Open Apereo 2016

100% Open for Education

Grouper in Action

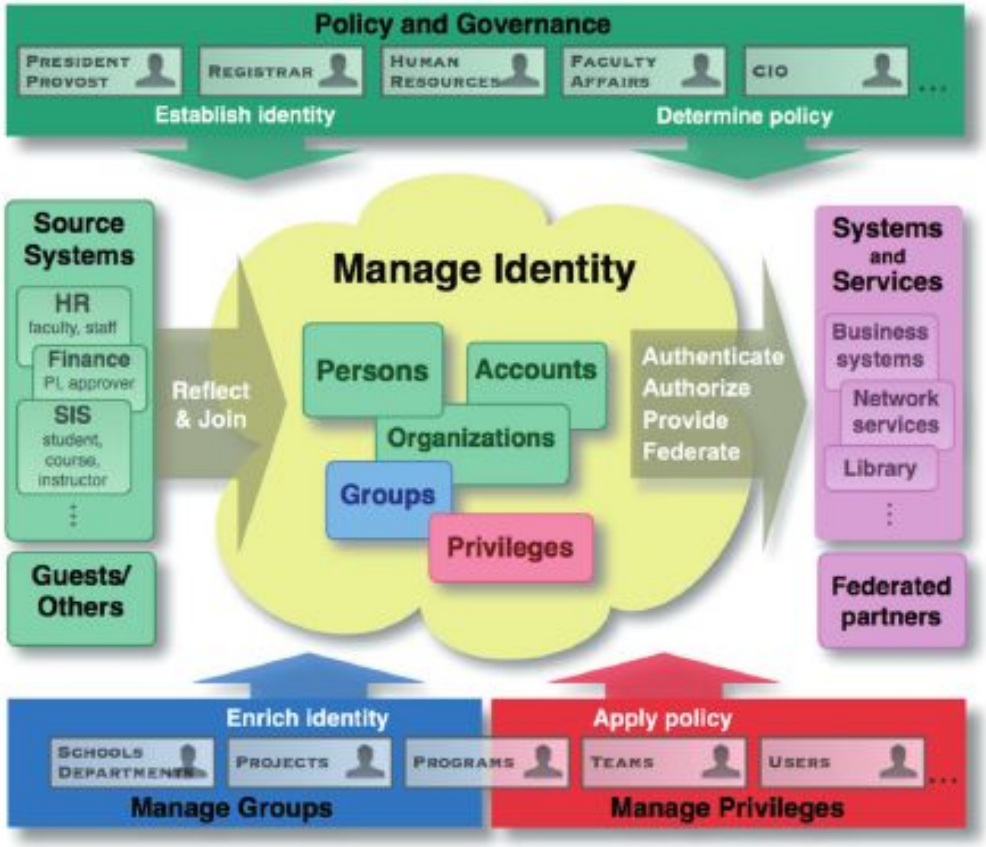
Access Management Strategies for Higher Education and Research

Chris Hyzer, University of Pennsylvania
Bill Thompson, Lafayette College
Jeff Pasch, New York University
Julio Mascavilca, New York University
Madan Dorairaj, New York University

Agenda

1. **Introduction to Grouper**
    a. Grouper Overview
    b. Features and capabilities
    c. What's new
2. **Grouper in Action**
    a. Access Policy and Reference Groups - Lafayette
    b. Grouper, Sakai, and Google - NYU
    c. Organizational Hierarchy and O365 - Penn
    d. Fine grained database permissions - Penn
3. **Hands on Grouper**
    a. Folder and grouper management
    b. Searching and adding subjects
    c. Direct vs indirect membership
    d. Grouper loader jobs
    e. Composite group
4. **Open Q&A**

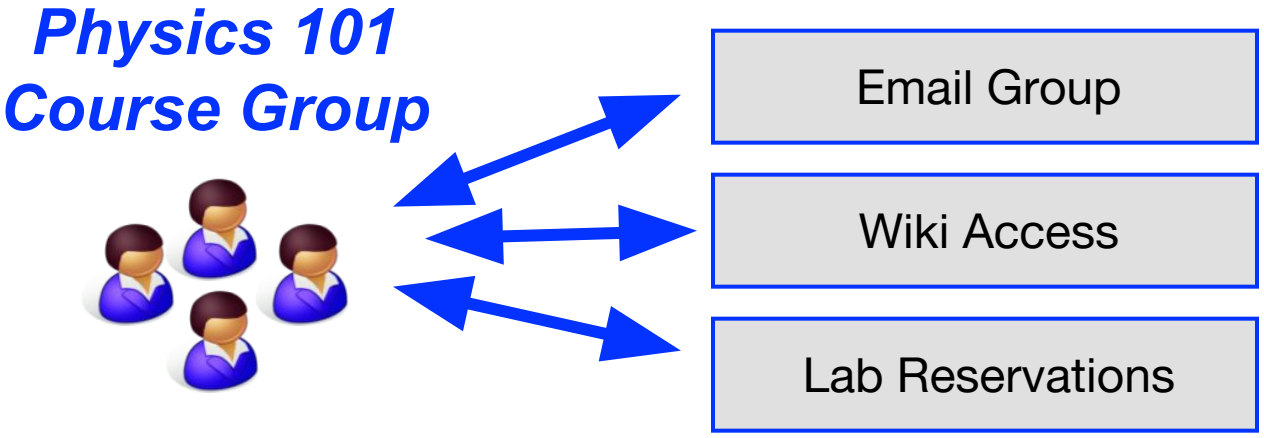
Access management strategy



- Tools & processes to translate IAM concepts into typical campus environment
  - Which people?
  - What systems & business processes?
  - What policies?
  - What purposes?
  - Whose authority?

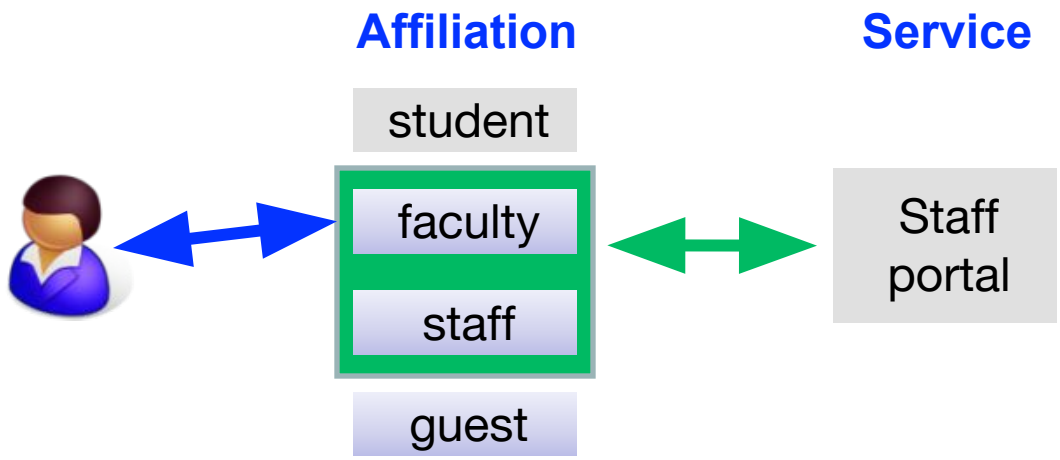
Why have an access management strategy?

- Lower cost and time to deliver a new service
- Simplify access management by using the same group in many places
- Empower the right people to manage access
- Answer who can access what



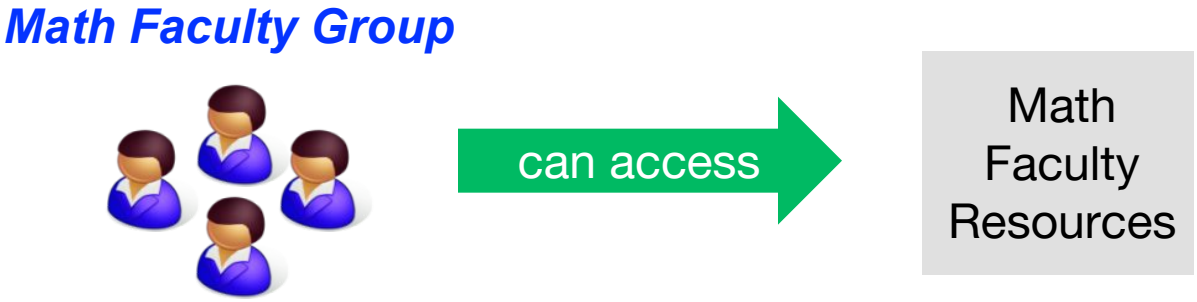
Access management stages:

1. Start out using a single user attribute, *affiliation*, in an Enterprise Directory. Services implement simple access policies.



