

InCommon®



Grouper<sub>T</sub>

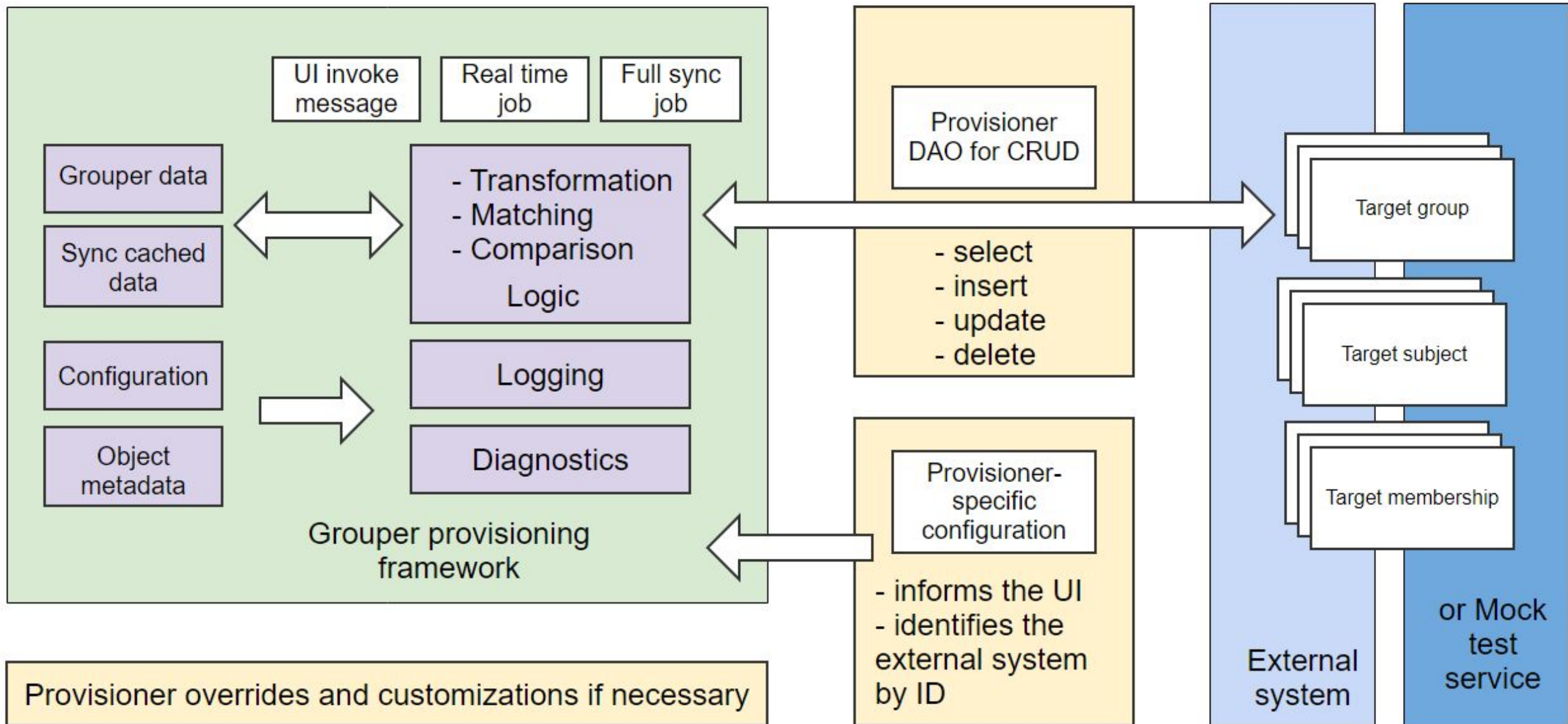
Base Camp 2022

# Grouper Provisioning

# Agenda

- 
1. Provisioning intro
  2. Glossary
  3. LDAP example
    - a. Start with
    - b. Configuration
    - c. Marking provisionable
    - d. Daemons

# Provisioning intro



# Targets

- 
1. LDAP
  2. SQL
  3. Azure
  4. Duo
  5. Duo roles
  6. Google
  7. Github
  8. SCIM
  9. Messaging

