

Grouper integration demo

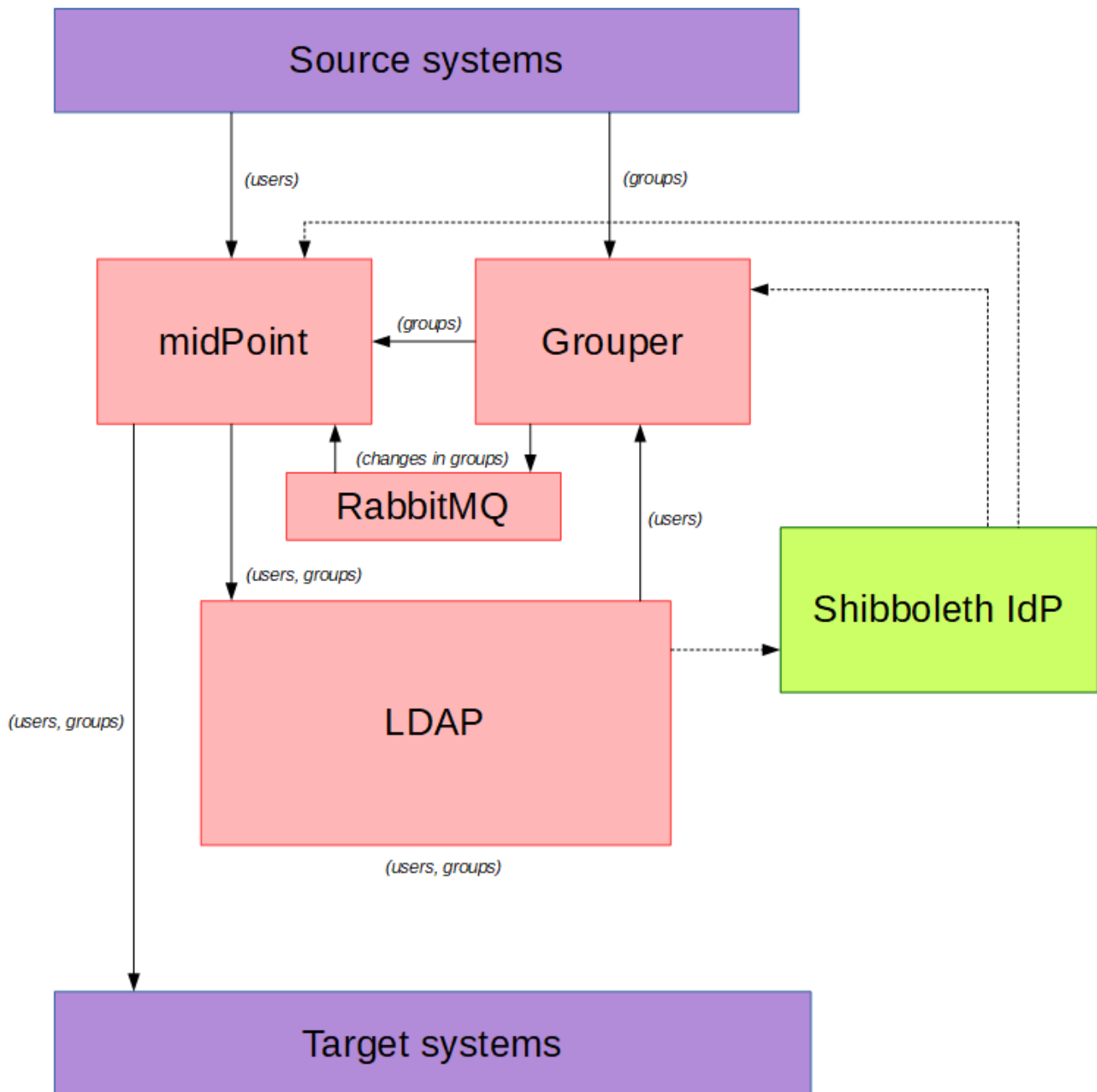


This demo is updated from time to time. If you encounter unexpected behavior, please let us know e.g. on [#incommon-midpoint](#) Internet2 Slack channel.

- [Installation](#)
 - [Checking the prerequisites](#)
 - [Starting the containers](#)
- [After installation](#)
 - [TL;DR](#)
 - [Checking the midPoint state \(optional\)](#)
 - [Importing from SIS persons resource](#)
 - [Checking the import task \(optional\)](#)
 - [Import of groups from SIS to Grouper](#)
 - [Checking groups in Grouper \(optional\)](#)
 - [Creating additional groups in Grouper](#)
 - [Importing of groups from Grouper to midPoint](#)
 - [Checking the groups in midPoint \(optional\)](#)
 - [Starting near real-time synchronization from Grouper to midPoint](#)
 - [Making some changes in Grouper \(optional\)](#)
 - [Switching midPoint authentication to Shibboleth \(optional\)](#)
 - [Additional Details](#)
- [Conclusion](#)

This is a demonstration of using midPoint in more realistic deployment, having various source and target systems along with other identity management components like LDAP, Grouper, and Shibboleth IdP.

The overall architecture looks like this:



If you would like to read more about this demo, please see [the detailed description](#).

Installation

Checking the prerequisites

In addition to the [general prerequisites](#) please check that the following ports are available on the local host:

Kind	Port(s)	Component
web	443	Shibboleth IdP
	4443	Grouper UI

	8443	midPoint UI and REST
	9443	Grouper REST
LDAP	389	LDAP directory
database	3306	Grouper database (MariaDB)
	13306	<i>sources</i> database (MariaDB)
	33306	midPoint repository (MariaDB)
other	15672	RabbitMQ management

Starting the containers

```
$ cd demo/grouper
$ docker-compose up
```

This will take a while. You can ignore the following errors:

Finally, you will see notices like these:

```
Creating grouper_directory_1 ... done
Creating grouper_idp_1 ...
Creating grouper_midpoint_data_1 ... done
Creating grouper_midpoint_server_1 ...
Creating grouper_grouper_data_1 ... done
Creating grouper_grouper_daemon_1 ...
Creating grouper_grouper_ui_1 ...
Creating grouper_grouper_ui_1
Creating grouper_sources_1 ... done
Attaching to grouper_directory_1, grouper_midpoint_data_1, grouper_midpoint_server_1, grouper_grouper_data_1,
grouper_grouper_daemon_1, grouper_targets_1, grouper_grouper_ui_1, grouper_idp_1, grouper_mq_1,
grouper_sources_1
```

followed by startup messages from individual Docker containers.

Note that errors like

```
com.evolveum.midpoint.util.exception.ObjectAlreadyExistsException: org.identityconnectors.framework.common.
exceptions.AlreadyExistsException(Error adding LDAP entry uid=banderson,ou=People,dc=internet2,dc=edu:
entryAlreadyExists: (68))
```

during first start are OK. They are related to the fact that midPoint tries to create LDAP entry `uid=banderson,ou=People,dc=internet2,dc=edu` that already exists in the directory. (As midPoint is designed to deal with situations like this, these errors are automatically resolved.)

Final messages should look like these:

```

midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 15:38:10,379 [] [main] INFO (org.springframework.
boot.actuate.endpoint.web.EndpointLinksResolver): Exposing 6 endpoint(s) beneath base path '/actuator'
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 15:38:10,526 [] [main] INFO (org.apache.coyote.
http11.Http11NioProtocol): Starting ProtocolHandler ["http-nio-8080"]
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 15:38:10,545 [] [main] INFO (org.apache.coyote.ajp.
AjpNioProtocol): Starting ProtocolHandler ["ajp-nio-9090"]
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 15:38:10,574 [] [main] INFO (org.springframework.
boot.web.embedded.tomcat.TomcatWebServer): Tomcat started on port(s): 8080 (http) 9090 (http) with context path
'/midpoint'
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 15:38:10,580 [] [main] INFO (com.evolveum.midpoint.
web.boot.MidPointSpringApplication): Started MidPointSpringApplication in 141.075 seconds (JVM running for
151.543)
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 15:38:10,705 [] [ajp-nio-9090-exec-1] INFO (org.
apache.catalina.core.ContainerBase.[Tomcat].[localhost].[/midpoint]): Initializing Spring DispatcherServlet
'dispatcherServlet'
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 15:38:10,705 [] [ajp-nio-9090-exec-1] INFO (org.
springframework.web.servlet.DispatcherServlet): Initializing Servlet 'dispatcherServlet'
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 15:38:10,728 [] [ajp-nio-9090-exec-1] INFO (org.
springframework.web.servlet.DispatcherServlet): Completed initialization in 23 ms

```

After installation

At this moment, main midPoint objects are in place but there are no users yet - in midPoint, LDAP, nor Grouper. So the first thing to do is to import them from the source system.

