



Grouper Birds of a Feather

PRESENTED BY: Chris Hyzer, Penn
Bill Thompson, Lafayette
Shilen Patel, Duke
Bert Bee-Lindgren
Chris Hubing, Internet2

Grouper BOF

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

Grouper Team (alphabetical)

- **Bert Bee-Lindgren** (Georgia Tech) - provisioning
- **Carey Matt Black** (Ohio) – general support
- **Emily Eisbruch** (Internet2) - work group support
- **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

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**, and COmanage) 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>

- Imminent release of 2.4 (immediate focus)
- 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>

- [Provisioning managed from UI](#)
- Allow configuration to be stored in database
- Membership reports
- Simple workflow approvals
- Workflow state changes in groups
- Separation of duties
- Subject source configuration in UI
- Real time loading from LDAP
- Atlassian integration to the atlassian cloud (or Rest API local)

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
- Provision lifecycle events

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

Note, most of these things are in 2.3.0 patches

- Migrate Admin and Lite UI to the New UI
- Delete old and/or inactive data
- Grouper Deployment Guide V2 progress
- Deprovisioning
- Loader metadata
- Harmonize subject source config and caching config to properties
- Require Java8 and Tomcat8 for Grouper 2.4
- PSPNG updates

Grouper progress in last 6 months (continued)

Note, most of these things are in 2.3.0 patches

- Improvements in GSH
- Migrate from VT-Ldap to Ldaptive
- Better logging in WS
- Update third party dependencies
- Performance improvements (caching, transaction management)
- Inherited privilege improvements
- Numerous fixes and minor improvements
- Provisioning to BMC remedy

Deprovisioning

- Not released yet
- 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

Delete old or inactive data

- Delete old audits
- Delete old audits with no logged in user (e.g. loader updates)
- Delete old deleted Point In Time data
- Delete old folders (e.g. course folders older than a certain date)

Harmonize subject source config and caching config

- Sources.xml is now subject.properties
- Ehcache.xml is now grouper.cache.properties
- 2.3 you can use either the old or new config
- 2.4 you need to use the properties
- Convert from XML to properties with the Grouper installer

Better logging in WS

- Each request to any Grouper web service is logged in a new log file
- Long running requests can be logged to a separated file
- See the metadata, inputs, outputs
- 2018-05-01 18:57:43,764: start: 18:57:43.638, remoteAddr: 127.0.0.1, requestUrl: http://localhost:8088/grouperWs/servicesRest/v2_3_000/permissionAssignments, method: getPermissionAssignments, clientVersion: 2.3.0, immediateOnly: false, includeAssignmentsOnAssignments: false, includeAttributeAssignments: false, includeAttributeDefNames: false, includeGroupDetail: false, includeLimits: false, includePermissionAssignDetail: false, includeSubjectDetail: false, pointInTimeFrom: 2018-05-01 18:57:43.076, pointInTimeTo: 2018-05-01 18:57:43.076, wsAttributeDefLookups: Array size: 1: [0]: name: aStem:permissionDef, userIdLoggedIn: GrouperSystem, userIdLoggedInSource: g:isa, success: T, resultCode: SUCCESS, serverVersion: 2.3.0, resultsSize: 0, elapsedMillis: 126

Performance improvements

- Reduced number of queries for some operations
- Added better caching for groups, folders, attributes, members
- Removed some transaction for huge operations
 - E.g. obliterate stem (note, units of work will still use transactions but not an overall transaction)
 - E.g. remove old records happens in batches

Inherited privilege improvements

- If you revoke an inherited privilege from folder, it will revoke from subobjects
- Applying an inherited privileges will also apply to the folder itself
- If you are a Grouper SysAdmin, you will not get redundant admin privileges on everything you create
- If you are a member of an inherited privilege group, you will not get a redundant individual ADMIN privilege

Provisioning to BMC remedy

- Penn is in process or provisioning 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
- Penn is soon to go live with Grouper-Box integration as well