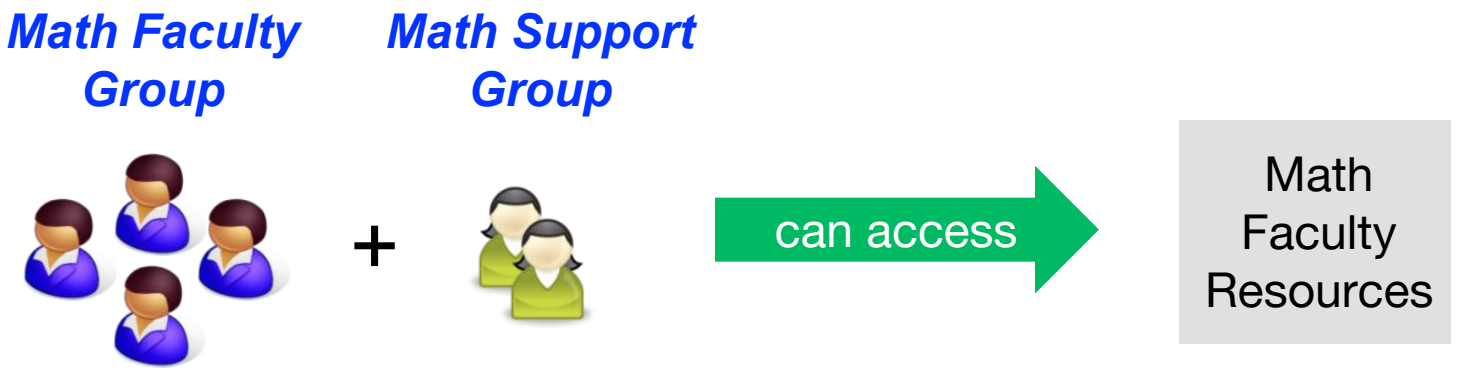
Access management stages

2. Maintain access groups determined from systems of record
   - Courses, departments,…
   - Define service-specific access policies in the centralized access management system



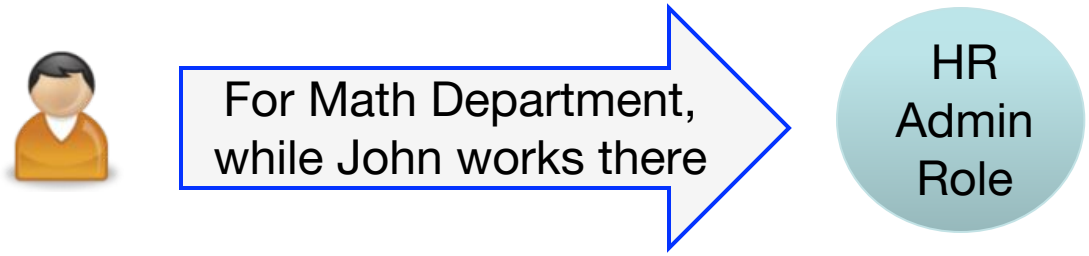
Access management stages

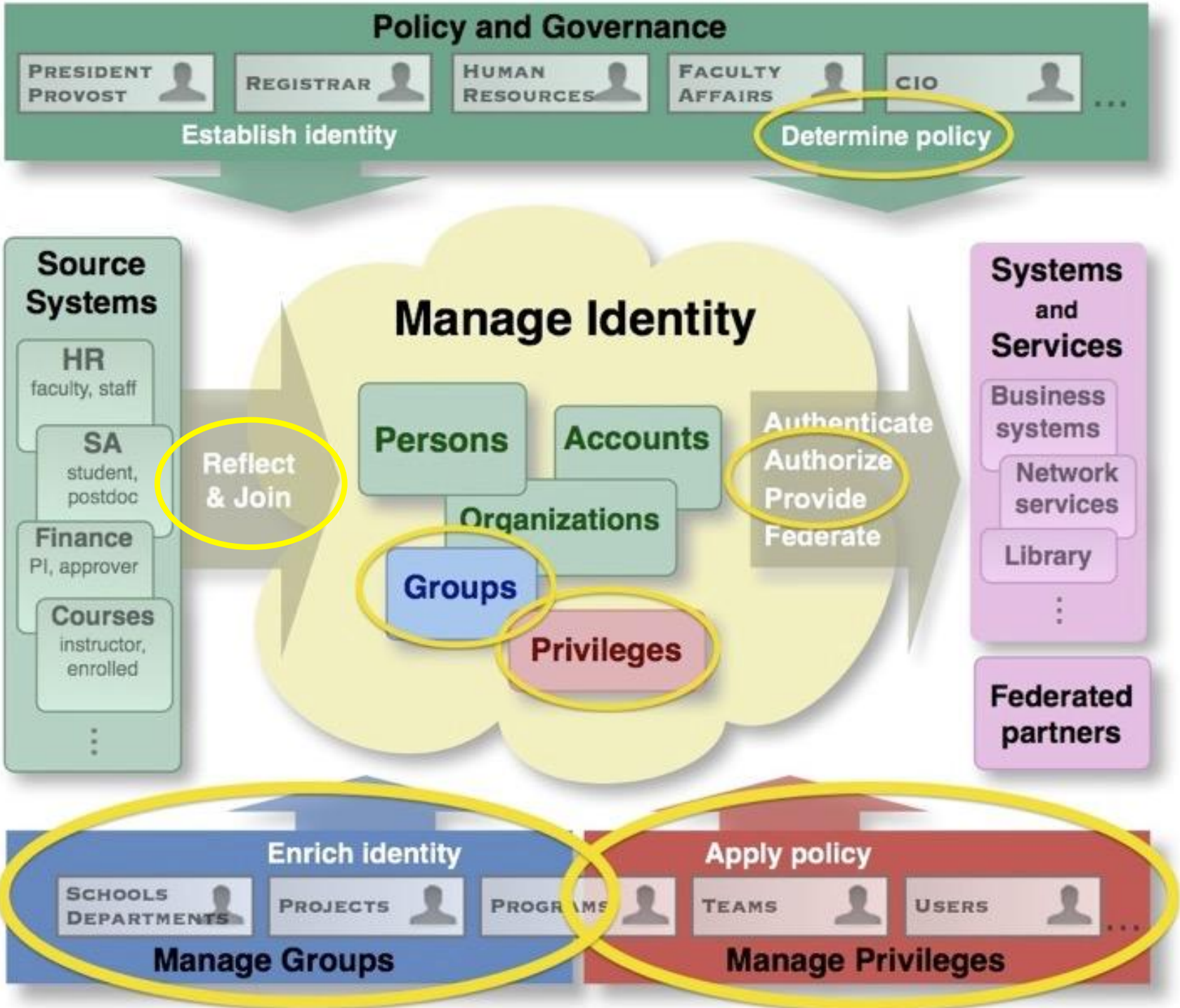
3. Distributed management
   - Departmental applications
   - Ad-hoc teams
   - Exceptions



Access management stages

4. Increase integration
   - Direct integration with applications
   - Roles & privileges to support applications more deeply




Policy and Governance
President
Provost
Registrar
Human Resources
Faculty Affairs
CIO
...
Establish identity
Determine policy
Source Systems
HR
faculty, staff
SA
student, postdoc
Finance
PI, approver
Courses
instructor, enrolled
Reflect & Join
Manage Identity
Persons
Accounts
Organizations
Groups
Privileges
Authenticate
Authorize
Provide
Federate
Systems and Services
Business systems
Network services
Library
Federated partners
Enrich identity
Schools
Departments
Projects
Programs
Manage Groups
Apply policy
Teams
Users
Manage Privileges

Grouper is…

Grouper is an **enterprise access management system** designed for the highly distributed management environment and heterogeneous information technology environment common to Universities.

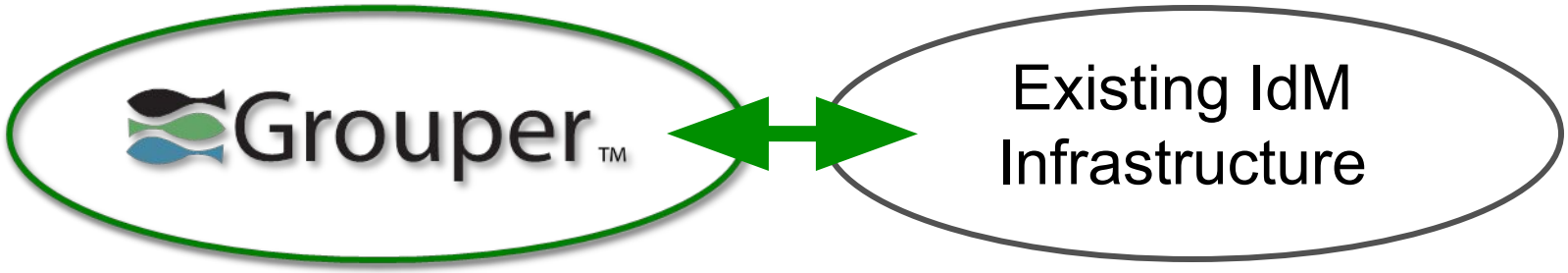
- Coordinated Collaboration
- Single Point of Control
- Distributed Management

The Grouper Story

- Mature, community driven project (2005 initial release)
- Internet2
- National Science Foundation (NSF) Grant No. OCI-0330626, OCI-0721896, and OCI-1032468
- Joint Information Systems Committee (JISC) (UK)
- University of Chicago, University of Pennsylvania, Duke University, University of Washington, University of Memphis, University of Bristol (UK)

The Grouper Story

- Key aims
  - Delegation and distributed management
  - Integration with most any existing Identity Management infrastructure

