INTERNET2

2022 TECHNOLOGY exchange

Grouper BoF

Chris Hyzer: Penn, Grouper lead
Shilen Patel: Duke, Grouper developer

INTERNET2

Table of Contents

- Grouper team
- What is Grouper
- Versioning
- Roadmap
- Community contributions
- Recent progress
- Training
- Discussion

Grouper team

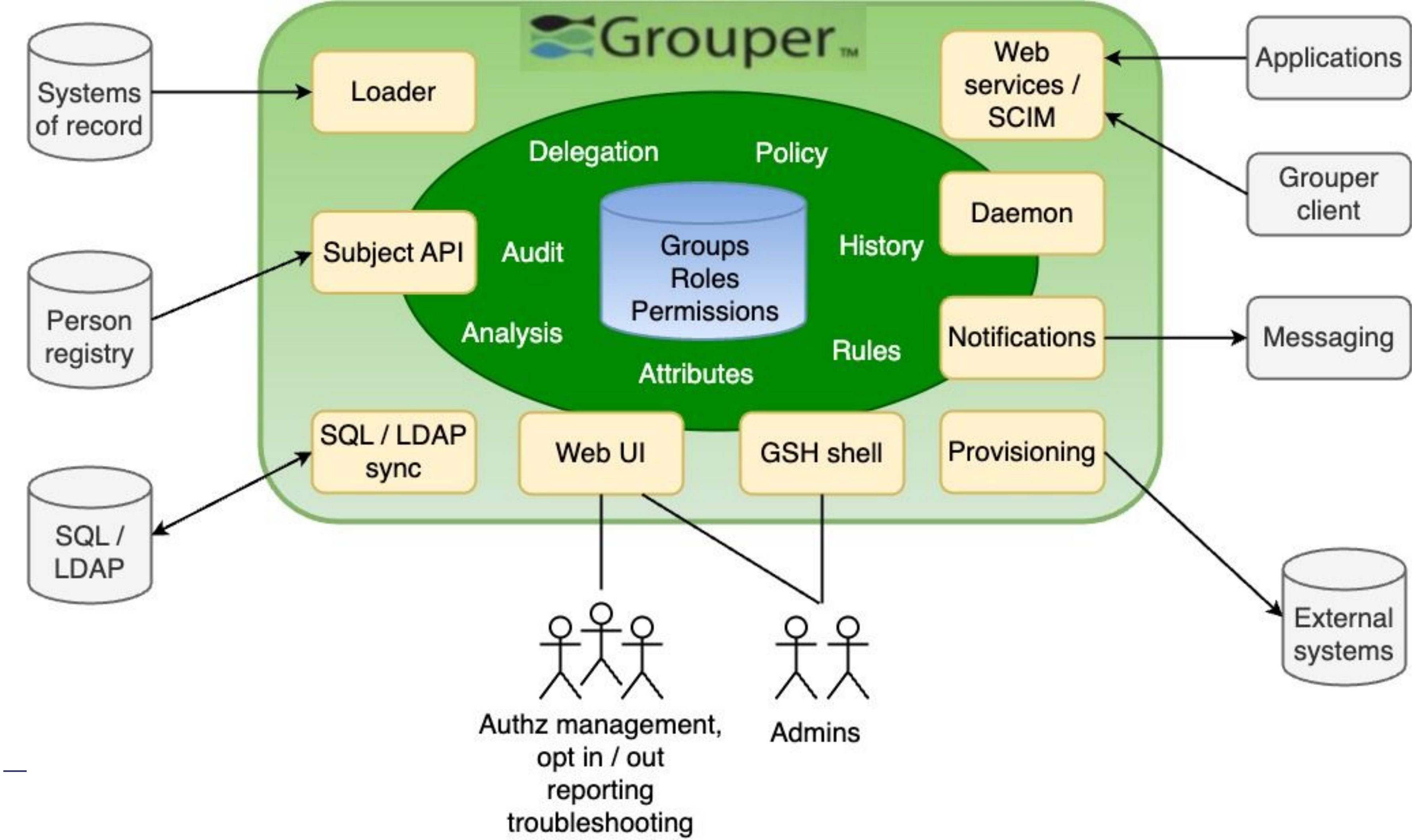
Grouper team (alphabetical)

- **Carey Matt Black** (Ohio State) – general support
- **Emily Eisbruch** (Internet2) - work group support
- **Chris Hubing** (Internet2) - systems support
- **Chris Hyzer** (Penn) - Grouper lead, training, developer
- **JJ (Johnson)** (Unicon) – Contributor
- **Shilen Patel** (Duke) – Developer
- **Chad Redman** (Unicon) – Developer, training
- **Vivek Sachdeva** (independent) – Developer