TL;DR

If you're in a hurry, just apply these commands. If not, you can skip this and continue following the same steps - but with more detailed explanation and optional actions - below.

```

$ ./upload-import-sis-persons.sh           # wait until uploaded task is complete
$ ./create-ref-loaders.sh                 # wait two minutes after this command
$ ./add-ref-groups.sh
$ ./upload-reconcile-grouper-groups.sh     # wait until uploaded task is complete
$ ./upload-recompute-users.sh             # wait until uploaded task is complete

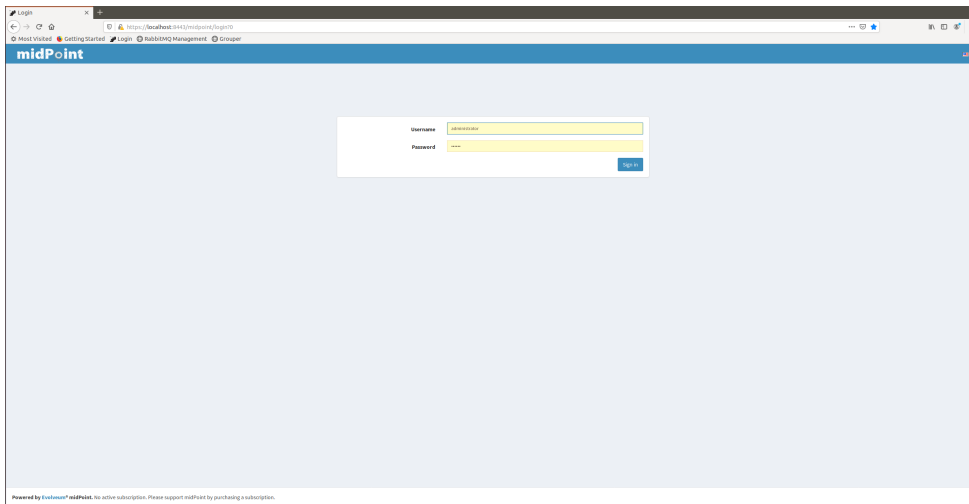
(optional steps to see how asynchronous updates work)
$ ./purge-queue.sh
$ ./upload-async-update-task.sh
$ ./update-bgasper-in-grouper.sh

```

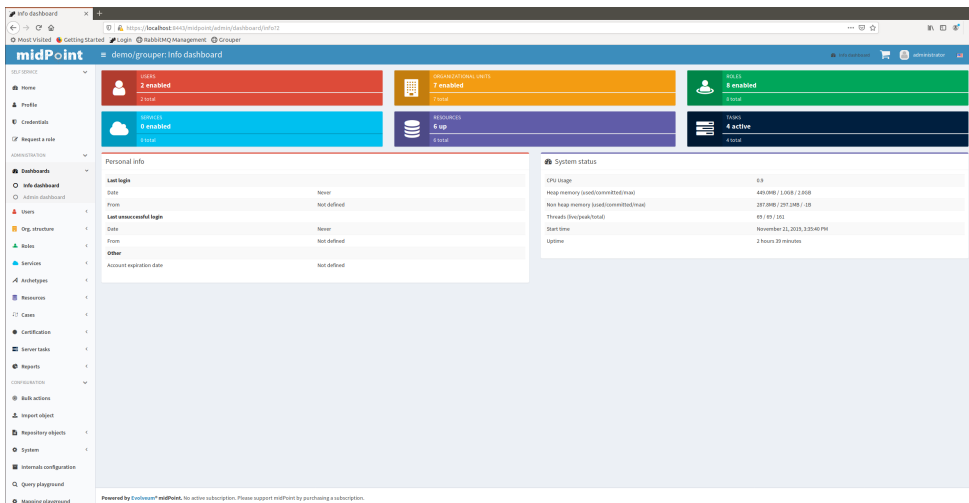
The detailed explanation starts here.

Checking the midPoint state (optional)

Now you can check if midPoint is up and running by logging into it. Please use URL of <https://localhost:8443/midpoint>, with user administrator, and password 5ecr3t.



After successful login:



Importing from SIS persons resource

There is a task that imports all user accounts from SIS Persons resource. For each account, appropriate midPoint user and LDAP account is created. This demo contains 100 such sample users.

So, import the task object in `midpoint-objects-manual/tasks/task-import-sis-persons.xml` and wait for its successful completion. You can import either using GUI or by invoking the following command:

```
$ ./upload-import-sis-persons.sh
Uploading midpoint-objects-manual/tasks/task-import-sis-persons.xml (tasks, 22c2a3d0-0961-4255-9eec-c550a79aeaaa)
```

Checking the import task (optional)

The task will look like this:

midPoint demo/group: Edit Import task 'Import from SIS persons'

SELF SERVICE: Home, Profile, Credentials, Request a role, Consents

ADMINISTRATION: Dashboards, Users, Org. structure, Roles, Services, Archetypes, Resources, Cases, Certification, Server tasks

Import from SIS persons
Progress: 100 (closed)
Last object processed: wvales
4/29/20, 5:32:21 PM - 4/29/20, 5:32:43 PM (00:00:21.405)

Run now (no refreshing)

Basic | Schedule | Operation statistics | Environmental performance | Internal performance | Result | Errors

Progress

Objects successfully processed: 100 (average time 188 ms, total processing time 18 seconds)
Last object successfully processed: wvales (ACCOUNT - default - AccountObjectClass) April 29, 2020, 5:32:43 PM (in 130 ms)

Objects failed to be processed: 0
Last object failed to be processed:
Last error when processing object:
Current object being processed:

Total objects processed: 100 (wall clock average: 214 ms, throughput: 280 per minute)

States of processed objects

Situation	Before (count)	After (count)
Unmatched	99	0
Unlinked	1	0
Linked	0	100
Deleted	0	0

Then you can check that users were successfully created:

midPoint demo/group: Users List

SELF SERVICE: Home, Profile, Credentials, Request a role, Consents

ADMINISTRATION: Dashboards, Users, Org. structure, Roles, Services, Archetypes, Resources, Cases, Certification, Server tasks, Reports, Bulk actions, Import objects, Repository objects, System, Internal configuration, Query playground, Mapping playground

Users List

Name	Given name	Family name	Full name	Email	Accounts
administrator	midpoint	Administrator	midPoint Administrator	administrator@example.edu	0
agaper	Ann	Gasper	Ann Gasper	agaper@example.edu	2
ahenderson	Ann	Henderson	Ann Henderson	ahenderson@example.edu	2
amorrison	Ann	Morrison	Ann Morrison	amorrison@example.edu	2
amorrison00	Ann	Morrison	Ann Morrison	amorrison00@example.edu	2
avales	Ann	Vales	Ann Vales	avales@example.edu	2
awhite	Ann	White	Ann White	awhite@example.edu	2
bhenderson	Bobb	Anderson	Bobb Anderson	bhenderson@example.edu	2
bholter	Betty	Butler	Betty Butler	bholter@example.edu	2
bdoe	Blake	Doe	Blake Doe	bdoe@example.edu	2
bgasper	Bill	Gasper	Bill Gasper	bgasper@example.edu	2
bgasper00	Bill	Gasper	Bill Gasper	bgasper00@example.edu	2
bgardy	Betty	Grady	Betty Grady	bgardy@example.edu	2
blee	Bill	Lee	Bill Lee	blee@example.edu	2
bpeterson	Betty	Peterson	Betty Peterson	bpeterson@example.edu	2
csmorrison	Colin	Morrison	Colin Morrison	csmorrison@example.edu	2
danderson	Dennis	Anderson	Dennis Anderson	danderson@example.edu	2
danderson00	David	Anderson	David Anderson	danderson00@example.edu	2
dbutler	Dennis	Butler	Dennis Butler	dbutler@example.edu	2
dmorris	David	Davis	David Davis	dmorris@example.edu	2

1 to 20 of 101

Powered by **Enthought** midPoint. No active subscription. Please support midPoint by purchasing a subscription.