# Glossary

---

- Provisioning - Taking grouper data and sending to target
- Provisioning framework - The Grouper system that manages provisioning UI, logic, compare, logging, etc
- Target - An external service that grouper can sync with LDAP, SQL, Box, etc
- Group - Collection of subjects/entities that can be managed in target.  
Could be a group or role etc
- Entity - Subject / entity / user in the target that can be managed
- Membership - Relationship between a target group and entity

# Glossary (continued)

---

- Full sync - Nightly (configurable) job that takes everything from Grouper and everything from Target and syncs them up by changing the target
- Incremental sync - Job that runs every minute (configurable) and takes change log events and messages and manipulates the target
- Group sync - Sync only one group or a collection of groups from grouper to the target using recalce.g. if a certain configurable threshold number of memberships changed at once, or if a user clicks a button on UI to sync a group or a folder

# Glossary (continued)

---

- Sync tables - Grouper SQL tables that store information for provisioning:
  - Groups, users, memberships, jobs
  - State in the target (is data provisioned, when, did Grouper put it there)
  - Cache target data (if there is a "link" then keep the uuid or dn or whatever on the grouper side)
  - Track when data starts or ends being provisionable

# Glossary (continued)

---

- Synchronous vs asynchronous sync
  - A full sync or group sync could be synchronous where it is the only provisioning action happening across all daemons and will update the target and update the grouper sync tables.
  - A full sync or group sync could be asynchronous where it looks at Grouper and the target and sees what is out of sync and sends messages to the Incremental sync to recalc certain objects (groups / entities / memberships / full sync)



# Glossary (continued)

---

- Recalc stateless action - An action on a membership, group, or entity that will retrieve data from Grouper and the target and compare and adjust the target to make it consistent with Grouper. Recalcs happen:
  - if a user clicks a button to recalc
  - if an error occurs and it gets requeued
  - if too many memberships appear on queue, just recalc the group
  - inconsistent events get converted to recalc (e.g. if its an add member but the sync object disagrees)
  - etc

# Glossary (continued)

---

- Non-recalc stateful action - An action that takes a Grouper change log event, and sends a command to the target.
- Provisioning attributes and metadata - Information that is internally stored in Grouper using the attribute framework that is used in provisioning. If provisionable, ID/name to use in target, flags used in target

# Glossary (continued)

---

- Provisionable - If grouper data should be in the target
  - If a group is flagged as provisionable directly or from ancestor folder, if entities are in the right subject source or group or exist in target, etc
- In target - If the grouper data is in the target Generally this means Grouper provisioned the data but it could mean that the data already existed in the target
- Target DAO - Data Access Object implementation of a Java contract that allows the provisioning framework to select, insert, update, delete data from target
  - Run SQL queries in the SQL DAO. Run web service calls in Azure DAO

# Glossary (continued)

---

- Target DAO capabilities - List of DAO actions supported by this target DAO implementation
  - Maybe a target DAO for box cannot bulk delete groups and needs to delete them individually
- Provisioner configuration - Configuration the Grouper admin does when setting up a provisioner e.g. specify the OU to look for groups in LDAP
- Provisioner behaviors - Intersection of target DAO capabilities and provisioner configuration so the framework knows what to do e.g. if a provisioner is not supposed to or cannot delete entities in the target

# Glossary (continued)

---

- Membership sync type - Memberships in target can be represented as objects, as group attributes, as entity attributes e.g. in box memberships are objects, but in LDAP memberships are group attributes or entity attributes
- Group target link - Maybe some data (e.g. DN or UUID) needs to be retrieved from a group object in the target. This data is "linked" to the membership generally by caching in a sync row in the database
- Entity target link - Maybe some data (e.g. DN or UUID) needs to be retrieved from an entity object in the target. This data is "linked" to the membership generally by caching in a sync row in the database
- Subject link - The target might refer to subjects as something other than the subject ID. So the subject needs to be resolved and that attribute needs to be used in provisioning

# Glossary (continued)

---

- Sync object cache - IDs (data) in the group target link, entity target link, or subject link, can be cached in the grouper sync objects in the database to help with deprovisioning when objects are deleted or for performance in non-recalc actions cache the entity DN in the database
- Translation - Grouper data is translated to target format in order to be able to retrieve data from target or to compare data e.g. put the group name in the CN of the target group object
- Attribute manipulation - Data fields and attributes from grouper or the target originate in a certain format. These are manipulated based on provisioner configuration to change the type or assign a default value e.g. change LDAP gidNumber from a string to an integer