What is Grouper

What is Grouper

- Central authorization
- Groups
- Permissions
- Loading
- Provisioning
- Auditing
- Analysis
- Delegation and distributed management
- Platform


Grouper™
Systems of record
Loader
Web services / SCIM
Applications
Grouper client
Delegation
Policy
Daemon
Subject API
Audit
Groups
Roles
Permissions
History
Person registry
Analysis
Rules
Notifications
Messaging
Attributes
SQL / LDAP sync
Web UI
GSH shell
Provisioning
SQL / LDAP
External systems
Authz management, opt in / out reporting troubleshooting
Admins

Versioning

Versioning

- Semantic versioning (like)
  - 3 version number only
- Major number (even): stable no enhancement version
  - Backwards compatible
  - Fewer upgrade steps
  - Requires less testing on upgrades
- Major version (odd): enhancement version
  - Newest features
  - Upgrade steps
  - Requires more testing on upgrades
- Version means something. (e.g. are you on 2.5 enhancement version or LTS?)

Versioning (continued)

- Use a supported version
- Upgrade every 1-3 months
- Select enhancement version or not based on needs
- Security fixes of third party libraries

Versioning (continued)

- 2.5 will remain 2.5
    - 2.5 supported until May 2023
- 2.6 will be v4.x.y when last enhancements done
- Next version is v5.x.y (ABAC)
- Once that is feature complete will be v6.x.y

Roadmap

Grouper v2.6

- Remaining features
  - Polish provisioning framework
  - Make sure the “Start withs” make sense
  - JEXL expression editor
  - Add remedy provisioner

Grouper v4.0

- Will be released in a month or two
- Same as v2.6.last
    - No upgrade steps
    - Direct path to upgrade
- Old SCIM will be removed
    - There is a new more secure SCIM WS
    - Not being used
    - Tomee -> Tomcat
- SOAP will be removed by default
    - Could be added back with config

Grouper v5.0

- Previous v2.7
- Removing SOAP

Grouper v5.0 - container changes

- Rocky linux
- Multi-platform (e.g. works with ARM)
- Apache and Shib SP removed
    - Could be installed in subimage
- Tomcat is single process
- Lightweight OIDC UI authn
- Many other authn options (SAML/CAS/etc)

Grouper v5.0 - provisioning changes

- Removing PSPNG
- Removing legacy Azure provisioner
- Removing legacy Google provisioner
- Removing legacy Box provisioner
- Removing legacy Duo provisioner
- Removing legacy etc provisioner
- Messaging change log consumers will still exist
    - Use the messaging provisioner? :)

Grouper v5.0 - roadmap

- ABAC
- Add data field based subject source
- etc

Grouper v6.0 - roadmap

- Is the non-enhancement version of v5.0

Grouper v7.0 - roadmap

- Previous v3.0
- Redo the Grouper database structure
- Focus on performance
- Reduce DB size
- Reduce query complexity
- Reduce data transfer on wire
- Reduce memory requirements
- Improve performance of all three supported databases

Community contributions

Community contributions

Princeton University - **(2022)** Using Grouper with Azure.

