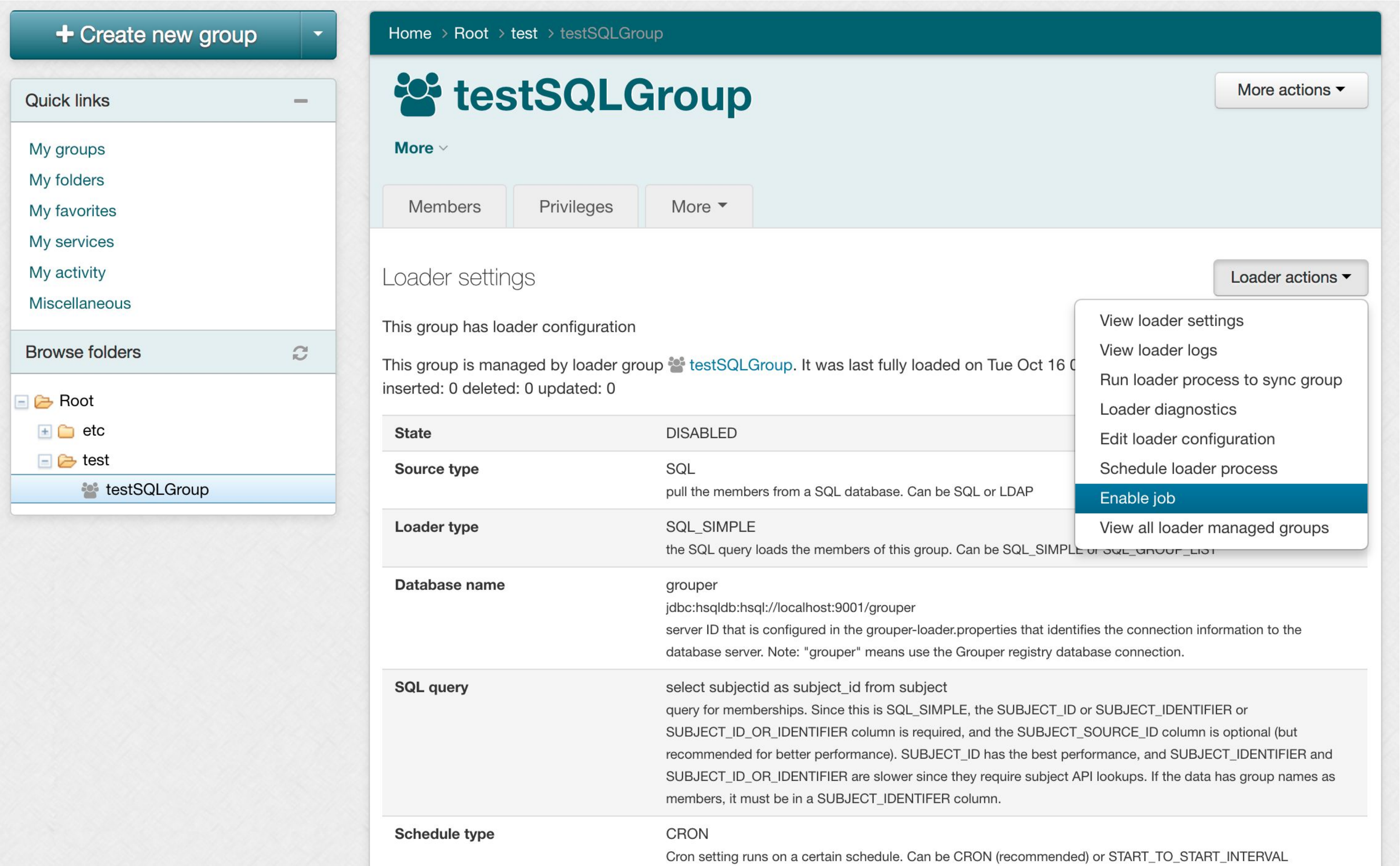
All daemon jobs

Filter for: Job name Apply filter Reset

Job name	State	Actions	Schedule	Next start time	Last run status
CHANGE_LOG_changeLogTempToChangeLog	ENABLED	Job actions ▾	CRON: 50 * * * * ? At 50 seconds past the minute	2018-10-16 10:15:50 EDT	SUCCESS
CHANGE_LOG_consumer_grouperRules	ENABLED	Job actions ▾	CRON: 0 * * * * ? Every minute	2018-10-16 10:16:00 EDT	SUCCESS
CHANGE_LOG_consumer_syncGroups	ENABLED	Job actions ▾	CRON: 2 * * * * ? At 2 seconds past the minute	2018-10-16 10:16:02 EDT	SUCCESS
MAINTENANCE__builtinMessagingDaemon	ENABLED	Job actions ▾	CRON: 0 10 * * * ? At 10 minutes past the hour	2018-10-16 11:10:00 EDT	SUCCESS
MAINTENANCE__enabledDisabled	ENABLED	Job actions ▾	CRON: 0 1 0,11,15 * * ? At 12:01 AM, 11:01 AM and 3:01 PM	2018-10-16 11:01:00 EDT	SUCCESS
MAINTENANCE__rules	ENABLED	Job actions ▾	CRON: 0 0 7 * * ? At 7:00 AM	2018-10-17 07:00:00 EDT	SUCCESS
MAINTENANCE_cleanLogs	ENABLED	Job actions ▾	CRON: 0 0 6 * * ? At 6:00 AM	2018-10-17 06:00:00 EDT	SUCCESS
MESSAGE_LISTENER_messagingListener	RUNNING 10 seconds	Job actions ▾	CRON: 0 * * * * ? Every minute	2018-10-16 10:15:00 EDT	SUCCESS
OTHER_JOB_attestationDaemon	ENABLED	Job actions ▾	CRON: 0 0 1 * * ? At 1:00 AM	2018-10-17 01:00:00 EDT	SUCCESS
OTHER_JOB_deprovisioningDaemon	ENABLED	Job actions ▾	CRON: 0 0 2 * * ? At 2:00 AM	2018-10-17 02:00:00 EDT	SUCCESS
OTHER_JOB_findBadMemberships	ENABLED	Job actions ▾	CRON: 0 0 1 * * ? At 1:00 AM	2018-10-17 01:00:00 EDT	SUCCESS
OTHER_JOB_incrementalLoader1	ENABLED	Job actions ▾	CRON: 0/5 * * * * ? Every 5 seconds	2018-10-16 10:15:10 EDT	ERROR