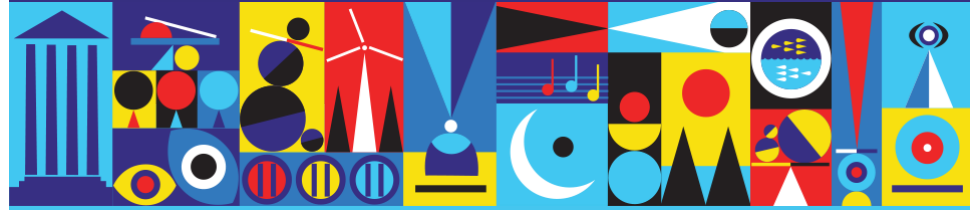
Numerous fixes and minor improvements

- See patches on [roadmap](#)
- Api - 24 patches since #82
- Ui - 11 patches since #33
- Ws - 1 patch since #12
- [85 Jira issues](#) (need to be authenticated to see them all)



Grouper Deployment Guide and Training Env

Bill Thompson

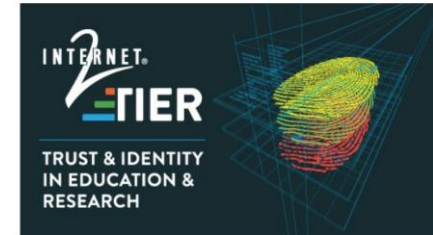


Grouper Deployment Guide (GDG)