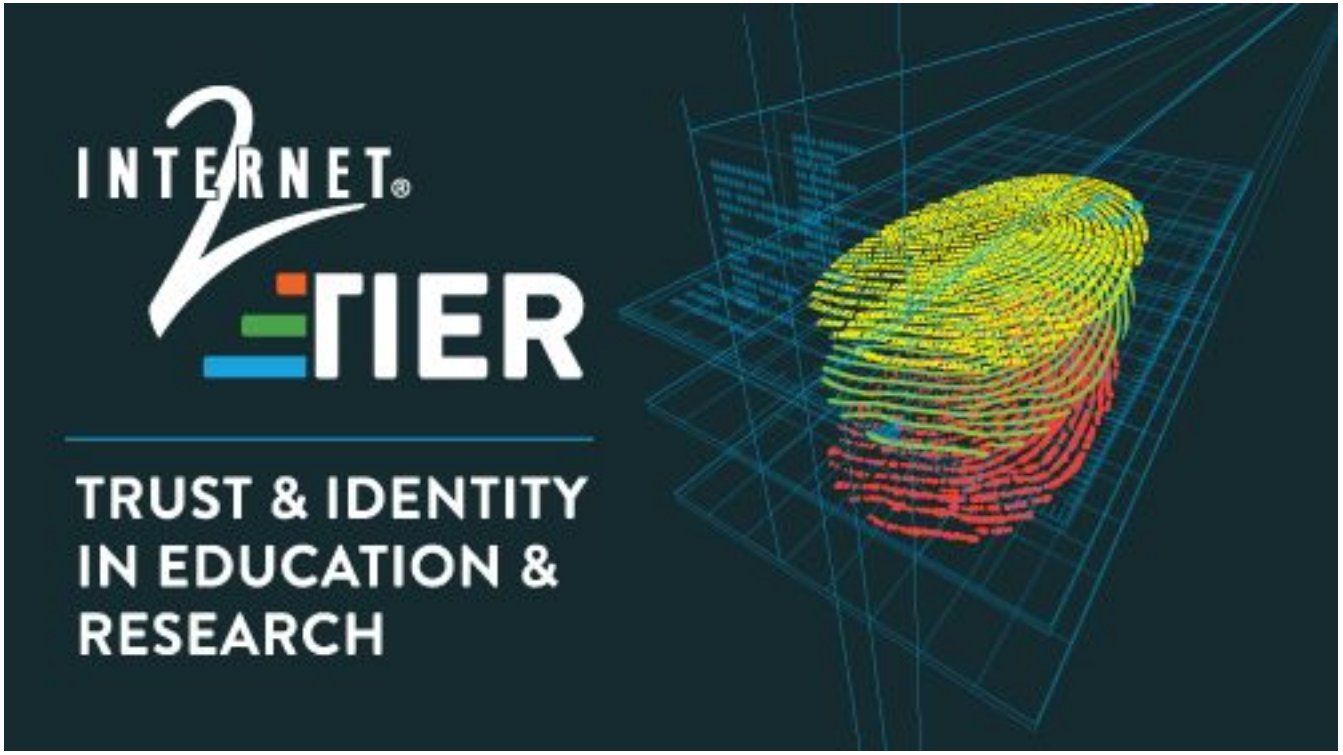


The Grouper Story

- Grouper v2.X expanded beyond groups
  - Roles & permissions

  - Rules

```
-  If
      removed from group A
-  then
       remove from group B
```

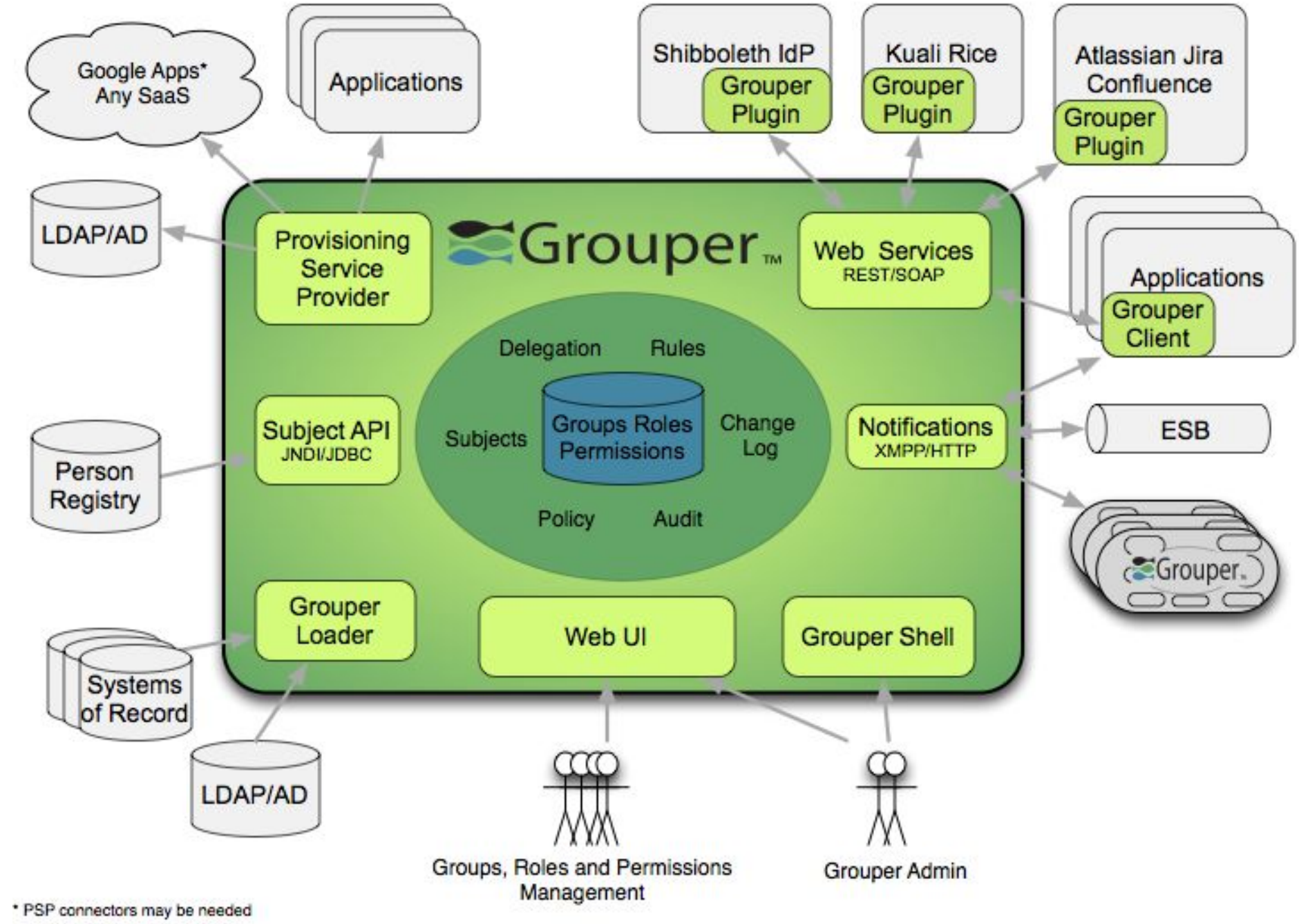


*"We view TIER as a **coordinated approach to enable trust and identity in education and research** at scale for thousands of institutions and service providers while also satisfying diverse local use cases."*

—Ron Kraemer, Vice President and CIDO, University of Notre Dame

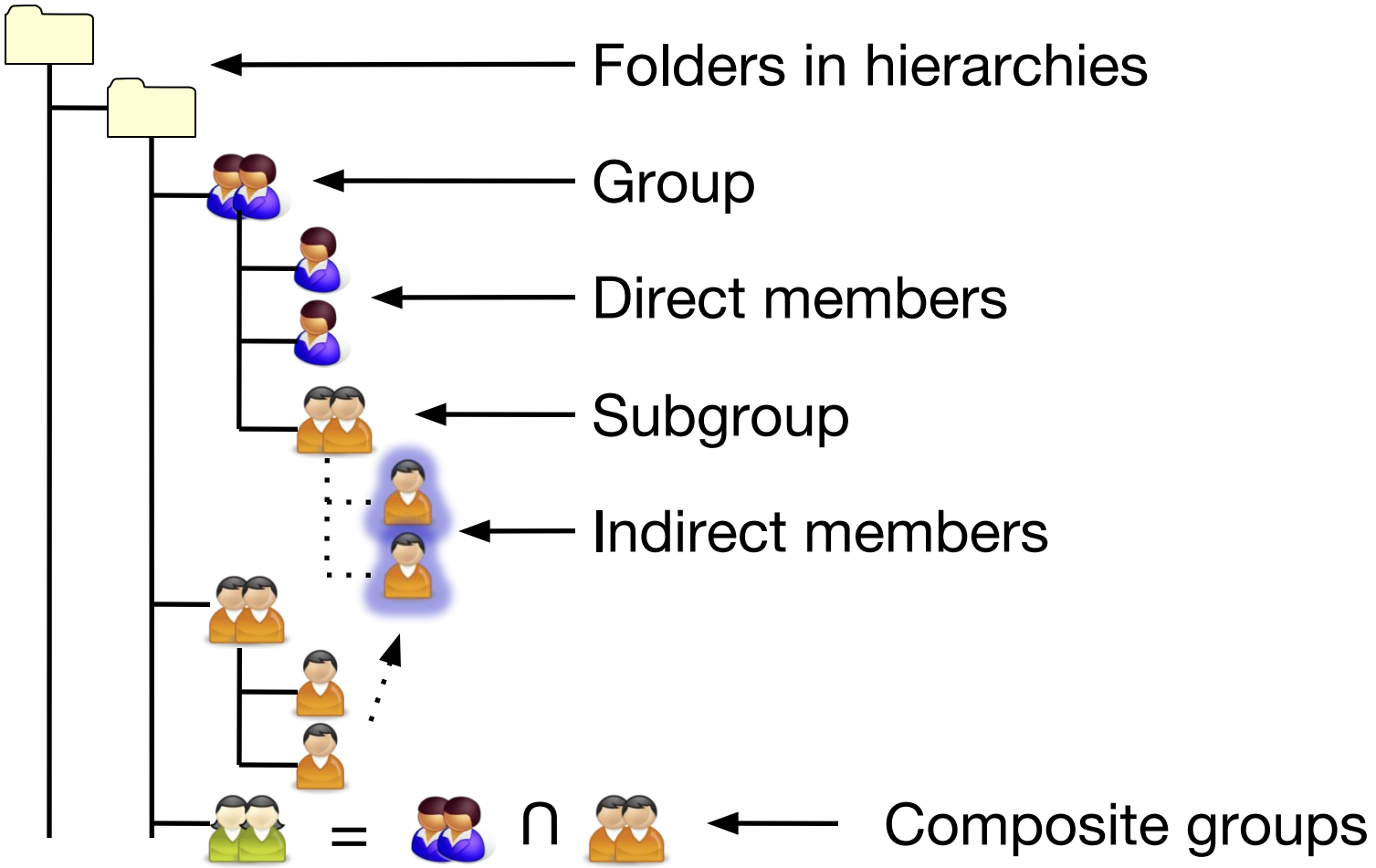
*"It's not just about federation, it's about **enabling high-value collaboration across thousands of disciplines and millions of people.** Hence agreement on attribute and authorization management, application integration, administration procedures,..."*