# Glossary (continued)

---

- Matching attribute - A field or attribute (or composite key) in the group/entity/membership objects in the target format that can be used to match grouper objects with target objects e.g. the gidNumber for posix groups
- Search attribute(s) - An attribute used to search for an object in the target e.g. gidNumber for posix groups, or the DN
- Comparison - Target data and grouper data translated in target format are compared to see what actions need to occur in target to sync state

# Demo

- 
- Existing LDAP external system with test
  - Browse LDAP
  - Configure provisioner with startWith scaffolding
  - groupOfNames
  - RDN: cn
  - idIndex: businessCategory
  - other attribute: description



# Demo (continued) - test external system

Success: grouper was able to connect to the external system

+ Create new group

Quick links

My groups

My folders

My favorites

My services

My activity

Miscellaneous

Browse folders

Root

Home > Miscellaneous > External systems

## Grouper external systems

Actions

Config id	External system type	Enabled	Actions
grouperBuiltinMessaging	GrouperInternalMessagingExternalSystem	Enabled	Actions
personLdap	Ldap	Enabled	Actions
smtp	SMTP	Enabled	Actions

# Demo (continued) - startWith / scaffolding

## Provisioning

Actions ▾

Configuration id	<input type="text" value="localGroupOfNames"/> *	The Config id is an alphanumeric key for the provisioner config. It is also used in the configuration keys. Example: myLdapProvisioner
Provisioner type	<input type="text" value="Ldap"/> *	Type of provisioner that will be connected to, for example LDAP or Duo
Start with	<input type="text" value="LDAP 'start with'"/> *	Start with
External system config id	<input type="checkbox"/> EL? <input type="text" value="personLdap"/> *	Pick the LDAP to connect to for this provisioner. If the LDAP is not in the list, first go and configure that in the Grouper external system UI screen.
Start with id	<input type="text" value="ldapMemberships"/>	Start with id
Ldap pattern	<input type="checkbox"/> EL? <input type="text" value="groupOfNames"/> *	Ldap pattern
Membership structure	<input type="checkbox"/> EL? <input type="text" value="groupAttributes"/> *	Membership structure
Membership value dn	<input type="checkbox"/> EL? <input checked="" type="radio"/> True <input type="radio"/> False *	Membership value dn
Group DN type	<input type="checkbox"/> EL? <input type="text" value="bushy"/> *	Group DN type
User attributes type	<input type="checkbox"/> EL? <input type="text" value="core"/> *	User attributes type
Group search base DN	<input type="checkbox"/> EL? <input type="text" value="ou=Groups,dc=example,dc=edu"/> *	Group search base DN
RDN groups attribute	<input type="checkbox"/> EL? <input type="text" value="cn "/> *	RDN groups attribute

# Demo (continued) - DN override

—

Other group ldap attributes

<b>Allow group dn override</b>	<input type="checkbox"/> EL?	<input type="radio"/> Default value (False) <input checked="" type="radio"/> True <input type="radio"/> False
		Allow group dn override. Default value is 'false'.
<b>Enable group base DN</b>	<input type="checkbox"/> EL?	<input type="text"/>

# Demo (continued) - enable full daemon / run

Home > Miscellaneous > All daemon jobs

## All daemon jobs

Daemon actions ▾

Filter for:

Common filters ▾

Show extended results?

Show only errors?

Job name	State	Overall status	Last run status	Actions	Schedule
<a href="#">CHANGE_LOG_consumer_provisioner_incremental_sdfasdf</a>	DISABLED	DISABLED		<input type="button" value="Job actions ▾"/>	CRON: 0 * * * * ? Every minute
<a href="#">OTHER_JOB_provisioner_full_sdfasdf</a>	DISABLED	SUCCESS	SUCCESS	<input type="button" value="Job actions ▾"/>	CRON: 0 30 3 * * ? At 3:30 AM


Show:  ▾

Showing 2 of 2 jobs

- Edit daemon
- View daemon logs
- Delete
- Delete daemon
- Enable job**

# Demo (continued) - mark provisionable / run

Home > Root > apps > wiki > wikiUsers > provisioning

 **wikiUsers**

[+ Add members](#)