After clicking on amorrison user check the basic properties:

midPoint demo/group: Edit SIS Person 'amorrison'

SELF SERVICE: Home, Profile, Credentials, Request a role, Consents

ADMINISTRATION: Dashboards, Users, Org. structure, Roles, Services, Archetypes, Resources, Cases, Certification, Server tasks, Reports, Bulk actions, Import objects, Repository objects, System, Internal configuration, Query playground

Ann Morrison (amorrison)

Basic | Properties | Assignments | History | Cases | Triggers | Permissions | Delegations | Delegated to me

Properties

Name	amorrison
Full name	Ann Morrison
Given name	Ann
Family name	Morrison
Email	amorrison@example.edu

Activation

Password

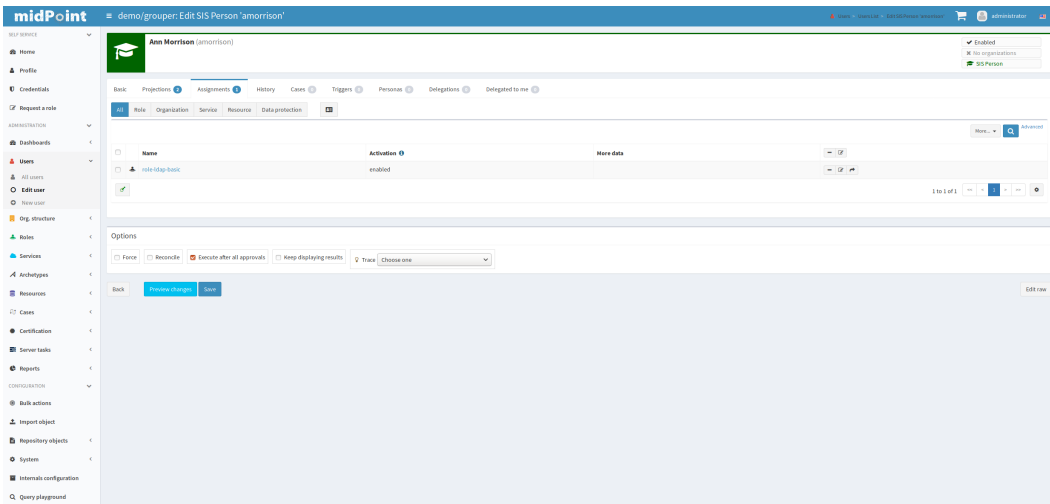
Options

☐ Force ☐ Reconcile ☒ Execute after all approvals ☐ Keep displaying results ☐ Choose one

Back **Save** **Edit user**

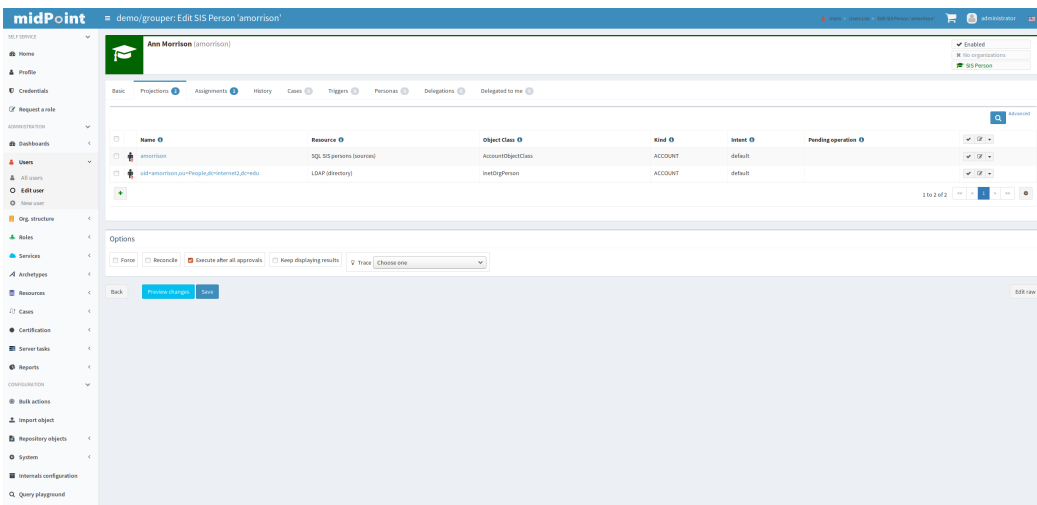
These data came from SIS_PERSONS table.

There is only a single assignment at this time - to role_ldap_basic. It is created automatically for all imported users.

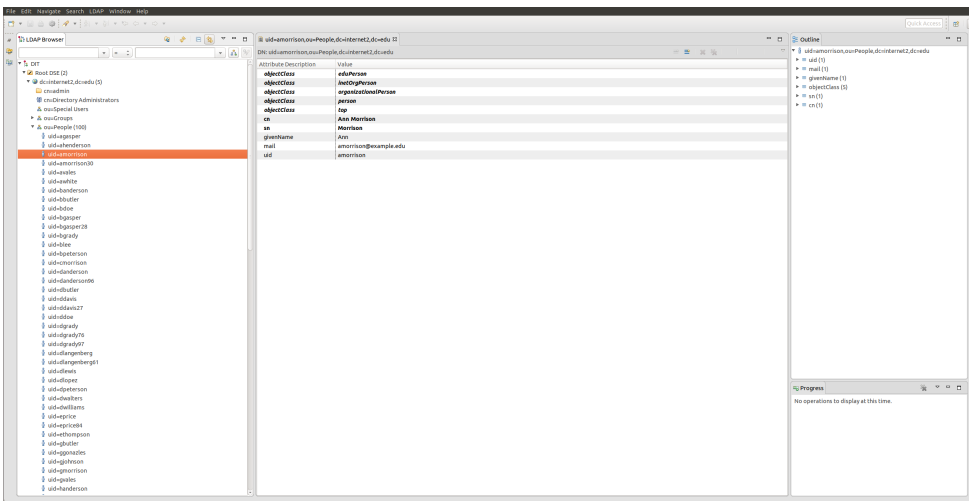


Other assignments (created according to Grouper group membership) will be created later, after groups are imported from Grouper.

You can also check there are 2 projections (accounts): SIS Persons and LDAP:



And you can verify the existence of LDAP account directly:



Note that there are only basic personal attributes now. No group membership yet.

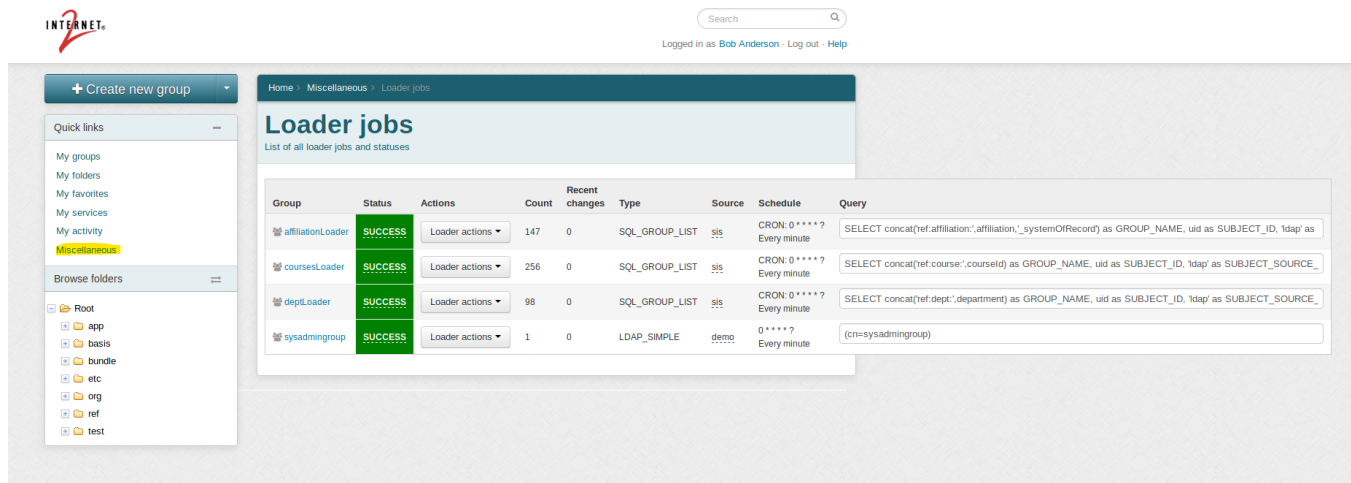
Import of groups from SIS to Grouper

Now you should import groups from the source system (SIS) to Grouper. There is a script `create-ref-loaders.sh` that does it:

[illegible]

Checking groups in Grouper (optional)

The loaders that were created run each minute. So after a while, when logging into Grouper (URL <https://localhost:4443/grouper>, user `banderson`, password `password`) you can see them. Note that the first time you'd have to accept invalid certificate and fill-in data for Shibboleth IdP. After successful login you'd choose Miscellaneous and Loader jobs you'd see this:



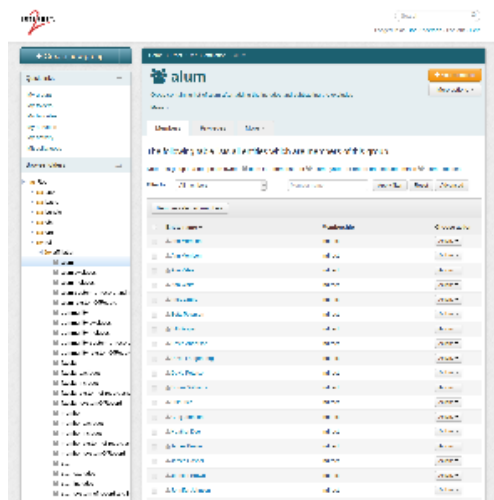
Home > Miscellaneous > Loader jobs

Loader jobs

List of all loader jobs and statuses

Group	Status	Actions	Count	Recent changes	Type	Source	Schedule	Query
affiliationLoader	SUCCESS	Loader actions ▾	147	0	SQL_GROUP_LIST	sis	CRON: 0 * * * * ? Every minute	SELECT concat(ref:affiliation:',affiliation_',systemOfRecord) as GROUP_NAME, uid as SUBJECT_ID, 'ldap' as
courseLoader	SUCCESS	Loader actions ▾	256	0	SQL_GROUP_LIST	sis	CRON: 0 * * * * ? Every minute	SELECT concat(ref:course:',courseId) as GROUP_NAME, uid as SUBJECT_ID, 'ldap' as SUBJECT_SOURCE,
deptLoader	SUCCESS	Loader actions ▾	98	0	SQL_GROUP_LIST	sis	CRON: 0 * * * * ? Every minute	SELECT concat(ref:dept:',department) as GROUP_NAME, uid as SUBJECT_ID, 'ldap' as SUBJECT_SOURCE,
sysadminGroup	SUCCESS	Loader actions ▾	1	0	LDAP_SIMPLE	demo	0 * * * * ? Every minute	(cn=sysadminGroup)

And, after selecting `ref:affiliation:alum` group you can see its members:



Home > Miscellaneous > alum

alum

Group of 25 members

Showing 25 members of this group

Username	Password	Visibility
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible
banderson	password	Visible

Creating additional groups in Grouper

This demo makes use of an extra group `app:cs` that contains all members of all `ref:course:CSxxx` groups. In order to create it, please execute `add-ref-groups.sh` command:

```

$ ./add-ref-groups.sh
Detected Grouper directory structure 'api' (valid is api or webapp)
Using GROUPER_HOME:          /opt/grouper/grouper.apiBinary
Using GROUPER_CONF:          /opt/grouper/grouper.apiBinary/conf
Using JAVA:                   /usr/lib/jvm/zulu-8/bin/java
Using CLASSPATH:              /opt/grouper/grouper.apiBinary/conf:/opt/grouper/grouper.apiBinary/dist/lib
/grouper.jar:/opt/grouper/grouper.apiBinary/lib/grouper/*:/opt/grouper/grouper.apiBinary/lib/custom/*:/opt
/grouper/grouper.apiBinary/lib/jdbcSamples/*:/opt/grouper/grouper.apiBinary/lib/ant/*:/opt/grouper/grouper.
apiBinary/lib/test/*:/opt/grouper/grouper.apiBinary/dist/lib/test/*:/opt/grouper/grouper.apiBinary/src/resources
using MEMORY:                  64m-750m
Grouper starting up: version: 2.4.0, build date: null, env: <no label configured>
grouperPatchStatus read from: /opt/grouper/grouper.apiBinary/grouperPatchStatus.properties
api patches installed:         0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22,
23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47
pspng patches installed:       0, 1, 2, 3, 4, 5, 6
grouper.properties read from: /opt/grouper/grouper.apiBinary/conf/grouper.properties
Grouper current directory is: /opt/grouper/grouper.apiBinary
log4j.properties read from:   /opt/grouper/grouper.apiBinary/conf/log4j.properties
Grouper is logging to file:    /tmp/logpipe, at min level WARN for package: edu.internet2.middleware.grouper,
based on log4j.properties
grouper.hibernate.properties: /run/secrets/grouper_grouper.hibernate.properties
grouper.hibernate.properties: root@jdbc:mysql://grouper_data:3306/grouper?
Charset=utf8&useUnicode=true&characterEncoding=utf8
subject.properties read from: /run/secrets/grouper_subject.properties
sources configured in:        subject.properties
subject.properties ldap source id: ldap: demo
subject.properties grouper source id: g:gsa
subject.properties grouper source id: grouperEntities
SLF4J: Class path contains multiple SLF4J bindings.
SLF4J: Found binding in [jar:file:/opt/grouper/grouper.apiBinary/lib/grouper/slf4j-log4j12.jar!/org/slf4j/impl
/StaticLoggerBinder.class]
SLF4J: Found binding in [jar:file:/opt/grouper/grouper.apiBinary/lib/custom/slf4j-log4j12-1.7.25.jar!/org/slf4j
/impl/StaticLoggerBinder.class]
SLF4J: See http://www.slf4j.org/codes.html#multiple_bindings for an explanation.
SLF4J: Actual binding is of type [org.slf4j.impl.Log4jLoggerFactory]
Type help() for instructions
Groovy Shell (2.5.0-beta-2, JVM: 1.8.0_212)
Type 'help' or 'h' for help.
-----
groovy:000> :load '/opt/grouper/grouper.apiBinary/conf/groovysh.profile'
groovy:000> :gshFileLoad '/tmp/add-ref-groups.gsh'
====> true
====> 9f26c411a68e46fdb32420b1236db96e, 'GrouperSystem', 'application'
====> Group[name=app:cs,uuid=8aaa8d8ec19d4487b5a3957a9c655beb]
Ignoring: Group[name=ref:course:ACCT101,uuid=3d175d5918404d55b7ac2c041cf235ec]
Ignoring: Group[name=ref:course:ACCT201,uuid=d58376315c8f4ba0bc4932b90ea3287c]
Adding: Group[name=ref:course:CS251,uuid=e236408ac58e470b8127e3d540c9123e]
Adding: Group[name=ref:course:CS252,uuid=c8373932b92d4bf097ab6296fbbcaff7]
Ignoring: Group[name=ref:course:MATH100,uuid=141df2d51edc4cc6899833d284267da4]
Ignoring: Group[name=ref:course:MATH101,uuid=e8b673fa50a84d5099915b395d0f912b]
Ignoring: Group[name=ref:course:SCI123,uuid=dbd45fb5ad1c4b2b968964bcaa7bfe1f]
Ignoring: Group[name=ref:course:SCI404,uuid=8f2b949af9c74f68b38444868f23bd58]
====> null
groovy:000> :exit

```

Note that this requires courses to be already imported. So it's advisable to wait about 2 minutes after loaders creation before issuing this command.

Importing of groups from Grouper to midPoint

Grouper allows you to tailor group membership by using includes and excludes, and to create new groups. So you can free to do that, either at this point or later.

Regardless of whether you do that now or later, you can import groups to midPoint now.