OTHER_JOB_schedulerCheckDaemon	ENABLED	Job actions ▾	CRON: 25 0/30 * * * ? At 25 seconds past the minute, every 30 minutes	2018-10-16 10:30:25 EDT	SUCCESS
SQL_SIMPLE__test:testSQLGroup__fc327dca8d0042f5b809e95b01933e3d	DISABLED	Job actions ▾	CRON: 0 0 6 * * ? At 6:00 AM		SUCCESS

Show: 50

Showing 1-14 of 14 · First | Prev | Next | Last



Loader settings

This group has loader configuration

This group is managed by loader group testSQLGroup. It was last fully loaded on Tue Oct 16 (
inserted: 0 deleted: 0 updated: 0

State	DISABLED
Source type	SQL pull the members from a SQL database. Can be SQL or LDAP
Loader type	SQL_SIMPLE the SQL query loads the members of this group. Can be SQL_SIMPLE or SQL_GROUP_LIST
Database name	grouper jdbc:hsqldb:hsql://localhost:9001/grouper server ID that is configured in the grouper-loader.properties that identifies the connection information to the database server. Note: "grouper" means use the Grouper registry database connection.
SQL query	select subjectid as subject_id from subject query for memberships. Since this is SQL_SIMPLE, the SUBJECT_ID or SUBJECT_IDENTIFIER or SUBJECT_ID_OR_IDENTIFIER column is required, and the SUBJECT_SOURCE_ID column is optional (but recommended for better performance). SUBJECT_ID has the best performance, and SUBJECT_IDENTIFIER and SUBJECT_ID_OR_IDENTIFIER are slower since they require subject API lookups. If the data has group names as members, it must be in a SUBJECT_IDENTIFER column.
Schedule type	CRON Cron setting runs on a certain schedule. Can be CRON (recommended) or START_TO_START_INTERVAL