— RL 'Bob' Morgan

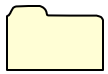


* PSP connectors may be needed

Grouper Concepts



Security and Delegation



- Create groups
- Create subfolders

- Admin
- Update membership
- Read membership
- View group
- Opt-in
- Opt-out

Delegation

Access management lifecycle support

- Membership start & end times (optional)
- Move or copy folders, groups, etc
- User audit
- Point in time audit
- Rules

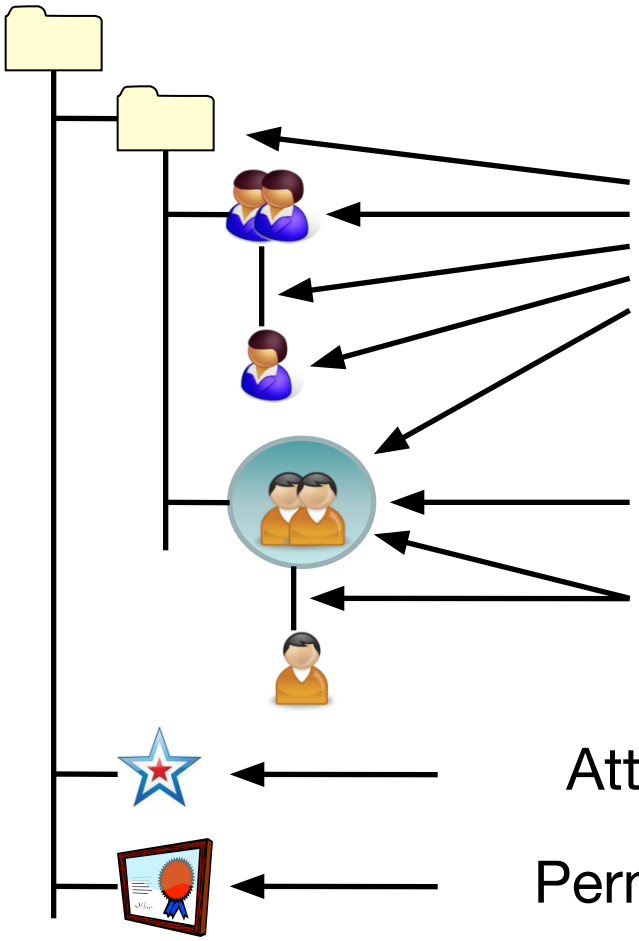
Auditing

- “User audit” will audit who does what
- Point-In-Time auditing will keep track of the history of the repository
  - Who was in this group at a point in time (or time range) in the past
  - Who are all the people who have been in this group
  - What groups was this person in at a point in the past (or time range)

Grouper loader

- Daemon that periodically syncs external sources with Grouper
- Can work for groups or permissions (e. g. org chart)
- SQL or LDAP sources
- Grouper admins can configure jobs based on attributes

Beyond groups...



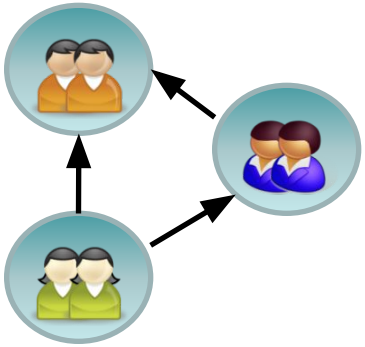
Attributes

Roles

Permissions

Attribute definition

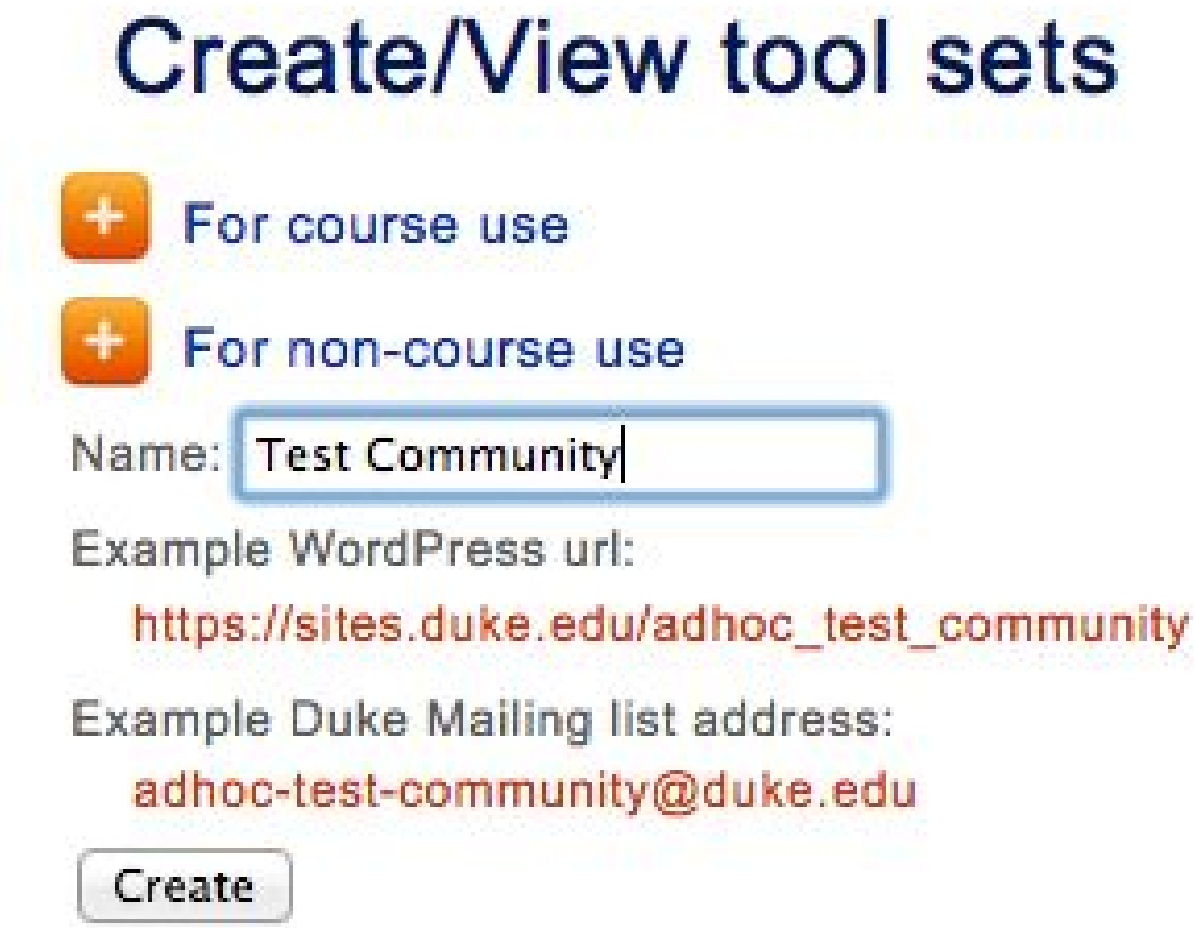
Permission definition



Role inheritance

Delegation model extends that for Groups

Ad-hoc Collaboration Communities
Creates various groups in Grouper



Ad hoc Community created - added shilen as a Community Manager

Tool Set for Test Community

Chat Room *A private Jabber chat room*	Add
Email Messaging *Email list using Sympa*	Add
Other *Placeholder to allow non-Toolkit resources to share activities*	Add
Quad *Quad is currently a Pilot project*	Add
Sakai *A learning management system*	Add
Virtual Computer Lab Access *VCL makes it possible to run lab software without visiting the lab in person*	Add

Groups and Roles for: Test Community

Use the links on this page to add or remove anyone with a Duke NetID from your course tool set. You can also add and remove guests with a Yahoo, Gmail or AOL email address. Once you add members to a group in Toolkits and set their roles, those members and their permissions are duplicated across all applications you open up to the community. Note that officially registered students, TAs, and instructors are automatically included in the appropriate groups and do not need to be added by hand.

Add Person with a Duke NetID Add a Guest Batch add users

All (1) Admin (1)

What do these roles mean?