It is done by importing `midpoint-objects-manual/tasks/task-reconciliation-grouper-groups.xml` or by executing `upload-reconcile-grouper-groups.sh` command:

```
$ ./upload-reconcile-grouper-groups.sh
Uploading midpoint-objects-manual/tasks/task-reconciliation-grouper-groups.xml (tasks, 605a0127-a313-442a-9d5e-151eac8b0745)
```

You can check the task using midPoint GUI:

midPoint demo/grouper: Edit Reconciliation task 'Grouper reconciliation (groups)'

Grouper reconciliation (groups)
Progress: 30 (closed)
Last object processed: testvolunteers
4/29/20, 5:44:46 PM - 4/29/20, 5:45:06 PM (00:00:19.888)

Buttons: Run now, Suspend, Refresh, Stop, Play (no refreshing)

Tabs: Basic, Schedule, Work management, Operation statistics, Environmental performance, Internal performance, Result, Errors

Progress

Objects successfully processed	30 (average time 357 ms, total processing time 10 seconds)
Last object successfully processed	testvolunteers (ENTITLEMENT - group - Group) April 29, 2020, 5:45:06 PM (in 187 ms)
Objects failed to be processed	0
Last object failed to be processed	
Last error when processing object	
Current object being processed	
Total objects processed	30 (wall clock average: 662 ms, throughput: 90 per minute)

States of processed objects

Situation	Before (count)	After (count)
Unmatched	30	0
Unlinked	0	0
Linked	0	30
Deleted	0	0

The second step of groups import is the recomputation of users in midPoint. It should be started after group reconciliation is done. Let's omit technical details for now; the reason lies in the way how group membership is represented in midPoint-Grouper connector.

This recomputation is done by importing midpoint-objects-manual/tasks/task-recomputation-users.xml or by executing upload-recompute-users.sh command:

```
$ ./upload-recompute-users.sh
Uploading midpoint-objects-manual/tasks/task-recomputation-users.xml (tasks, 83a737ea-5eb7-4e78-b431-331cccf02354)
```

The corresponding task should look like this:

midPoint demo/grouper: Edit Recomputation task 'User recomputation'

User recomputation
Progress: 78 out of 102
Last object processed: gjohansson
Started 4/29/20, 5:48:03 PM (00:00:36.201 ago)

Buttons: Suspend, Run now, Refresh, Stop, Play (Refreshing each 2 sec)

Tabs: Basic, Schedule, Operation statistics, Environmental performance, Internal performance, Result, Errors

Progress

Objects successfully processed	78 (average time 457 ms, total processing time 35 seconds)
Last object successfully processed	User Greg Johnson (gjohansson) April 29, 2020, 5:48:39 PM (0 seconds ago - in 345 ms)
Objects failed to be processed	0
Last object failed to be processed	
Last error when processing object	
Current object being processed	User Donna Langenberg (dlangenberg81) April 29, 2020, 5:48:39 PM (0 seconds ago)
Total objects processed	78 (wall clock average: 464 ms, throughput: 129 per minute)

States of processed objects

Situation	Before (count)	After (count)
Unmatched	78	0
Unlinked	0	0
Linked	0	78
Deleted	0	0

Actions executed (resulting actions)

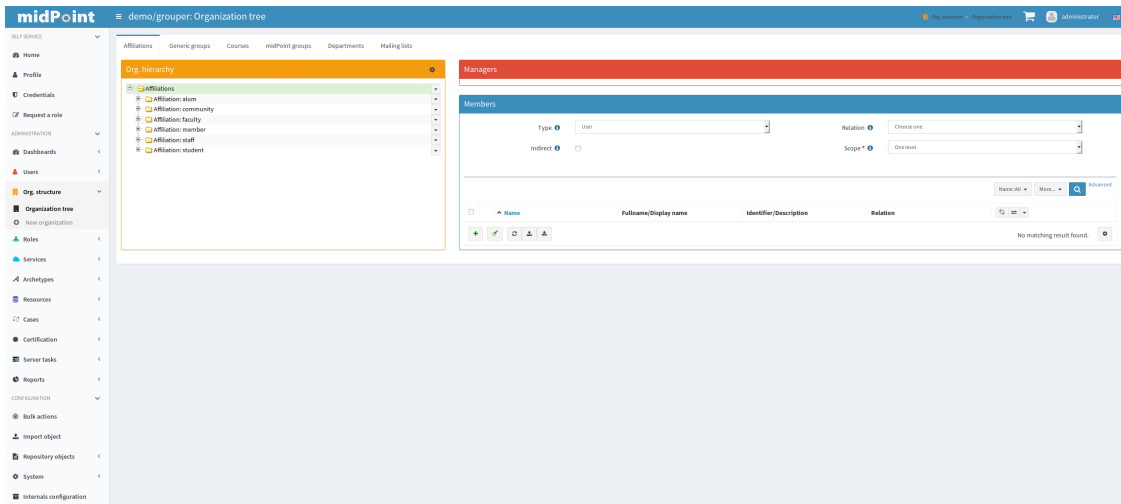
Showing "resulting actions" only. E.g. user ADD and MODIFY in one synchronization operation is shown as ADD.

Object type	Operation	Channel	Count (OK)	Last (OK)	Time	Count (failure)

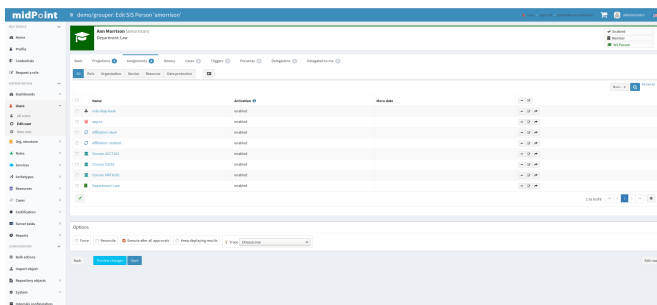
Checking the groups in midPoint (optional)

Groups in Grouper are represented as midPoint organizations. And group membership is then represented as userorganization assignments.

The organization tree looks like this:



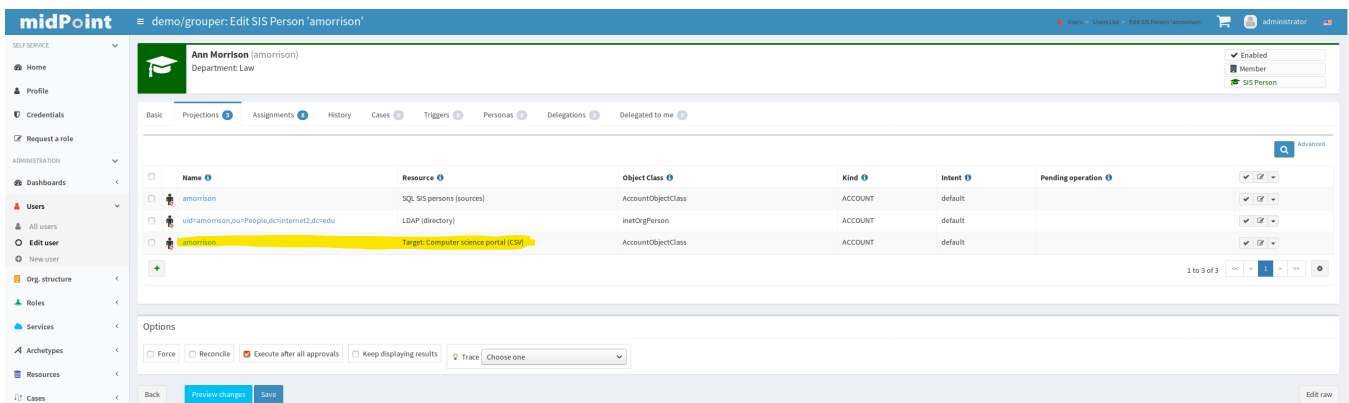
And user assignments are (e.g. for amorrison):



We can see she has an affiliations of `alum` and `student`, courses `ACCT101`, `CS251`, `MATH101`, department of `Law`, and one other membership in `app:CS`.

Memberships in these organizations induces other accounts and entitlements, as defined in midPoint configuration.

In this case, enrollment in CS courses gives Ann an account on Computer Science portal:



Also, there is a membership in appropriate LDAP groups for her account:

The screenshot shows the midPoint user profile for Ann Morrison. The 'Attributes' tab is selected, displaying various LDAP attributes. The 'Associations' tab is also visible, showing group memberships. A red circle highlights the group memberships in the 'Associations' tab.