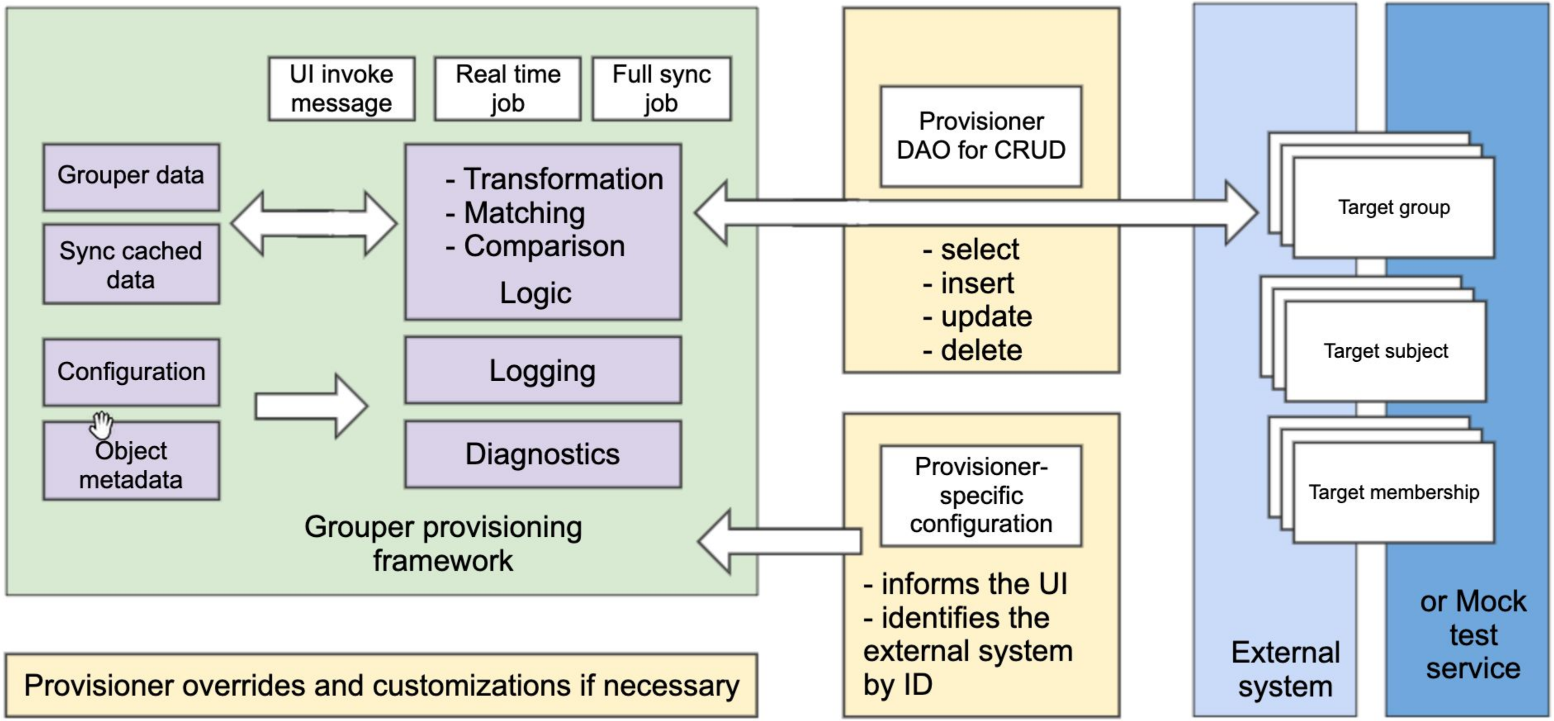
Illinois State University **(New October 2021) -** Using Grouper for IAM needs

Community contributions

- Share your Grouper experience on the Grouper wiki
  - Update it from time to time
  - https://spaces.internet2.edu/display/Grouper/Community+Contributions
- Email Emily Eisbruch (emily@internet2.edu) for help
  - Setting up your Grouper contributions page
  - Updating the last updated date for your institution
- Thanks to all those who have recently updated their Grouper Contrib page!

Recent progress

Provisioning framework



UI invoke message

Real time job

Full sync job

Grouper data

Sync cached data

- Transformation
- Matching
- Comparison

Logic

Configuration

Object metadata

Logging

Diagnostics

Grouper provisioning framework

Provisioner overrides and customizations if necessary

Provisioner DAO for CRUD

- select
- insert
- update
- delete

Provisioner-specific configuration

- informs the UI
- identifies the external system by ID

Target group

Target subject

Target membership

External system

or Mock test service

Provisioning framework

- All provisioners use same framework
- Any framework fixes or enhancements apply to app provisioners
- Provisioners differ by
  - DAO (how it inserts/updates/deletes/selects)
  - Provisioning specific configuration (e.g. base DN)
  - Validation
  - Start withs