- GDG V1 released @ Summit 2017
 - <http://doi.org/10.26869/TI.25.1>
- Grouper seminars
 - Tech Exchange 2017 and Summit 2018
- 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)
 - set of 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 389:389 -p 443:443 -p 3306:3306 -p 4443:4443 \
--name grouper-demo tier/grouper_training_full_demo:latest
```

Browse to <https://localhost/grouper>

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>

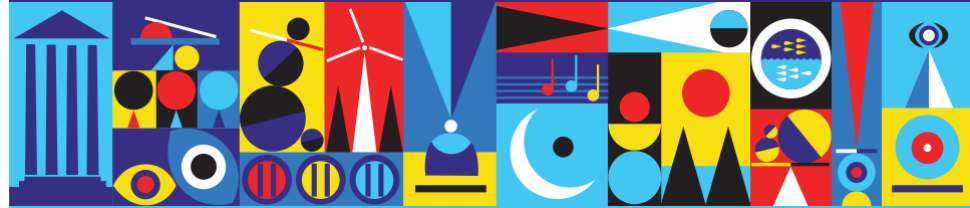
Grouper Basics (Grouper 101)

Grouper Subject API	4
Exercise - Basic Subject API	4
Exercise - Search and Selection Methods	4
Exercise - Changing Subject Identifiers	5
Exercise - Resolvable vs Active	5
Exercise - Subject Filter and Attribute Decorator (advanced config, anyone using this?)	5
Exercise - Grouper Local Entities (advanced config, anyone using this?)	5
Grouper Objects - Folders, Groups, and Attributes	6
Exercise - Create a Group	6
Exercise - Create a Folder	8
Exercise - Create an Attribute (Attribute Definition and Attribute Name)	10
Exercise - Create new Attribute Definition Name	12
Finding Grouper objects via quick links, browser, search	14
Exercise - Find objects in recent activity	14
Exercise - Find groups in Quick links -> My groups	15
Exercise - Find folders in Quick links -> My folders	15
Exercise - Find objects in Quick links -> My Favorites	15
Exercise - Find objects in Quick links -> My Services (anybody using this feature in practice?)	15
Exercise - Find objects in Browser folders [refresh]	16



UI update

Vivek Sachdeva



Migrate Lite UI to New UI

- Attribute actions can be handled (CRUD) in new UI
- Attributes at folder, group, subject, and membership level can now be assigned and viewed in new UI
- All permissions related tasks can now be done in new UI

[+ Create new group](#)

Quick links

- My groups
- My folders
- My favorites
- My services
- My activity
- Miscellaneous
- Admin UI
- Lite UI

Browse folders

- Root
 - attestation_folder
 - etc
 - root
 - test
 - test1
 - test-group
 - test-loader-group
 - permission_attribute_def
 - test-entity-attribute
 - assign
 - blog entry
 - test-entity-attribute name
 - test-attestation-folder

Home > Root > test > test1

test1

[Edit folder](#)
[More actions](#)

More

[Folder contents](#)
[Privileges](#)

Attribute Assignments

[+ Assign attribute](#)

The following table lists all attributes assigned to this folder

Assignment type	Attribute name	Enabled?	Assignment values	Attribute definition	Choose action
Direct assignment	attestation	enabled		attestationDef	Actions
Metadata on assignment	attestationHasAttestation	enabled	false	attestationValueDef	Actions
Metadata on assignment	attestationDateCertified	enabled		attestationValueDef	Actions
Direct assignment	rule	enabled		rulesTypeDef	Actions

[+ Create new group](#)

Quick links —

- [My groups](#)
- [My folders](#)
- [My favorites](#)
- [My services](#)