Name	NetID	Role	Action
Shilen Patel	shilen	Admin	Edit

Group	Chat Room	Wiki	WebFiles Space	Email Messaging	WordPress Site	Sakai Site
Instructor	Owner	View, Modify, Comment, Admin	owner	List Owner	Admin: Can edit site appearance, manage users and privacy settings, and write posts and pages	Instructor
Manager/TA	Admin	View, Modify, Comment, Admin	Read/Write /Delete	subscriber	Admin	Instructor
Developer	Participant	View, Modify, Comment	Read/Write /Delete	subscriber	Editor: Can create, edit and publish pages and blog posts	Course Builder
Mentor	Participant	View, Modify, Comment	Read/Write	subscriber	Editor	Teaching Assistant
Student	Participant	View, Modify, Comment	Read/Write	subscriber	Author: Can create and publish posts, but not access or edit pages	Student
Visitor/Auditor	Participant	View	Read	subscriber	Subscriber: Can access a private blog and write comments	Visitor

Open Apereo 2016

100% Open for Education

Grouper - What's new?

Release 2.3.0 new features

- Grouper Loader improvements including scheduling configuration to facilitate high-availability changes and, handling unresolvable subjects
- New Web Service operations for attribute definitions, actions, and messaging

Release 2.3.0 new features (continued)

- Grouper messaging system with integration to the change log and ESB
- UI screens for attribute definitions and inherited privileges
- Export to GSH - allows export of Grouper objects to a Grouper Shell (GSH) script
- Folder privileges have been changed to be "admin" and "create" instead of "stem" and "create)
- TIER API "hasMember" operation implemented in the Grouper web services module to support integration and interoperability. Well, this is already out of date

Release 2.3.0 - provisioning

- Provisioning Service Provider Next Generation (PSPNG)
  - Simplify configuration
  - Increase performance
- 2.3.0 Provisioning targets
  - LDAP groups
  - Active Directory groups
  - LDAP attributes (entitlements)
- Other features:
  - Incremental and full refresh
  - Group selection: by folder or group, or both
  - Higher-level and higher-performance programming API

Grouper roadmap

- TIER packaging (continued)
- Revise building and package management (continued)
- UI
  - incorporate more rules
  - wizards for configuration
  - support attributes / permissions / etc
- PSPNG refinements
- Upgrade vt-ldap to ldaptive
- Improve GSH
- TIER SCIM API
- Grouper instrumentation

Provisioning opportunities (post 2.3.0)

- Grouper messaging
- Automated integration tests
- Deprovisioning safety nets
- More targets: suggestions?

Grouper roadmap schedule

- Grouper 2.4 in Q1 2017
- This release is time based, not feature based, so not exactly sure what will be in it, will know more at TechEx
- We will be spending time supporting 2.3 in the near term and then focusing on 2.4
- We would like to do yearly major releases in the spring
- Minor releases we are not sure
  - If they don't take a lot of time maybe quarterly
  - Maybe snapshot releases that include patches?
- Patches as needed

Upcoming event

IAM online

- IAM Webinar Wed. July 13 2016 at 2pm ET (Grouper stories)

Open Apereo 2016

100% Open for Education

Grouper - Access Policy and Reference Groups @ Lafayette College

Open Apereo 2016

100% Open for Education

Grouper - Grouper, Sakai, and Google @ NYU

Open Apereo 2016

100% Open for Education

Grouper - Organizational hierarchy in Grouper at Penn

Grouper @ Penn

- Used Grouper centrally at Penn
- 120k groups
- 2.7 million immediate memberships
- 10k permission assignments
- Heavily delegated

Organizational hierarchy at Penn

- Penn uses a loader job to sync organizational chart
- SQL warehouse has:
  - Orgs with people
  - Org rollups
- Loader job to load the orgs with people
- Loader job to load the rollups
- Includes / excludes
- Wiki document

Example org

Org loader configuration

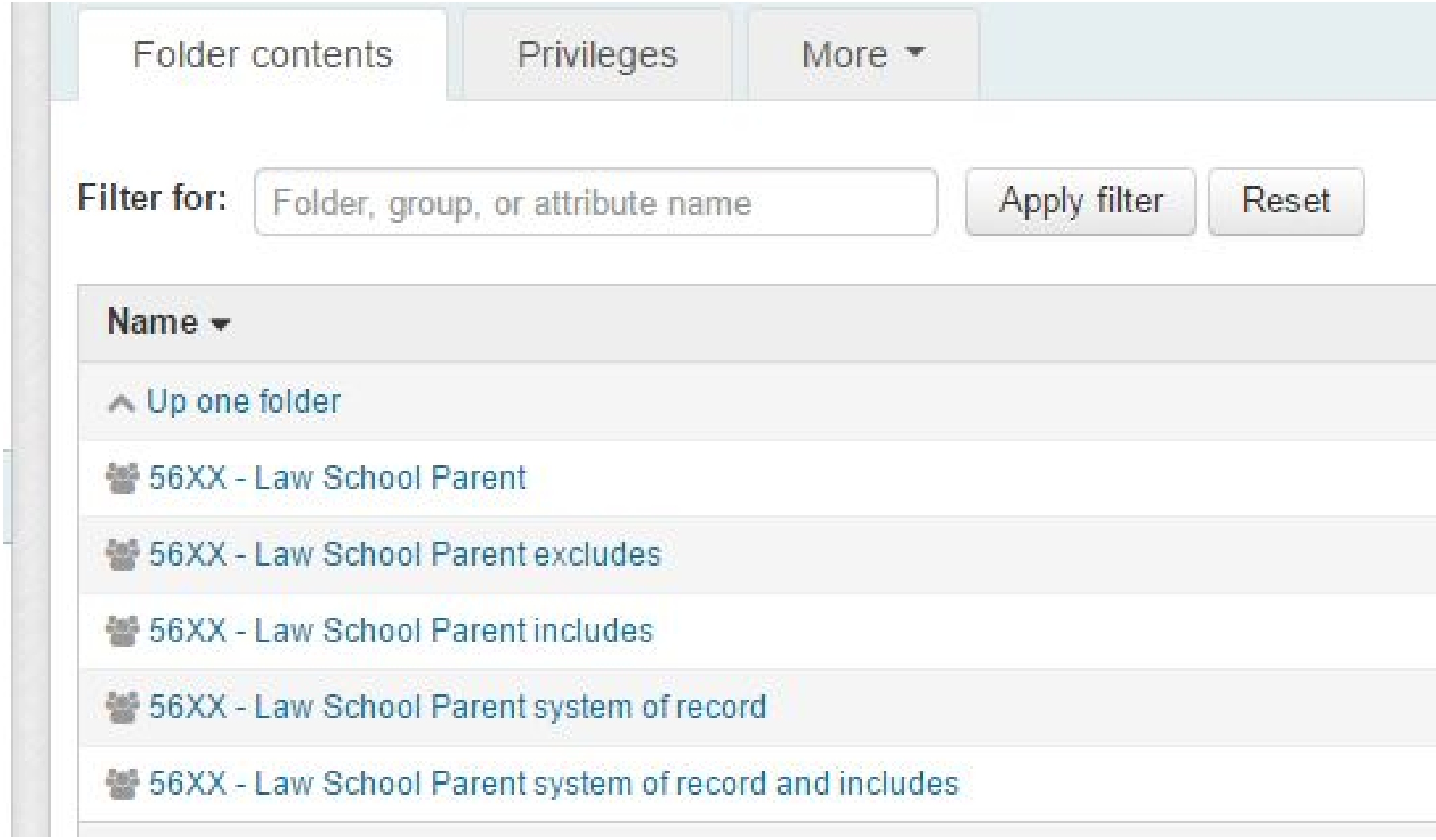
Types			
	grouperLoader	grouperLoaderAndGroups	
		grouperLoaderDbName	grouper
		grouperLoaderGroupQuery	select olpmv.GROUP_NAME as group_name, olpmv.GROUP_DISPLAY_NAME as group_display_name, olpmv.READERS, olpmv.VIEWERS, olpmv.ORG_ID from ORG_LOADER_PERSON_META_V olpmv
		grouperLoaderGroupTypes	
		grouperLoaderGroupsLike	penn:community:employee:org:%_personorg
		grouperLoaderIntervalSeconds	
		grouperLoaderPriority	
		grouperLoaderQuartzCron	0 46 6 * * ?
		grouperLoaderQuery	select group_name, subject_id from org_loader_person_v
		grouperLoaderScheduleType	CRON
		grouperLoaderType	SQL_GROUP_LIST
	base	members	*List field*