Provisioning framework

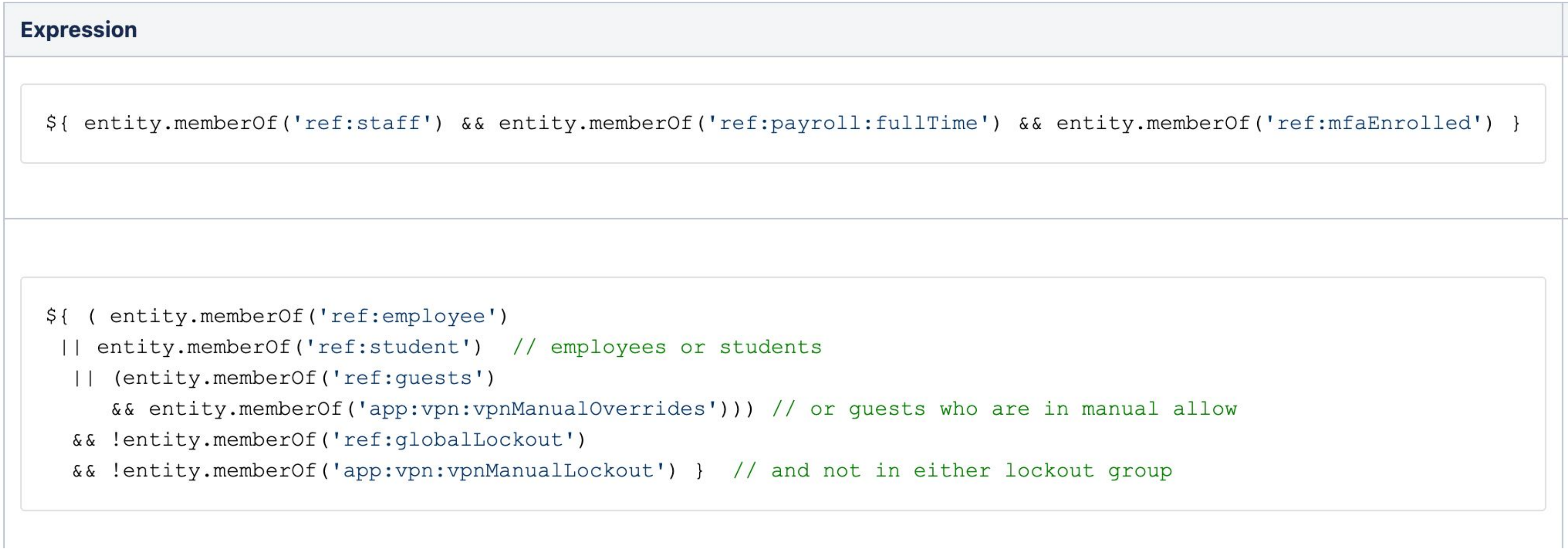
- Consistent unit tests
- Mock services
- Extensive UI support
  - Troubleshooting
  - Recalc
- Delegatable
- Caching target state in database
- Helpful logs
- Full and incremental for all (well, except messaging)
- Loading
- Metadata
- Will only get better

Provisioning framework

- Demo?
- https://grouperdemo.internet2.edu/grouper_v2_6/grouperUi/app/UiV2Main.index?operation=UiV2ProvisionerConfiguration.addProvisionerConfiguration
-