[Group actions](#) ▾

[Show details](#) ▾

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

### Group provisioning settings

[Provisioning actions](#) ▾

**Target name**  ▾ \*

Target where you want to provision

**Type**  ▾

If this group/folder has provisioning configuration directly assigned

**Provision**  ▾

If this object should be provisioned or not

**Group DN override**

If this group should point to an LDAP group which is not in the normal location, enter the DN where this group should sync to

[Save](#) [Cancel](#)

# Demo (continued) - see logs / error

---

```
at edu.internet2.middleware.grouper.GrouperSession.internal_callbackRootGrouperSession(GrouperSession.java:1036)
at edu.internet2.middleware.grouper.app.loader.OtherJobBase.execute(OtherJobBase.java:392)
at edu.internet2.middleware.grouper.app.loader.OtherJobBase.execute(OtherJobBase.java:376)
at edu.internet2.middleware.grouper.app.loader.GrouperDaemonJob.execute(GrouperDaemonJob.java:57)
at org.quartz.core.JobRunShell.run(JobRunShell.java:202)
at org.quartz.simpl.SimpleThreadPool$WorkerThread.run(SimpleThreadPool.java:573)
by: javax.naming.directory.SchemaViolationException: [LDAP: error code 65 - object class 'groupOfNames' requires attribute 'member'];
at com.sun.jndi.ldap.LdapCtx.mapErrorCode(LdapCtx.java:3185)
at com.sun.jndi.ldap.LdapCtx.processReturnCode(LdapCtx.java:3100)
at com.sun.jndi.ldap.LdapCtx.processReturnCode(LdapCtx.java:2891)
at com.sun.jndi.ldap.LdapCtx.c_createSubcontext(LdapCtx.java:812)
at com.sun.jndi.toolkit.ctx.ComponentDirContext.p_createSubcontext(ComponentDirContext.java:341)
at com.sun.jndi.toolkit.ctx.PartialCompositeDirContext.createSubcontext(PartialCompositeDirContext.java:268)
at org.ldaptive.provider.jndi.JndiConnection.add(JndiConnection.java:315)
... 30 more
```

# Demo (continued) - configure default / run




(objectClass=top)

Allow DN override	<input type="checkbox"/> EL?	<input type="radio"/> Default value (False) <input checked="" type="radio"/> True <input type="radio"/> False
		When marking a group as provisionable, allow the DN to be set to a different value than the default (to point a Grouper group to an arbitrary LDAP group as a one-off). Default value is 'false'.
Group DN type	<input type="checkbox"/> EL?	<input type="text" value="bushy"/> *

# Demo (continued) - change DN / run

Home > Root > apps > wiki > wikiUsers > provisioning

 **wikiUsers**

[+ Add members](#)

[Group actions ▾](#)

[Show details ▾](#)

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

### Group provisioning settings [Provisioning actions ▾](#)

<b>Target name</b>	<input type="text" value="sdfasdf"/> ▾ *
	<small>Target where you want to provision</small>
<b>Type</b>	<input type="text" value="Yes, has direct provisioning configuration"/> ▾
	<small>If this group/folder has provisioning configuration directly assigned</small>
<b>Provision</b>	<input type="text" value="Yes, provision the object"/> ▾
	<small>If this object should be provisioned or not</small>
<b>Group DN override</b>	<input type="text" value="cn=wikiUsersNew,ou=wiki,ou=apps,ou=Groups,dc=example,dc=e"/>
	<small>If this group should point to an LDAP group which is not in the normal location, enter the DN where this group should sync to</small>

[Save](#) [Cancel](#)



# Demo (continued) - enable incremental / change

Home > Miscellaneous > All daemon jobs

## All daemon jobs

Daemon actions ▾

Filter for:

Common filters ▾

Show extended results?

Show only errors?

Job name	State	Overall status	Last run status	Actions	Schedule
<a href="#">CHANGE_LOG_consumer_provisioner_incremental_sdfasdf</a>	DISABLED	DISABLED		Job actions ▾	CRON: 0 * * * * ? Every minute
<a href="#">OTHER_JOB_provisioner_full_sdfasdf</a>	DISABLED	SUCCESS	SUCCESS		CRON: 0 30 3 * * ? At 3:30 AM

Show:  ▾

Showing 2 of 2 jobs

Last

- Edit daemon
- View daemon logs
- Delete
- Delete daemon
- Enable job

Done!

---