- [My activity](#)
- [Miscellaneous](#)
- [Admin UI](#)
- [Lite UI](#)

Browse folders ↻

- [-] [Root](#)
 - [+] [attestation_folder](#)
 - [+] [etc](#)
 - [+] [root](#)
 - [-] [test](#)
 - [+] [test1](#)
 - test-group
 - [test-loader-group](#)
 - [permission_attribute_def](#)
 - [test-entity-attribute](#)
 - [assign](#)
 - [blog entry](#)
 - [test-entity-attribute name](#)
 - [+] [test-attestation-folder](#)

Home > Root > test > test-group

test-group

[More actions](#) ▾

this is for testing

More ▾

- [Members](#)
- [Privileges](#)
- [More](#) ▾

Role permissions

[+ Assign permission](#)

Permissions assigned to roles are inherited to all entities who are members of the role

		Actions					
Role	Resource	action1	action2	action3	assign	def	Permission Definition
test-group	book				<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	permission_attribute_def
Limit	Action: assign	<u>Expression</u>					<u>Assigned to</u>
		Actions					
Role	Resource	action1	action2	action3	assign	def	Permission Definition
test-group	resource1	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>		permission_attribute_def1
Limit	Action: assign	<u>Expression</u>					<u>Assigned to</u>

[Save](#)

Loader Metadata

- Add additional attributes for groups managed by loader
 - grouperLoaderMetadataLoaded
 - grouperLoaderMetadataGroupId
 - grouperLoaderMetadataLastFullMillisSince1970
 - grouperLoaderMetadataLastIncrementalMillisSince1970
 - grouperLoaderMetadataLastSummary
- Attributes above can be viewed in UI

Home > Root > test > loader > groups > testGroup1

testGroup1

More actions ▾

testGroup1 auto-created by grouperLoader

More ▾

Members


Privileges

More ▾

Loader settings

Loader actions ▾

This group does not have loader configuration

This group is managed by loader group  testSqlGroupList2. It was last fully loaded on Wed Feb 14 11:18:50 UTC 2018. Summary is:
total: 167 inserted: 167 deleted: 0 updated: 0



3rd party library updates

Chad Redman



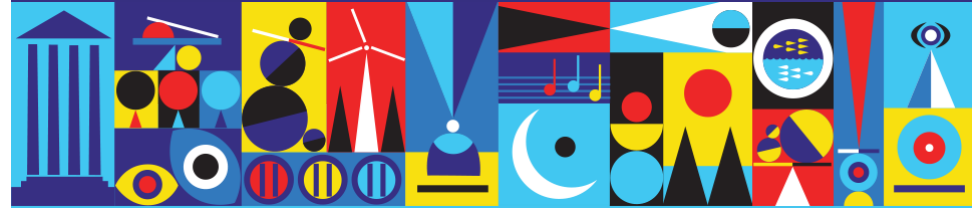
Update 3rd party dependencies

- Updated 3rd party libraries in API and UI to latest version possible
 - Removed Admin UI, Struts dependency
 - WS planned for 2.5
 - Upgrading libraries and removing struts lowers vulnerability scan hits
- Updated Maven builds to match ant builds
 - scim-ws and scim server are Maven builds, so this will help development of these projects
- Restored Travis CI functions
 - Travis CI builds now publish snapshot jars of the API, UI, and WS to the Sonatype repository, any Maven or gradle project can use these
- Supporting Java 8 and Tomcat 8 (servlet version 3.1)



Vt-Idap to Ldaptive And GSH update

Shilen Patel



vt-ldap to Idaptive migration

- Many components of Grouper may optionally access LDAP

Component	v2.3	v2.4	How it impacts you
Subject API (if your subjects are sourced from LDAP)	vt-ldap via sources.xml	Idaptive via grouper-loader.properties	Must move connection info to grouper-loader.properties