Scripted groups

- Multi-factor composites

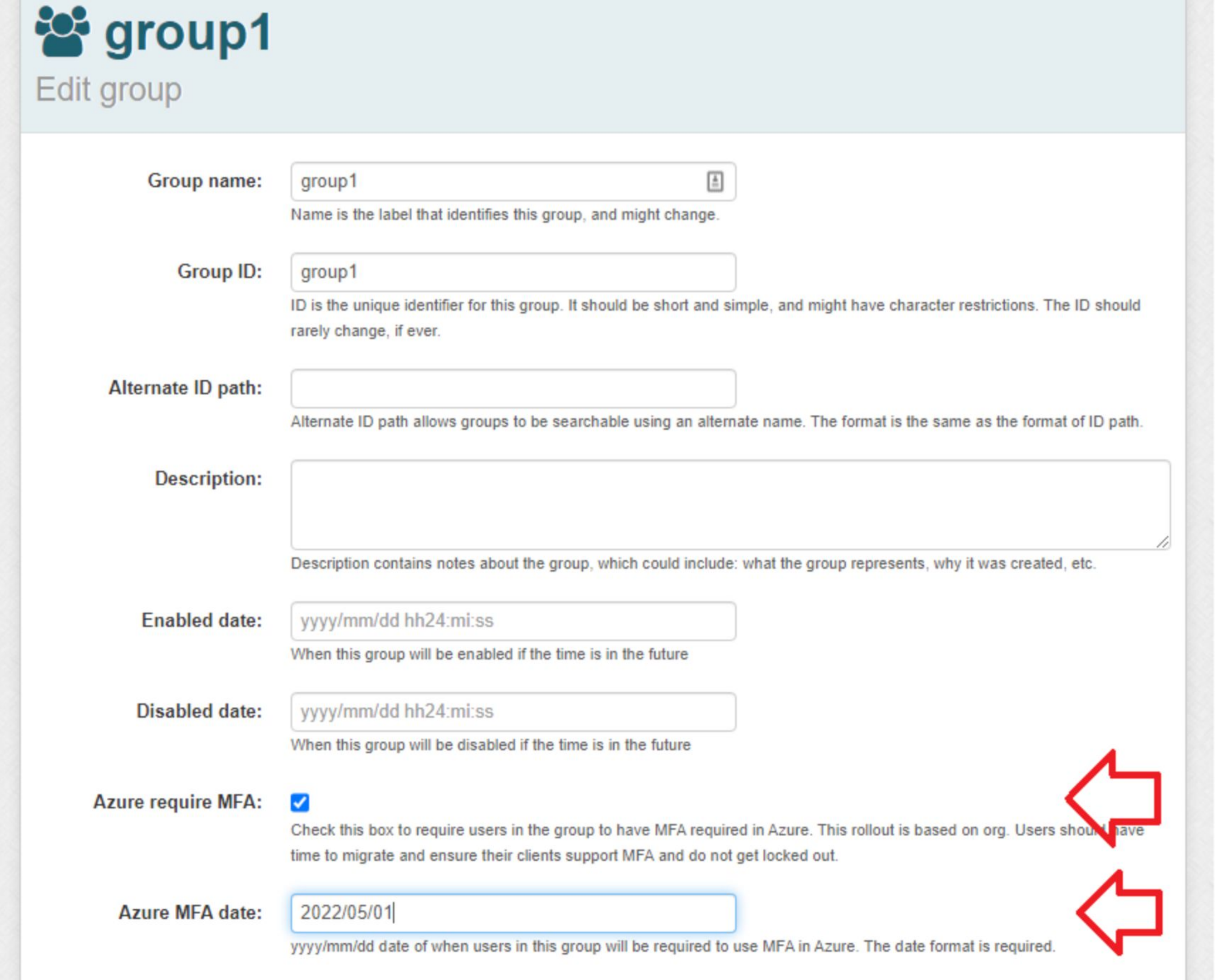


Expression

```
${ entity.memberOf('ref:staff') && entity.memberOf('ref:payroll:fullTime') && entity.memberOf('ref:mfaEnrolled') }
```

```
${ ( entity.memberOf('ref:employee')
 || entity.memberOf('ref:student')  // employees or students
  || (entity.memberOf('ref:guests')
     && entity.memberOf('app:vpn:vpnManualOverrides'))) // or guests who are in manual allow
  && !entity.memberOf('ref:globalLockout')
  && !entity.memberOf('app:vpn:vpnManualLockout') }  // and not in either lockout group
```

Attributes on group edit screen



group1

Edit group

Group name: group1

Name is the label that identifies this group, and might change.

Group ID: group1

ID is the unique identifier for this group. It should be short and simple, and might have character restrictions. The ID should rarely change, if ever.

Alternate ID path:

Alternate ID path allows groups to be searchable using an alternate name. The format is the same as the format of ID path.

Description:

Description contains notes about the group, which could include: what the group represents, why it was created, etc.

Enabled date: yyyy/mm/dd hh24:mi:ss

When this group will be enabled if the time is in the future

Disabled date: yyyy/mm/dd hh24:mi:ss

When this group will be disabled if the time is in the future

Azure require MFA: ☑

Check this box to require users in the group to have MFA required in Azure. This rollout is based on org. Users should have time to migrate and ensure their clients support MFA and do not get locked out.

Azure MFA date: 2022/05/01

yyyy/mm/dd date of when users in this group will be required to use MFA in Azure. The date format is required.

Authn methods

- Trusted JWT WS
- Self-service JWT WS
- OIDC WS
- OIDC UI

Folder privileges

- View privilege on folders
- Secure folder viewing
  - Users only see folders they have access to objects (or can VIEW)
  - Performance works

Membership requirements

- See wiki

https://spaces.at.internet2.edu/display/Grouper/Penn+membership+requirements

SOAP Deprecation

- SOAP web services will be removed in Grouper 5.0.0
- When you upgrade to the next 2.6 version (2.6.19+), logs will show SOAP requests

```
2022-12-02T15:13:00,033: [http-nio-8080-exec-2] WARN  GrouperService.addMemberLite(1878) - [< test.subject.0 -
0:0:0:0:0:0:0:1 >] - DEPRECATED-SOAP will be removed in Grouper 5.0.0+.  subjectLoggedIn=Subject id: test.subject.0,
sourceId: jdbc, name: my name is test.subject.0
```