Old org structure in org name

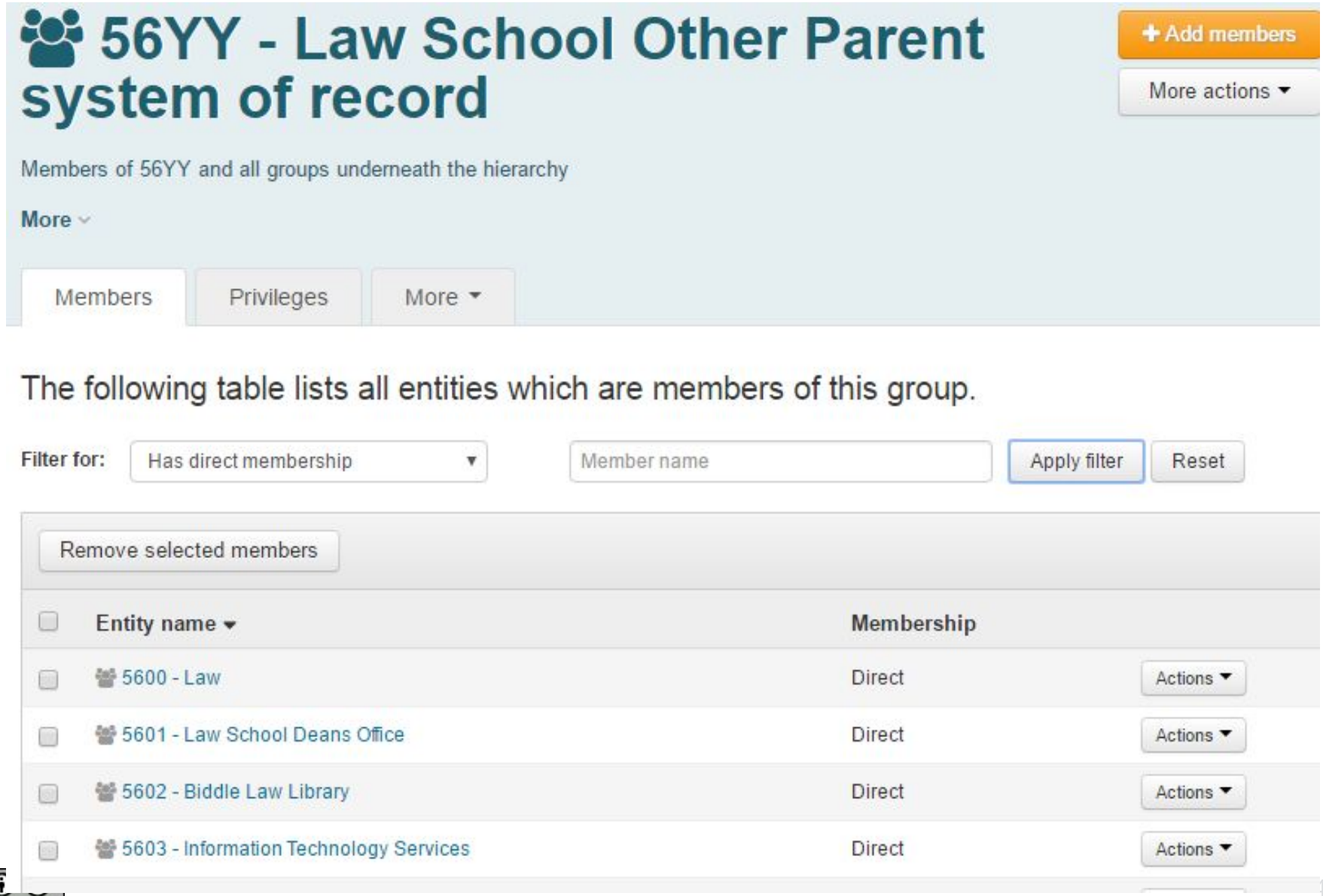
penn:community:employee:org:TOPU:UNIV:UCAC:UUAC:
USCH:56XX:56YY:5600

When we had a re-org and apps broke we changed this

Orgs as groups



Org rollup structure



Using organizational hierarchy in apps

- Create an app group
- Add the organizational group(s) to app group
- App group could be include/exclude or all other additions

O365 needs the organization for billing

- O365 needs the sponsoring organization / division
- Person could be in more than one organization
- Use the primary org code
- Allow an org override
- Do not allow multiple overrides
- Admins have access to read/write various orgs or rollups

O365 overrides original solution

- Admins would use Grouper UI to manage override group
- Create if not exist
- Have READ/UPDATE privileges on org override groups or by group to rollup
- Problems
  - Users might not have correct access
  - Steps to use the Grouper UI to inspect/assign orgs
  - Don’t know if there is another org assigned
  - Daily process to pick up changes

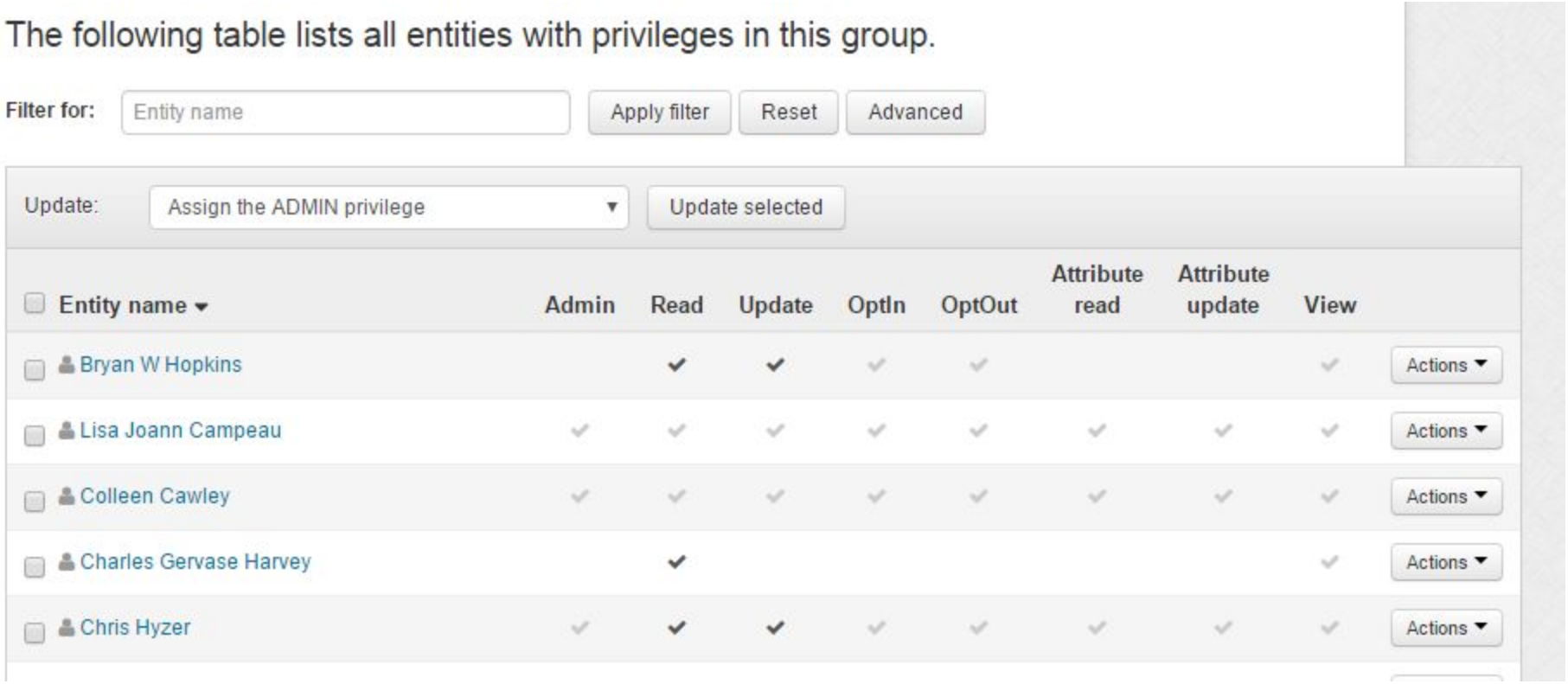
O365 overrides final solution

- Application using the Grouper WS to manage better
- Shows the overrides in a table for orgs/divs
- Tells the user there are multiple overrides for a user without showing data they are not allowed to see
- Kicks off process to provision user to FIM
- Allows assignments to org rollups for easier management
- Leverages Grouper groups/privileges