Packaging update

Chris Hubing

Package Options for TIER Grouper

- **Appliances (first offering… being deprecated)**
  - VirtualBox VMs
  - AMIs (for AWS)
  - Pull necessary containers from Dockerhub/some helpful scripting
- **Docker Image Source Code (github.internet2.edu/docker/grouper)**
  - Build, and run in Docker Swarm
  - Test-Compose includes all components to compose for a functional Grouper ecosystem:

    Grouper Loader, Grouper UI, Grouper WS, Shibboleth IDP, Shibboleth SP, LDAP, MariaDB, RabbitMQ
- **Pre-built Image (dockerhub.com/r/tier/grouper)**
  - Pushed to Dockerhub
  - Includes all Grouper components in single container (UI, WS, Loader, SCIM)
  - Based on CMD flag in Dockerfile, can assume any role (chameleon)
  - Updated weekly (or so) as new patches are published

Email Lists

- tier-packaging@internet2.edu
- tier-pack-grouper@internet2.edu
- grouper-study@internet2.edu

Slack Channels (internet2.slack.com)

- #tier-packaging
- #tier-grouper
- #tier-devops-discuss

Links

- github.internet2.edu/docker/grouper
- spaces.internet2.edu/display/TPD

Provisioning update

Bert Bee-Lindgren

Grouper provisioning - Recent PSPNG work

- Reliability - Bug fixes, simplification
- Quieter: Problem avoidance and recovery instead of logging and retry
- Modularity

Provisioning - Jiras

- GRP-1345 - Updating non-membership attributes
- GRP-1707 - Recovery from out-of-band LDAP changes
- GRP-1552 - Enable full control of an LDAP attribute
- GRP-1683 and GRP-1730 - Group-deletion and -cleanup

PSPNG: Recent Work

- PSPNG patches stalled since Tech Ex
- Finished GRP-1345, -1346(Group Attributes & DN Changes), but...
- Original docker test harness broke
    - Grouper-demo container dependencies
    - Attempts to fix it failed…
        - Violating Docker Best Practices == Bad Idea
- Built new test harness
    - Docker-Compose
    - Better modularity
    - Took much longer than expected (technical and other)
- Moving forward again with Patches!

Provisioning - PSPNG Roadmap

- Performance
  - Trigger FullSync from heavy changelog load
- FullSync: More selective
  - Rate-limiting(?)
  - GUI: Config, Feedback, Control
- Documentation: Extending PSPNG
- Bugs & Gaps:
  - Multi-schema groups
  - DN-searching and escaping

Grouper provisioning - Recent PSPNG work

- Reliability - Bug fixes, simplification
- Quieter: Problem avoidance and recovery instead of logging and retry
- Modularity

2018 TECHNOLOGY exchange

ORLANDO FL OCTOBER 15-18

Legacy UI removal, Library Updates

Chad Redman

INTERNET2®

Legacy UI Removal

- Admin UI and Lite UI’s removed in Grouper 2.4.0
  - Struts library removed = security scanners are happier
  - Also gets rid of a few XSS issues in Admin UI
  - Functions should all be implemented in New UI (did we miss any?)

- Can be optionally restored if still needed
  - Download a zip file containing all the removed files and classes
  - Uncompress into war directory

Library Updates

- Updated most 3rd party libraries in API and UI to latest version possible
  - WS planned for 2.5
  - Libraries with changed API's still need upgrading (hibernate, etc.)
- Updated Maven builds to match ant builds
  - helps development of Maven projects: scim-server, pspng, …
  - Travis CI builds snapshots, can get Maven repositories
- Supporting Java 8 and Tomcat 8 (servlet version 3.1)

Internet2 Techex 2018

Grouper Birds of a Feather

Thanks!

Chris Hyzer, Penn
Shilen Patel, Duke
Bill Thompson, Lafayette
Bert Bee-Lindgren, Georgia Tech
John Gasper, Unicon
Chad Redman, UNC