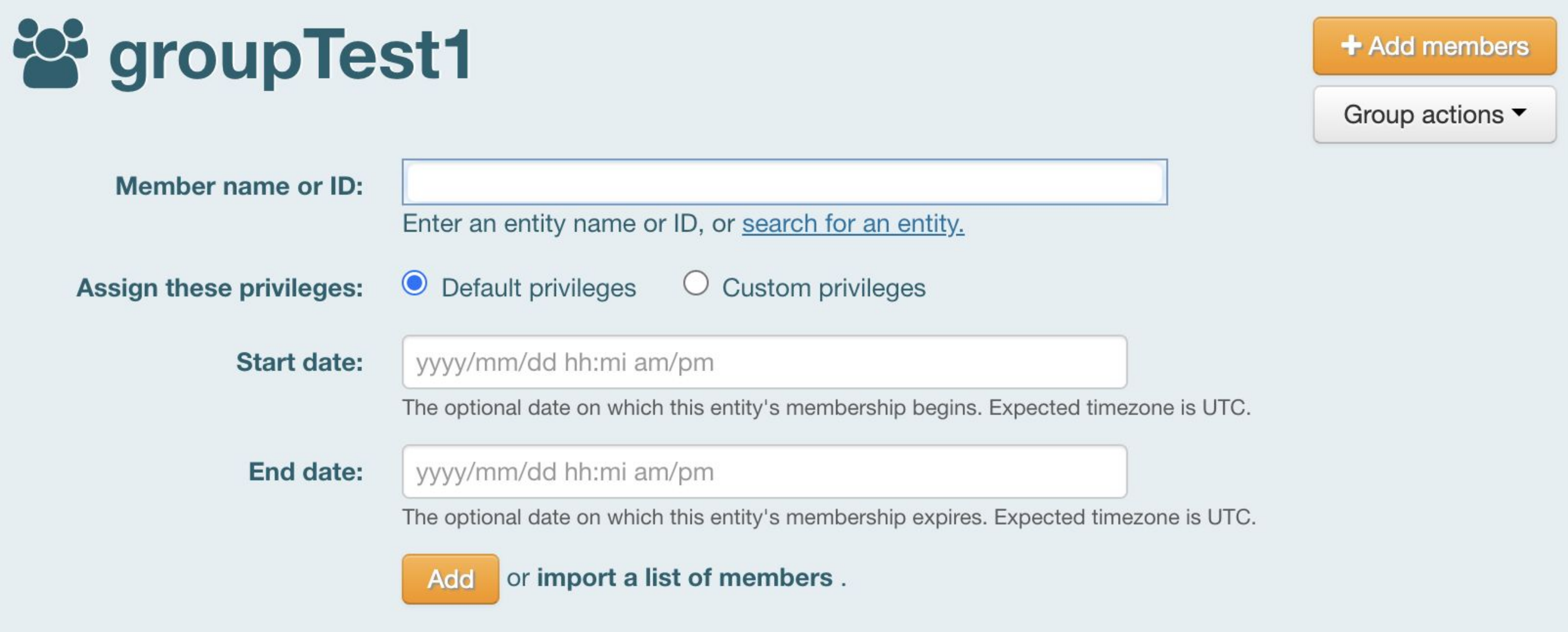
Unresolvable Subjects in Provisioning

- An unresolvable subject is a subject who no longer exists in your subject source.
- Grouper checks for unresolvable subjects every day. By default, when a subject is seen as unresolvable for more than 30 days, Grouper will consider them deleted.
- Provisioning framework needed to allow options for how unresolvable subjects are handled.
- Two new options now
  - Unresolvable subjects insert
  - Unresolvable subjects remove

Enable / Disable Dates

- When adding a member to a group, you can now optionally specify the enable and disable dates.
- When importing members to a group, you can specify enable and disable dates too. And existing memberships are updated if the dates are different.
- The daemon to enable and disable objects now runs every minute instead of only a couple of times a day.

Enable / Disable Dates (continued)



groupTest1

Member name or ID:	Enter an entity name or ID, or search for an entity.
Assign these privileges:	● Default privileges ○ Custom privileges
Start date:	yyyy/mm/dd hh:mi am/pm The optional date on which this entity's membership begins. Expected timezone is UTC.
End date:	yyyy/mm/dd hh:mi am/pm The optional date on which this entity's membership expires. Expected timezone is UTC.

or **import a list of members** .