Department is reflected in businessCategory LDAP attribute.

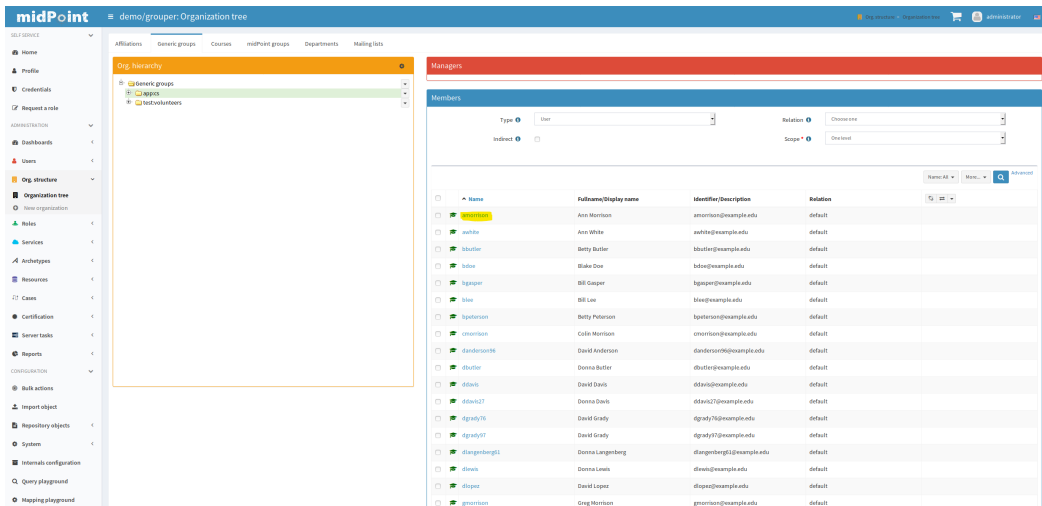
The same information can now be seen via LDAP browser:

The screenshot shows the LDAP browser displaying the user profile for Ann Morrison. The 'Attributes' tab is selected, showing LDAP attributes. The 'Outline' tab is also visible, showing the object structure.

...and for membership, e.g. in app:cs group:

The screenshot shows the LDAP browser displaying the group membership for the app:cs group. The 'Attributes' tab is selected, showing LDAP attributes. The 'Outline' tab is also visible, showing the object structure.

The members of groups (organizations) can be seen also in midPoint:



Starting near real-time synchronization from Grouper to midPoint

Besides "full" synchronization (in midPoint it's called reconciliation) this demo provides near real-time synchronization using asynchronous messages emitted by Grouper and provided to midPoint via RabbitMQ message-queuing system.

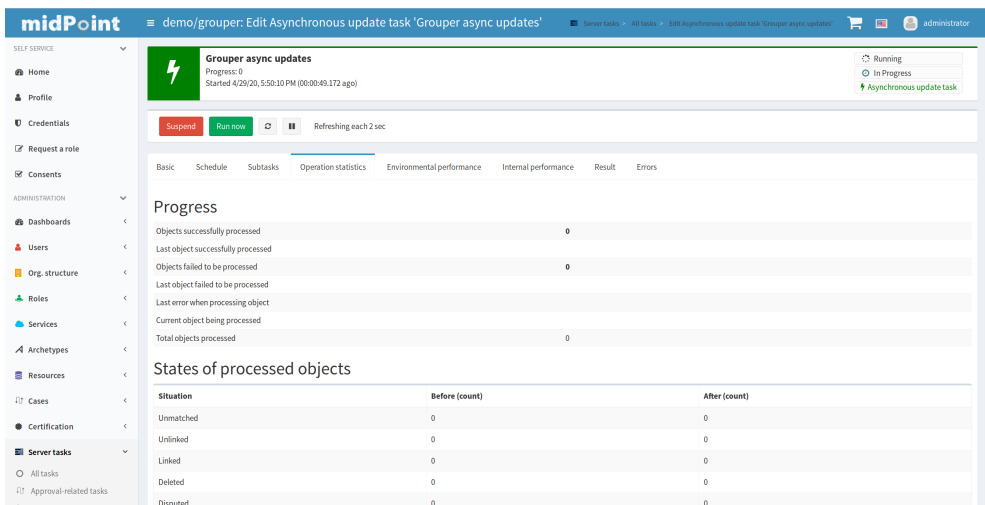
First, you can clear the queue from messages that were generated so far. Information they carry was already passed to midPoint using direct connection during previous reconciliation:

```
$ ./purge-queue.sh
Purging queue 'sampleQueue' in vhost '/' ...
```

Then you can import the task that handles asynchronous update messages:

```
$ ./upload-async-update-task.sh
Uploading midpoint-objects-manual/tasks/task-async-update-grouper.xml (tasks, 47fc57bd-8c34-4555-9b9f-7087ff179860)
```

The task does nothing at this stage. It simply waits for messages that will be generated after any changes occur in Grouper.



Making some changes in Grouper (optional)

Initially, Bill Gasper (bgasper) is a member of ref:affiliation:alum, ref:course:CS251, ref:course:MATH100, ref:dept:Business and ap p:cs groups.

Let's make slight changes in Grouper.

1. add him to ref:affiliation:alum_excludes, effectively removing his alum membership,
2. add him to ref:affiliation:faculty_includes, effectively adding him to faculty group even if he's not declared as such in SIS,
3. add him to app:mailinglist:chess, app:mailinglist:idm-fans, and test:volunteers groups.

You can do that either from Grouper GUI or by simply running the `./update-bgasper-in-grouper.sh` command:

```
$ ./update-bgasper-in-grouper.sh
Detected Grouper directory structure 'api' (valid is api or webapp)
Using GROUPER_HOME:           /opt/grouper/grouper.apiBinary
Using GROUPER_CONF:           /opt/grouper/grouper.apiBinary/conf
Using JAVA:                    /usr/lib/jvm/zulu-8//bin/java
Using CLASSPATH:               /opt/grouper/grouper.apiBinary/conf:/opt/grouper/grouper.apiBinary/dist/lib
/grouper.jar:/opt/grouper/grouper.apiBinary/lib/grouper/*:/opt/grouper/grouper.apiBinary/lib/custom/*:/opt
/grouper/grouper.apiBinary/lib/jdbcSamples/*:/opt/grouper/grouper.apiBinary/lib/ant/*:/opt/grouper/grouper.
apiBinary/lib/test/*:/opt/grouper/grouper.apiBinary/dist/lib/test/*:/opt/grouper/grouper.apiBinary/src/resources
using MEMORY:                  64m-750m
Grouper starting up: version: 2.4.0, build date: null, env: <no label configured>
grouperPatchStatus read from: /opt/grouper/grouper.apiBinary/grouperPatchStatus.properties
api patches installed:         0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22,
23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47
pspng patches installed:       0, 1, 2, 3, 4, 5, 6
grouper.properties read from: /opt/grouper/grouper.apiBinary/conf/grouper.properties
Grouper current directory is: /opt/grouper/grouper.apiBinary
log4j.properties read from:   /opt/grouper/grouper.apiBinary/conf/log4j.properties
Grouper is logging to file:    /tmp/logpipe, at min level WARN for package: edu.internet2.middleware.grouper,
based on log4j.properties
grouper.hibernate.properties: /run/secrets/grouper_grouper.hibernate.properties
grouper.hibernate.properties: root@jdbc:mysql://grouper_data:3306/grouper?
Charset=utf8&useUnicode=true&characterEncoding=utf8
subject.properties read from: /run/secrets/grouper_subject.properties
sources configured in:         subject.properties
subject.properties ldap source id: ldap: demo
subject.properties grouperSource id: g:gsa
subject.properties grouperSource id: grouperEntities
SLF4J: Class path contains multiple SLF4J bindings.
SLF4J: Found binding in [jar:file:/opt/grouper/grouper.apiBinary/lib/grouper/slf4j-log4j12.jar!/org/slf4j/impl
/StaticLoggerBinder.class]
SLF4J: Found binding in [jar:file:/opt/grouper/grouper.apiBinary/lib/custom/slf4j-log4j12-1.7.25.jar!/org/slf4j
/impl/StaticLoggerBinder.class]
SLF4J: See http://www.slf4j.org/codes.html#multiple_bindings for an explanation.
SLF4J: Actual binding is of type [org.slf4j.impl.Log4jLoggerFactory]
Type help() for instructions
Groovy Shell (2.5.0-beta-2, JVM: 1.8.0_212)
Type ':help' or ':h' for help.

-----
groovy:000> :load '/opt/grouper/grouper.apiBinary/conf/groovysh.profile'
groovy:000> :gshFileLoad '/tmp/update-bgasper-in-grouper.gsh'
====> true
====> 40b6d30710d548108b27566f18e9a074, 'GrouperSystem', 'application'
====> Subject id: bgasper, sourceId: ldap, name: Bill Gasper
====> true
====> true
====> true
====> true
====> true
groovy:000> :exit
```