Grouper Loader (if you load groups into Grouper from LDAP)	vt-ldap via grouper-loader.proeprties	Idaptive via grouper-loader.properties	Changes likely not needed.
Grouper Web Services (if authentication there is via LDAP BINDs)	vt-ldap via grouper-loader.proeprties	Idaptive via grouper-loader.properties	Changes likely not needed.
PSPNG (if you provision groups to LDAP)	Idaptive	Idaptive	No impact

vt-ldap to Idaptive migration (continued)

- Generic LDAP interface is used now
- Also Subject API moved into Grouper
- <https://spaces.internet2.edu/display/Grouper/vt-ldap+to+Idaptive+migration+for+LDAP+access>

Other

- GSH improvements
 - Transitioned from BeanShell to Groovy before Tech Ex
 - A few improvements made since then:
 - Upgraded Groovy
 - Support for typed variables
 - Fixed issues with Windows
 - Fixed issue with “runarg” option
- Alternate name web service changes
 - Alternate name’s can be assigned to a group to allow them to be found when a group is renamed or moved.
 - Improvements made with web services include:
 - Preventing alternate names from being assigned during a rename.
 - Adding, updating, deleting alternate names

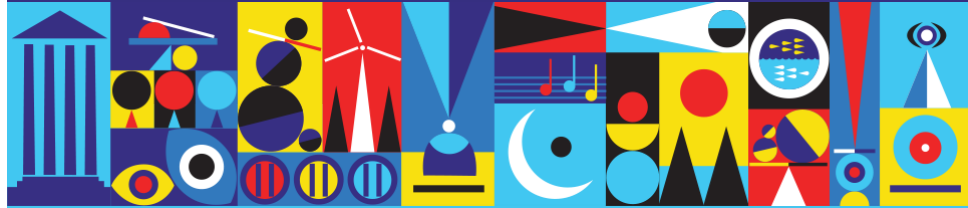
Next steps

- Grouper daemon with multiple clusters
- Real-time loader updates for better LDAP integration



Packaging update

Chris Hubing



Package Options for TIER Grouper

- **Appliances (first offering)**
 - VirtualBox VMs
 - AMIs (for AWS)
 - Pull necessary containers from Dockerhub/some helpful scripting
- **Source Code ([github.internet2.edu/docker/grouper](https://github.com/internet2.edu/docker/grouper))**
 - Build, and run in Docker Swarm
 - Includes all components to compose for a functional Grouper ecosystem:
Grouper Loader, Grouper UI, Grouper WS, Shibboleth IDP, Shibboleth SP, LDAP, MariaDB, RabbitMQ
- **Standalone Container (dockerhub.com/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)

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](https://github.com/internet2/docker/grouper)
- spaces.internet2.edu/display/TPD

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
 - Grouper UI - Config, Control & Status

Provisioning - PSPNG Current

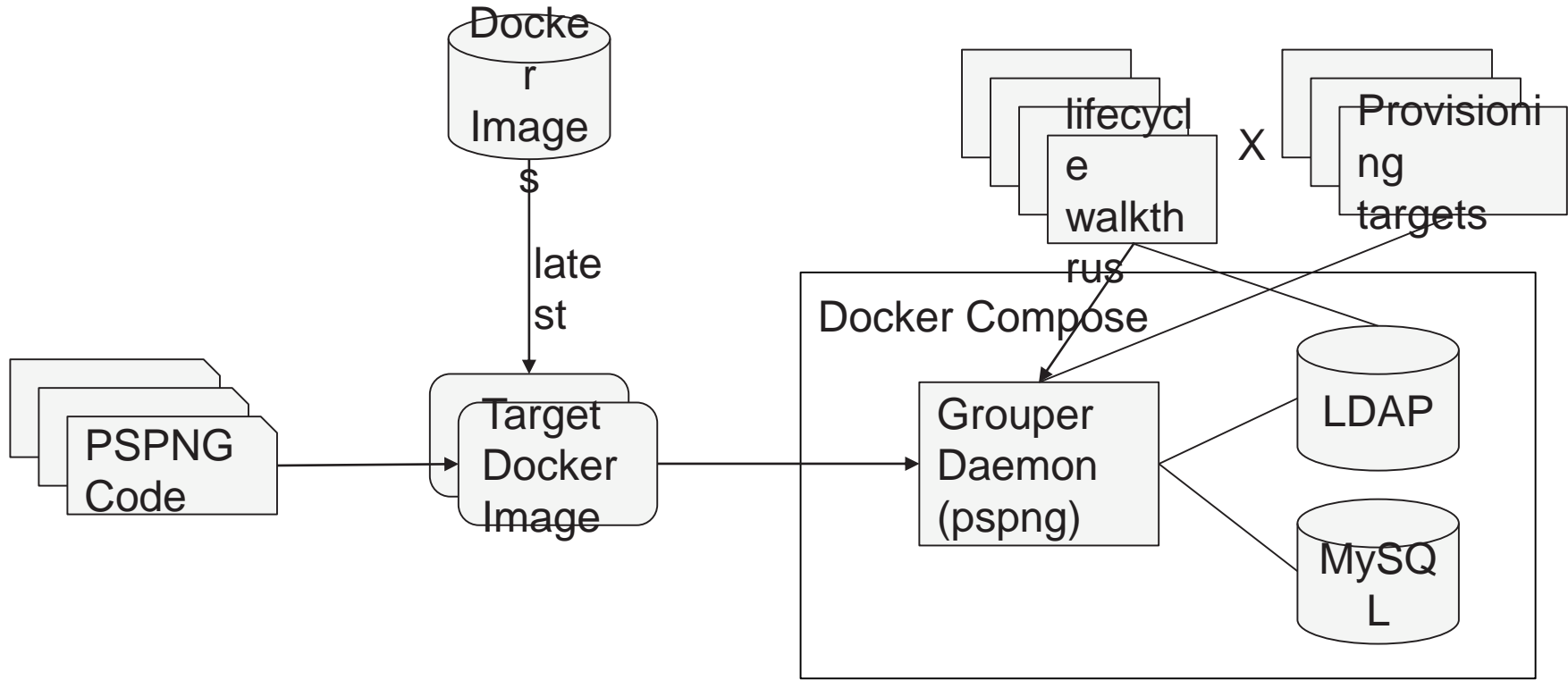
Current Functionality: (v2.3)

- 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 \[Coming Soon\]](#)

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!

PSPNG: Test Harness v2



Provisioning - PSPNG Roadmap

v2.4 patches

- Bugs & Gaps
 - Group-attribute updates
 - Total control of provisioned attribute (prefix=*)
 - Multi-schema groups (multiple membership attributes)
 - Cleaning up empty OUs
 - DN-searching and escaping
- 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
- Documentation: Extending PSPNG



Thank you for attending

GROUPER BoF

PRESENTED BY: Chris Hyzer, Penn
Bill Thompson, Lafayette
Shilen Patel, Duke
Bert Bee-Lindgren