Self Read

- New property for global self read of memberships
- Allows users to see their own memberships for groups that they have the VIEW privilege on

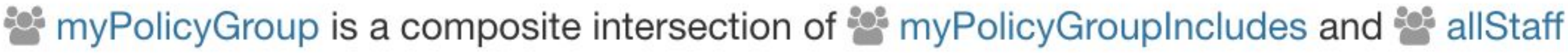
Trace Memberships

- Changes made to the ‘trace memberships’ screen to better assist with analyzing access

- Previously 'trace memberships' would only work on current memberships

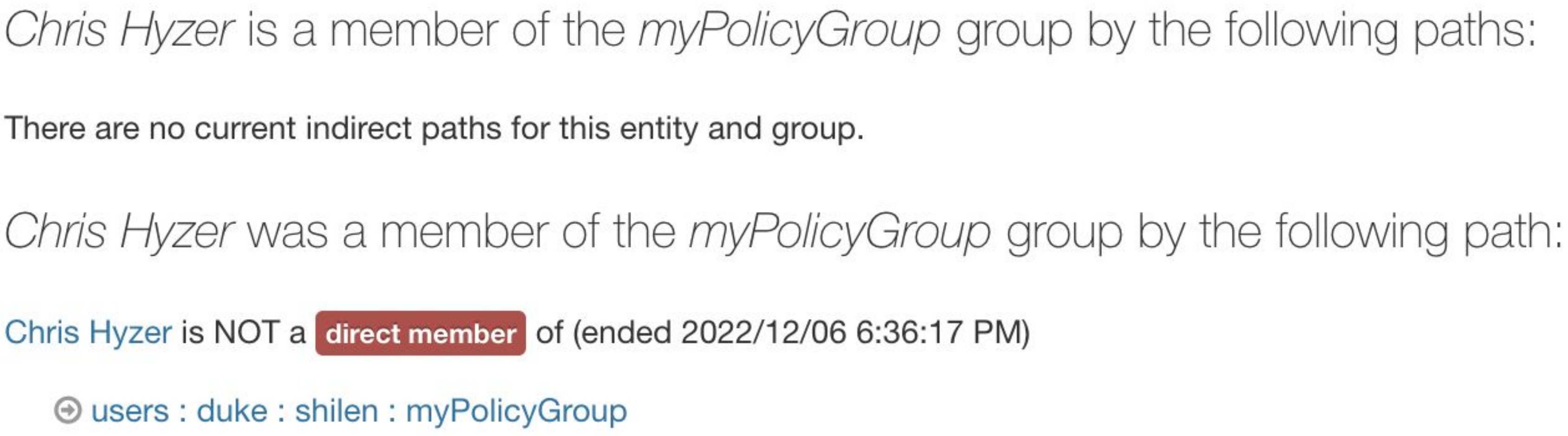
- Now you can perform the action on previous memberships based on point in time data

Trace Memberships (continued)



myPolicyGroup is a composite intersection of myPolicyGroupIncludes and allStaff

Trace Memberships (continued)



Chris Hyzer is a member of the *myPolicyGroup* group by the following paths:

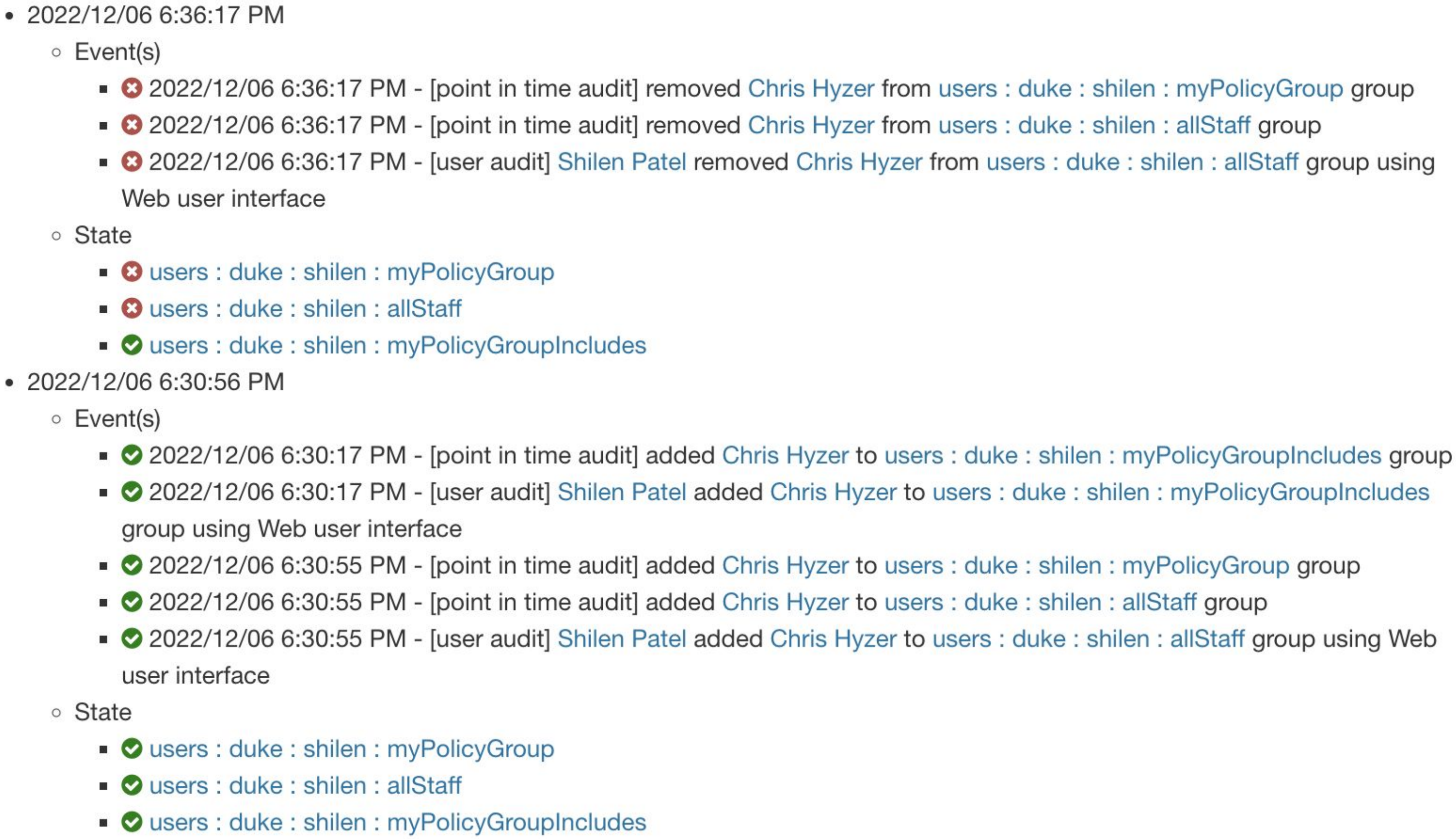
There are no current indirect paths for this entity and group.

Chris Hyzer was a member of the *myPolicyGroup* group by the following path:

Chris Hyzer is NOT a **direct member** of (ended 2022/12/06 6:36:17 PM)

➔ users : duke : shilen : myPolicyGroup

Trace Memberships (continued)



- 2022/12/06 6:36:17 PM
  - Event(s)
    - ✖ 2022/12/06 6:36:17 PM - [point in time audit] removed Chris Hyzer from users : duke : shilen : myPolicyGroup group
    - ✖ 2022/12/06 6:36:17 PM - [point in time audit] removed Chris Hyzer from users : duke : shilen : allStaff group
    - ✖ 2022/12/06 6:36:17 PM - [user audit] Shilen Patel removed Chris Hyzer from users : duke : shilen : allStaff group using Web user interface
  - State
    - ✖ users : duke : shilen : myPolicyGroup
    - ✖ users : duke : shilen : allStaff
    - ✔ users : duke : shilen : myPolicyGroupIncludes
- 2022/12/06 6:30:56 PM
  - Event(s)
    - ✔ 2022/12/06 6:30:17 PM - [point in time audit] added Chris Hyzer to users : duke : shilen : myPolicyGroupIncludes group
    - ✔ 2022/12/06 6:30:17 PM - [user audit] Shilen Patel added Chris Hyzer to users : duke : shilen : myPolicyGroupIncludes group using Web user interface
    - ✔ 2022/12/06 6:30:55 PM - [point in time audit] added Chris Hyzer to users : duke : shilen : myPolicyGroup group
    - ✔ 2022/12/06 6:30:55 PM - [point in time audit] added Chris Hyzer to users : duke : shilen : allStaff group
    - ✔ 2022/12/06 6:30:55 PM - [user audit] Shilen Patel added Chris Hyzer to users : duke : shilen : allStaff group using Web user interface
  - State
    - ✔ users : duke : shilen : myPolicyGroup
    - ✔ users : duke : shilen : allStaff
    - ✔ users : duke : shilen : myPolicyGroupIncludes

Training

Training

- Given 4 times this year
- For all types of users
  - Admins
  - Power users
  - Helpdesk
- Hands on
- VM to use

Discussion

(not)

End