After 1-2 minutes, appropriate messages are sent from Grouper and received by midPoint, as can be seen at the console, like this:

```
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 19:37:01,288 [MODEL] [AMQP-consumer-3-1] INFO (com.
evolveum.midpoint.expression): esbEvent = {sourceId=ldap, membershipType=flattened, fieldName=members,
groupId=a9d13f7cb8e84c5e9cefe28dela6f47b, changeOccurred=false, createdOnMicros=1574364982157000,
subjectId=bgasper, id=b8cff3f2c4e3407e9dd712020e32caa4, sequenceNumber=2010, eventType=MEMBERSHIP_DELETE,
groupName=ref:affiliation:alum}
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 19:37:01,295 [MODEL] [AMQP-consumer-3-1] INFO (com.
evolveum.midpoint.expression): ### bgasper - MEMBERSHIP_DELETE - ref:affiliation:alum
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 19:37:01,385 [MODEL] [AMQP-consumer-3-1] INFO (com.
evolveum.midpoint.expression): Recompute trigger for bgasper: added
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 19:37:01,477 [] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.provisioning.ucf.impl.builtin.async.sources.Amqp091AsyncUpdateSource): Received a message on
```



```
amq.ctag-ZzhDMBfPuwM8TuxUFeznfg
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,477 [] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.provisioning.ucf.impl.builtin.async.sources.Amqp091AsyncUpdateSource): Message is:
midpoint_server_1 | midpoint:midpoint.log;demo;;{"encrypted":false,"esbEvent":[{"sourceId":"ldap","
membershipType":"flattened","fieldName":"members","groupId":"75b9bf96091a4fc1a84f20d1107dc3c4","changeOccurred":
false,"createdOnMicros":1574364982164000,"subjectId":"bgasper","id":"be9cf480499f409f8ef392556602f66b","
sequenceNumber":"2011","eventType":"MEMBERSHIP_ADD","groupName":"ref:affiliation:alum_excludes"}]}
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,484 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): esbEvent = {sourceId=ldap, membershipType=flattened, fieldName=members,
groupId=75b9bf96091a4fc1a84f20d1107dc3c4, changeOccurred=false, createdOnMicros=1574364982164000,
subjectId=bgasper, id=be9cf480499f409f8ef392556602f66b, sequenceNumber=2011, eventType=MEMBERSHIP_ADD,
groupName=ref:affiliation:alum_excludes}
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,484 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): Irrelevant group membership change, ignoring it: ref:affiliation:alum_excludes
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,486 [] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.provisioning.ucf.impl.builtin.async.sources.Amqp091AsyncUpdateSource): Received a message on
amq.ctag-ZzhDMBfPuwM8TuxUFeznfg
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,486 [] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.provisioning.ucf.impl.builtin.async.sources.Amqp091AsyncUpdateSource): Message is:
midpoint_server_1 | midpoint:midpoint.log;demo;;{"encrypted":false,"esbEvent":[{"sourceId":"ldap","
membershipType":"flattened","fieldName":"members","groupId":"9a33a4bd9b034defbc526d912d9e99ae","changeOccurred":
false,"createdOnMicros":1574364982326000,"subjectId":"bgasper","id":"e514333ba14b4e2fa93c2123efab9d5c","
sequenceNumber":"2012","eventType":"MEMBERSHIP_ADD","groupName":"ref:affiliation:faculty"}]}
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,488 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): esbEvent = {sourceId=ldap, membershipType=flattened, fieldName=members,
groupId=9a33a4bd9b034defbc526d912d9e99ae, changeOccurred=false, createdOnMicros=1574364982326000,
subjectId=bgasper, id=e514333ba14b4e2fa93c2123efab9d5c, sequenceNumber=2012, eventType=MEMBERSHIP_ADD,
groupName=ref:affiliation:faculty}
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,488 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): ### bgasper - MEMBERSHIP_ADD - ref:affiliation:faculty
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,489 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): Recompute trigger for bgasper: not added (already present or user not found)
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,525 [] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.provisioning.ucf.impl.builtin.async.sources.Amqp091AsyncUpdateSource): Received a message on
amq.ctag-ZzhDMBfPuwM8TuxUFeznfg
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,525 [] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.provisioning.ucf.impl.builtin.async.sources.Amqp091AsyncUpdateSource): Message is:
midpoint_server_1 | midpoint:midpoint.log;demo;;{"encrypted":false,"esbEvent":[{"sourceId":"ldap","
membershipType":"flattened","fieldName":"members","groupId":"c6379b765f0547f9b452eea801d60ddb","changeOccurred":
false,"createdOnMicros":1574364982337000,"subjectId":"bgasper","id":"17ccf93101d545ce8d95d27a7b386011","
sequenceNumber":"2013","eventType":"MEMBERSHIP_ADD","groupName":"ref:affiliation:faculty_includes"}]}
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,527 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): esbEvent = {sourceId=ldap, membershipType=flattened, fieldName=members,
groupId=c6379b765f0547f9b452eea801d60ddb, changeOccurred=false, createdOnMicros=1574364982337000,
subjectId=bgasper, id=17ccf93101d545ce8d95d27a7b386011, sequenceNumber=2013, eventType=MEMBERSHIP_ADD,
groupName=ref:affiliation:faculty_includes}
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,527 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): Irrelevant group membership change, ignoring it: ref:affiliation:faculty_includes
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,528 [] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.provisioning.ucf.impl.builtin.async.sources.Amqp091AsyncUpdateSource): Received a message on
amq.ctag-ZzhDMBfPuwM8TuxUFeznfg
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,528 [] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.provisioning.ucf.impl.builtin.async.sources.Amqp091AsyncUpdateSource): Message is:
midpoint_server_1 | midpoint:midpoint.log;demo;;{"encrypted":false,"esbEvent":[{"sourceId":"ldap","
membershipType":"flattened","fieldName":"members","groupId":"97956145001742bda00fe6f034300ce3","changeOccurred":
false,"createdOnMicros":1574364982337000,"subjectId":"bgasper","id":"17ccf93101d545ce8d95d27a7b386011","
sequenceNumber":"2014","eventType":"MEMBERSHIP_ADD","groupName":"ref:affiliation:
faculty_systemOfRecordAndIncludes"}]}
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,529 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): esbEvent = {sourceId=ldap, membershipType=flattened, fieldName=members,
groupId=97956145001742bda00fe6f034300ce3, changeOccurred=false, createdOnMicros=1574364982337000,
subjectId=bgasper, id=17ccf93101d545ce8d95d27a7b386011, sequenceNumber=2014, eventType=MEMBERSHIP_ADD,
groupName=ref:affiliation:faculty_systemOfRecordAndIncludes}
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,530 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): Irrelevant group membership change, ignoring it: ref:affiliation:
faculty_systemOfRecordAndIncludes
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,531 [] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.provisioning.ucf.impl.builtin.async.sources.Amqp091AsyncUpdateSource): Received a message on
amq.ctag-ZzhDMBfPuwM8TuxUFeznfg
midpoint_server_1 | midpoint:midpoint.log;demo;;2019-11-21 19:37:01,531 [] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.provisioning.ucf.impl.builtin.async.sources.Amqp091AsyncUpdateSource): Message is:
```

```

midpoint_server_1 | midpoint;midpoint.log;demo;;{"encrypted":false,"esbEvent":[{"sourceId":"ldap","
membershipType":"flattened","fieldName":"members","groupId":"dd700af2446b45d3b807f531e779cd8a","changeOccurred":
false,"createdOnMicros":1574364982401000,"subjectId":"bgasper","id":"8b993f08d63847dea37dd1999e635ff2","
sequenceNumber":"2015","eventType":"MEMBERSHIP_ADD","groupName":"app:mailinglist:chess"}]}
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 19:37:01,532 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): esbEvent = {sourceId=ldap, membershipType=flattened, fieldName=members,
groupId=dd700af2446b45d3b807f531e779cd8a, changeOccurred=false, createdOnMicros=1574364982401000,
subjectId=bgasper, id=8b993f08d63847dea37dd1999e635ff2, sequenceNumber=2015, eventType=MEMBERSHIP_ADD,
groupName=app:mailinglist:chess}
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 19:37:01,532 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): ### bgasper - MEMBERSHIP_ADD - app:mailinglist:chess
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 19:37:01,533 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): Recompute trigger for bgasper: not added (already present or user not found)
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 19:37:01,573 [] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.provisioning.ucf.impl.builtin.async.sources.Amqp091AsyncUpdateSource): Received a message on
amq.ctag-ZzhDMBfPuwM8TuxUFeznfg
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 19:37:01,573 [] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.provisioning.ucf.impl.builtin.async.sources.Amqp091AsyncUpdateSource): Message is:
midpoint_server_1 | midpoint;midpoint.log;demo;;{"encrypted":false,"esbEvent":[{"sourceId":"ldap","
membershipType":"flattened","fieldName":"members","groupId":"dceb02717aec43f085ebaabd49c01462","changeOccurred":
false,"createdOnMicros":1574364982479000,"subjectId":"bgasper","id":"444e88225882479a84d8b5c857e57d06","
sequenceNumber":"2016","eventType":"MEMBERSHIP_ADD","groupName":"app:mailinglist:idm-fans"}]}
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 19:37:01,574 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): esbEvent = {sourceId=ldap, membershipType=flattened, fieldName=members,
groupId=dceb02717aec43f085ebaabd49c01462, changeOccurred=false, createdOnMicros=1574364982479000,
subjectId=bgasper, id=444e88225882479a84d8b5c857e57d06, sequenceNumber=2016, eventType=MEMBERSHIP_ADD,
groupName=app:mailinglist:idm-fans}
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 19:37:01,575 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): ### bgasper - MEMBERSHIP_ADD - app:mailinglist:idm-fans
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 19:37:01,575 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): Recompute trigger for bgasper: not added (already present or user not found)
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 19:37:01,612 [] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.provisioning.ucf.impl.builtin.async.sources.Amqp091AsyncUpdateSource): Received a message on
amq.ctag-ZzhDMBfPuwM8TuxUFeznfg
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 19:37:01,612 [] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.provisioning.ucf.impl.builtin.async.sources.Amqp091AsyncUpdateSource): Message is:
midpoint_server_1 | midpoint;midpoint.log;demo;;{"encrypted":false,"esbEvent":[{"sourceId":"ldap","
membershipType":"flattened","fieldName":"members","groupId":"5ae830647de347babff3f5bfbfd733bc5","changeOccurred":
false,"createdOnMicros":1574364982559000,"subjectId":"bgasper","id":"7bd7d7689d5443fe84ffd9097ddfc98f","
sequenceNumber":"2017","eventType":"MEMBERSHIP_ADD","groupName":"test:volunteers"}]}
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 19:37:01,614 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): esbEvent = {sourceId=ldap, membershipType=flattened, fieldName=members,
groupId=5ae830647de347babff3f5bfbfd733bc5, changeOccurred=false, createdOnMicros=1574364982559000,
subjectId=bgasper, id=7bd7d7689d5443fe84ffd9097ddfc98f, sequenceNumber=2017, eventType=MEMBERSHIP_ADD,
groupName=test:volunteers}
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 19:37:01,614 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): ### bgasper - MEMBERSHIP_ADD - test:volunteers
midpoint_server_1 | midpoint;midpoint.log;demo;;2019-11-21 19:37:01,614 [MODEL] [AMQP-consumer-3-2] INFO (com.
evolveum.midpoint.expression): Recompute trigger for bgasper: not added (already present or user not found)

```

Corresponding changes are stored in midPoint now. But for performance reasons, user recomputation (including e.g. LDAP account modifications, additional accounts provisioning or deprovisioning, and so on) is carried out by Trigger Scanner that runs regularly. So, at most after 6 minutes, user bgasper should be recomputed in midPoint:

midPoint demo/grouper:Edit SIS Person 'bgasper'

SELF SERVICE

- Home
- Profile
- Credentials
- Request a role

ADMINISTRATION

- Dashboards
- Users
 - All users
 - Edit user
 - New user
- Org. structure
- Roles
- Services
- Archetypes
- Resources
- Cases
- Certification
- Server tasks
- Reports

CONFIGURATION

- Build actions
- Import object
- Repository objects

Bill Gasper (bgasper) app:cs

Basic Projections Assignments History Cases Triggers Personas Delegations Delegated to me

Role: Role basic

Name	Activation	More data
role: Role basic	enabled	
app:cs	enabled	
Course: CS251	enabled	
Course: MATH100	enabled	
Department: Business	enabled	
Affiliation: Faculty	enabled	
Mailing list: idm-fans	enabled	
Mailing list: chess	enabled	
Testvolunteers	enabled	

Options

Force Reconcile Execute after all approvals Keep displaying results Trace Choose one

Back Preview changes Save Edit row

midPoint demo/grouper:Edit SIS Person 'bgasper'

SELF SERVICE

- Home
- Profile
- Credentials
- Request a role

ADMINISTRATION

- Dashboards
- Users
 - All users
 - Edit user
 - New user
- Org. structure
- Roles
- Services
- Archetypes
- Resources
- Cases
- Certification
- Server tasks

Bill Gasper (bgasper) app:cs

Basic Projections Assignments History Cases Triggers Personas Delegations Delegated to me

Projection

Name	Resource	Object Class	Kind	Intent	Pending operation
bgasper	SQL SIS persons (sources)	AccountObjectClass	ACCOUNT	default	
uid=bgasper,ou=People,dc=internet2,dc=edu	LDAP (directory)	inetOrgPerson	ACCOUNT	default	
bgasper	Target: Computer science portal (CSV)	AccountObjectClass	ACCOUNT	default	
bgasper	Target: Mailing lists (CSV)	AccountObjectClass	ACCOUNT	default	
bgasper	Target: Faculty portal (CSV)	AccountObjectClass	ACCOUNT	default	

Options

Force Reconcile Execute after all approvals Keep displaying results Trace Choose one

Back Preview changes Save Edit row

Switching midPoint authentication to Shibboleth (optional)

Finally we can switch midPoint authentication from the internal one to Shibboleth-based. You rewrite name of authentication module for sequence admin-gui-default in Default Security Policy. You have to find:

```
<sequence>
  <name>admin-gui-default</name>
  <description>
    Default GUI authentication sequence.
  </description>
  <channel>
    <channelId>http://midpoint.evolveum.com/xml/ns/public/common/channels-3#user</channelId>
    <default>true</default>
    <urlSuffix>gui-default</urlSuffix>
  </channel>
  <module>
    <name>internalLoginForm</name>
    <order>30</order>
    <necessity>sufficient</necessity>
  </module>
</sequence>
```

And change `<name>internalLoginForm</name>` to `<name>mySamlSso</name>`. After saving of security policy you have to logout.

Now you can log into midPoint at <http://localhost:8443/midpoint>. You will be redirected to Shibboleth login page where you would log in using banderson/password.

You can log into midPoint using the emergency URL <https://localhost:8443/midpoint/auth/emergency> that will point you to midPoint login page (instead of Shibboleth one). Then you will use administrator as a user name and 5ecr3t as a password.

Additional Details

Conclusion

This sample environment shows a proposal how to use midPoint along with Grouper for managing identities at a university. It is **not** a complete solution. Due to time limitations, some of the components are more sketches than production-ready implementations. For example, scripted SQL connectors do not support filtering, paging, nor live synchronization. Data model is greatly simplified. Security and performance issues were taken into account, but not yet fully validated.

Nevertheless, we consider this to be a good basis for getting acquainted with midPoint/Grouper integration as well as for future discussion on suitable architecture of midPoint/Grouper deployment in higher education.