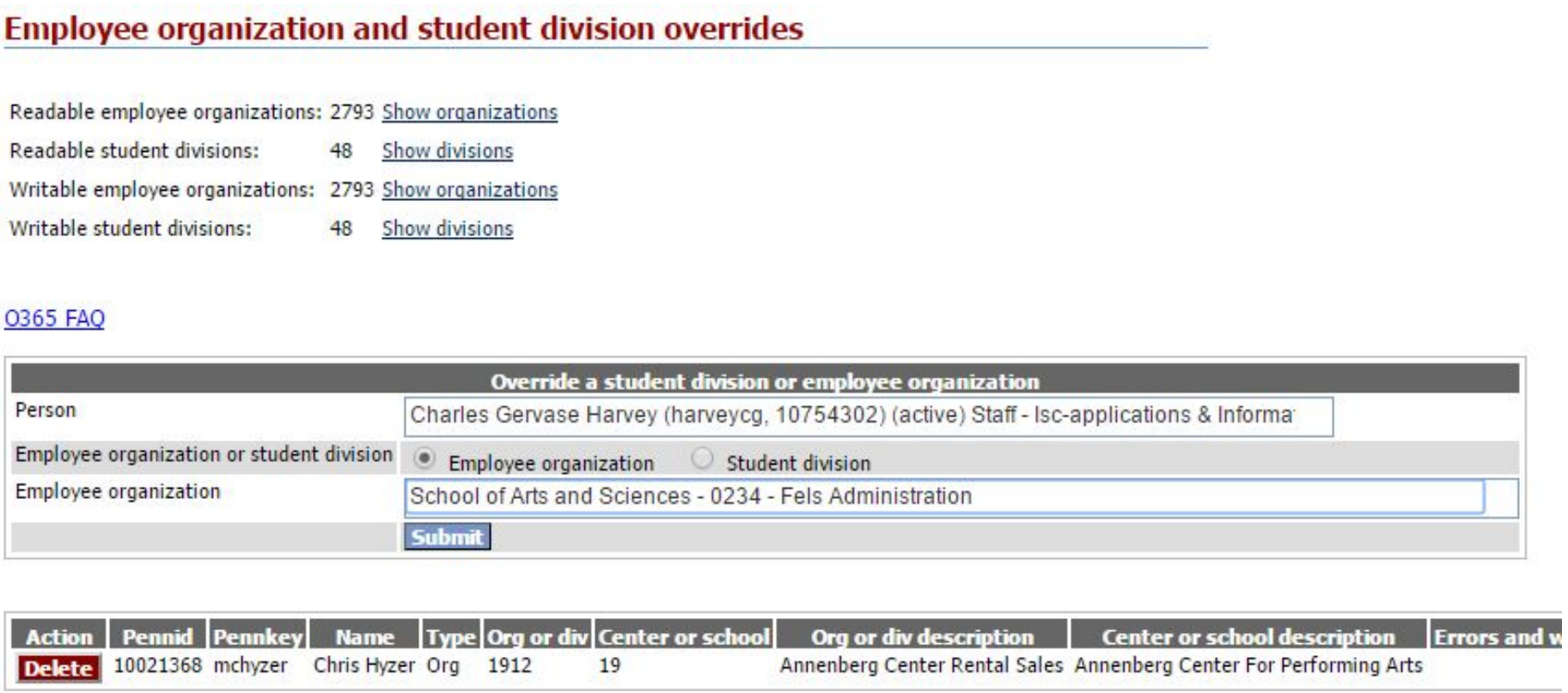
O365 overrides final solution

- Application using the Grouper WS to manage better
- Shows the overrides in a table for orgs/divs
- Tells the user there are multiple overrides for a user without showing data they are not allowed to see
- Kicks off process to provision user to FIM
- Allows assignments to org rollups for easier management
- Leverages Grouper groups/privileges

O365 privileges on org in Grouper (test env)



Manage org overrides screen



Employee organization and student division overrides

Readable employee organizations: 2793 Show organizations
Readable student divisions: 48 Show divisions
Writable employee organizations: 2793 Show organizations
Writable student divisions: 48 Show divisions

O365 FAQ

Override a student division or employee organization

Person	Charles Gervase Harvey (harveycg, 10754302) (active) Staff - Isc-applications & Informa
Employee organization or student division	(•) Employee organization ( ) Student division
Employee organization	School of Arts and Sciences - 0234 - Fels Administration
	Submit

Action	Pennid	Pennkey	Name	Type	Org or div	Center or school	Org or div description	Center or school description	Errors and v
Delete	10021368	mchyzer	Chris Hyzer	Org	1912	19	Annenberg Center Rental Sales	Annenberg Center For Performing Arts	

Manage org overrides screen logic

- Global context cache of objects (few minutes)
- When user logs in, look in membership cache to get memberships and privileges
- Expand privileges to be indirect by org
- Of the memberships in overrides, filter the ones the user can READ
- In drop down for orgs/divs, only show results that the user can UPDATE
- Make sure everything ok and give error message to right of result

Open Apereo 2016

100% Open for Education

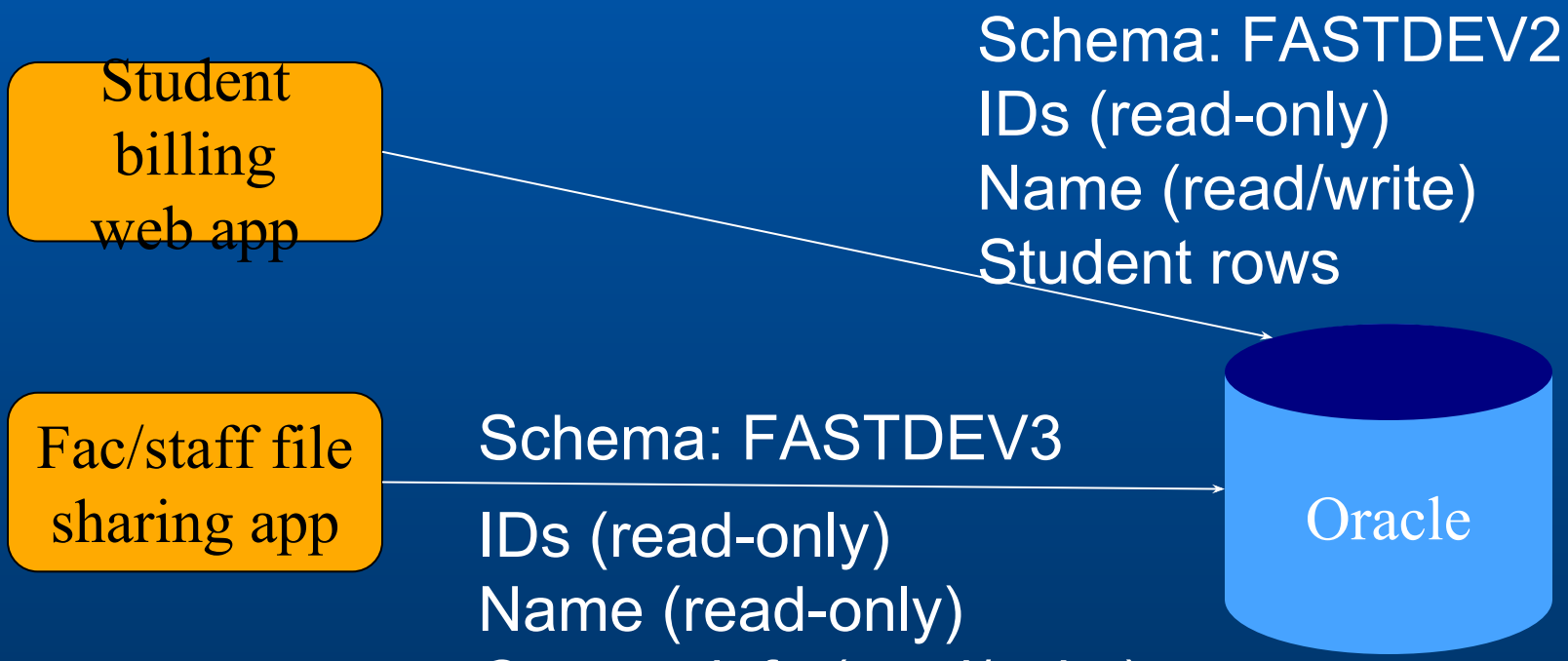
Grouper - Fine grained database permissions

Use case description

- Personal user data stored in SQL DB
- Applications across the University need to access the data
- Principle of least privilege at a row and column level
- User information (test data set):
  - PersonID
  - NetID
  - First and last name
  - Email address
  - Phone numbers
- SQL access will take place with different schemas per application

Use case description (continued)

- Only need read-only access managed, but for this example, let's manage READ/WRITE



Sample data

ID	PersonID	NetID	First	Last	Email	Work#	Home#
A3	12345	js	John	Smith	js@a.edu	3-1234	123-4567
B4	98765	sd	Sara	Davis	sd@a.edu	5-2345	234-5678
C5	54321	rj	Ryan	Jones	rj@a.edu	7-4567	345-6789
T7	56789	jc	Julia	Clark	jc@a.edu	9-6789	456-7890

ID	PersonID	NetID	First	Last	Email	Work#	Home#
A3	12345	js	John	Smith	js@a.edu	3-1234	123-4567
B4	98765	sd	Sara	Davis	sd@a.edu	5-2345	234-5678
C5	54321	rj	Ryan	Jones	rj@a.edu	7-4567	345-6789
T7	56789	jc	Julia	Clark	jc@a.edu	9-6789	456-7890

Browse groups hierarchy

You can look for groups throughout the hierarchy.
(You might not be able to see some groups if you lack appropriate privil

Browse or list groups

Current location is:

Root: fgac: apps: secureUserData: **schemas**

Showing 1-2 of 2 items

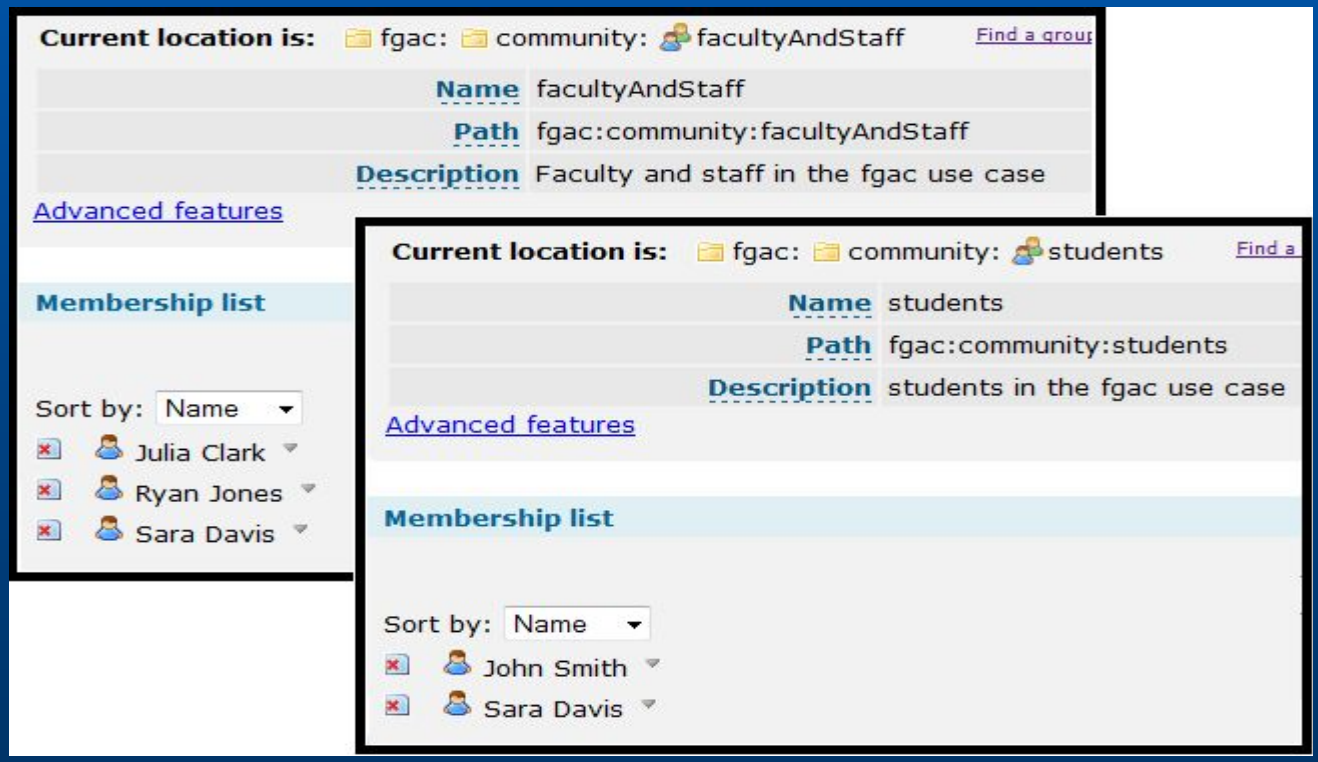
FASTDEV2
FASTDEV3

Architecture

- One table in Oracle with personal user information
- Secure the table with Oracle FGAC (Fine grained access control) / VPD (Virtual private database)
- Security data needs to be replicated from Grouper to Oracle for performance reasons
- Store memberships for rows and permissions for schemas in Grouper
- Access request workflow with Kuali Rice edoclite / Grouper
- Note: a schema in Oracle is the connecting DB user

Setup on Grouper demo server: affiliations

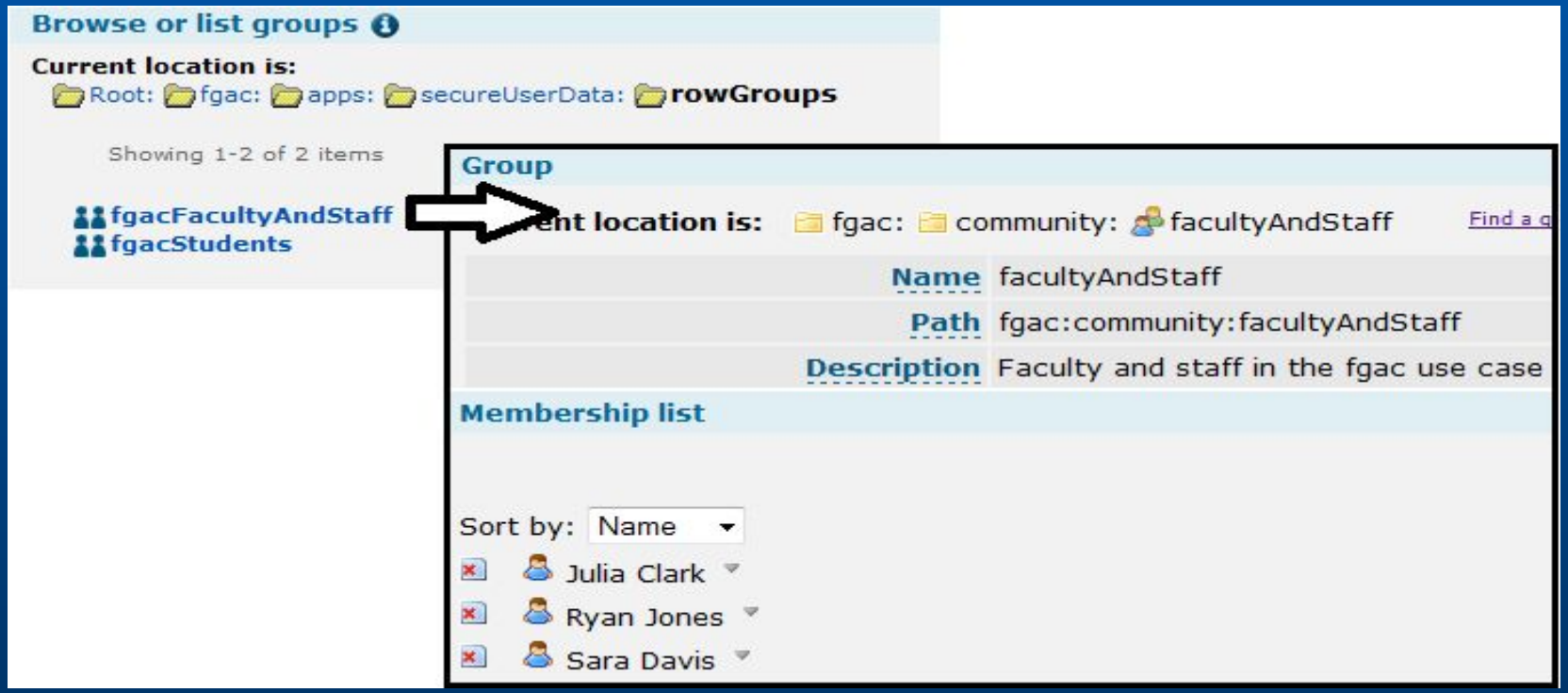
- Normally these would be available in Grouper as loader jobs
- They are not on the Grouper demo server, so add



*

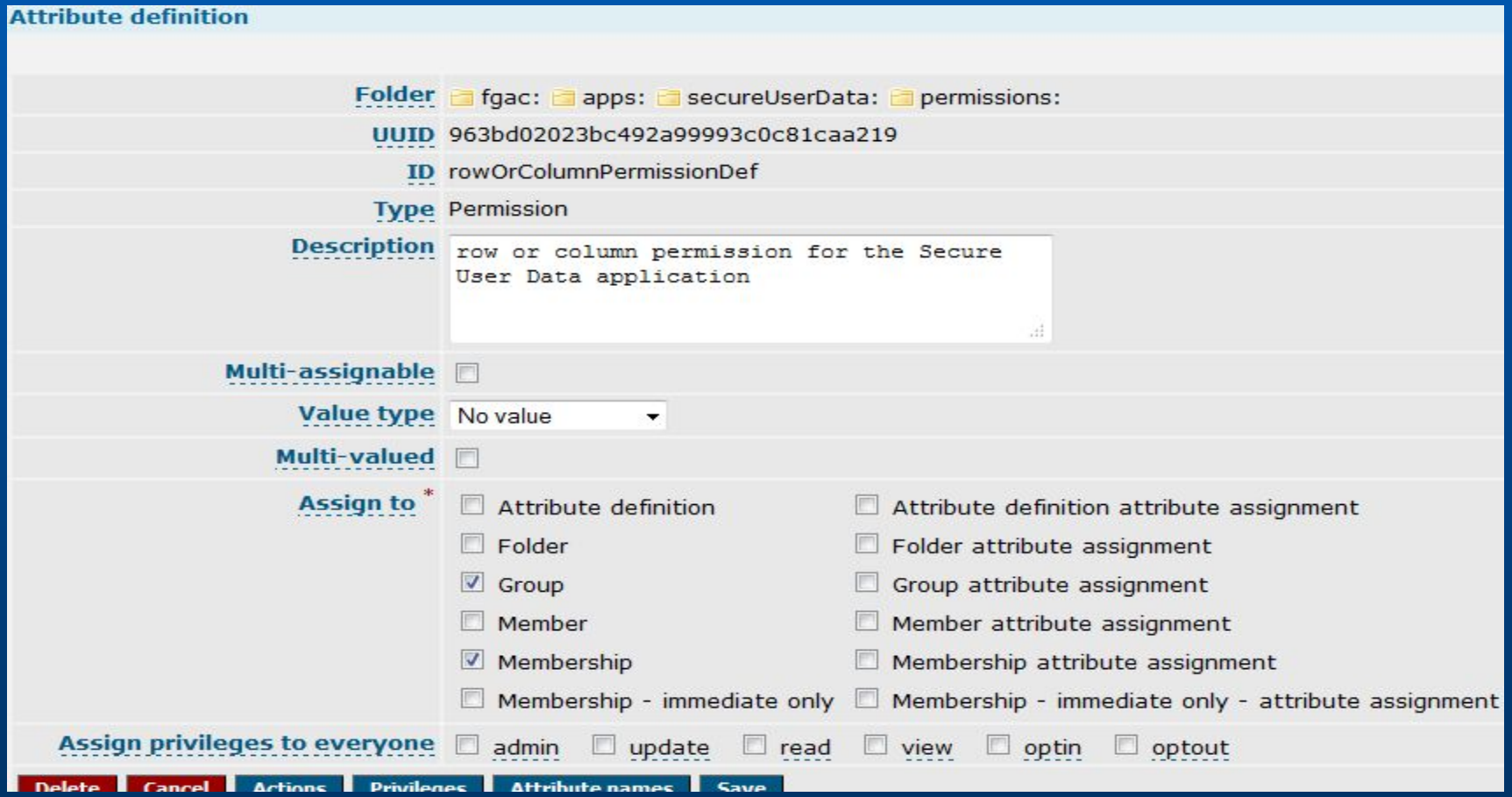
Setup: row level groups

- Create the application folder, and organize subfolders
- Add the community groups as members

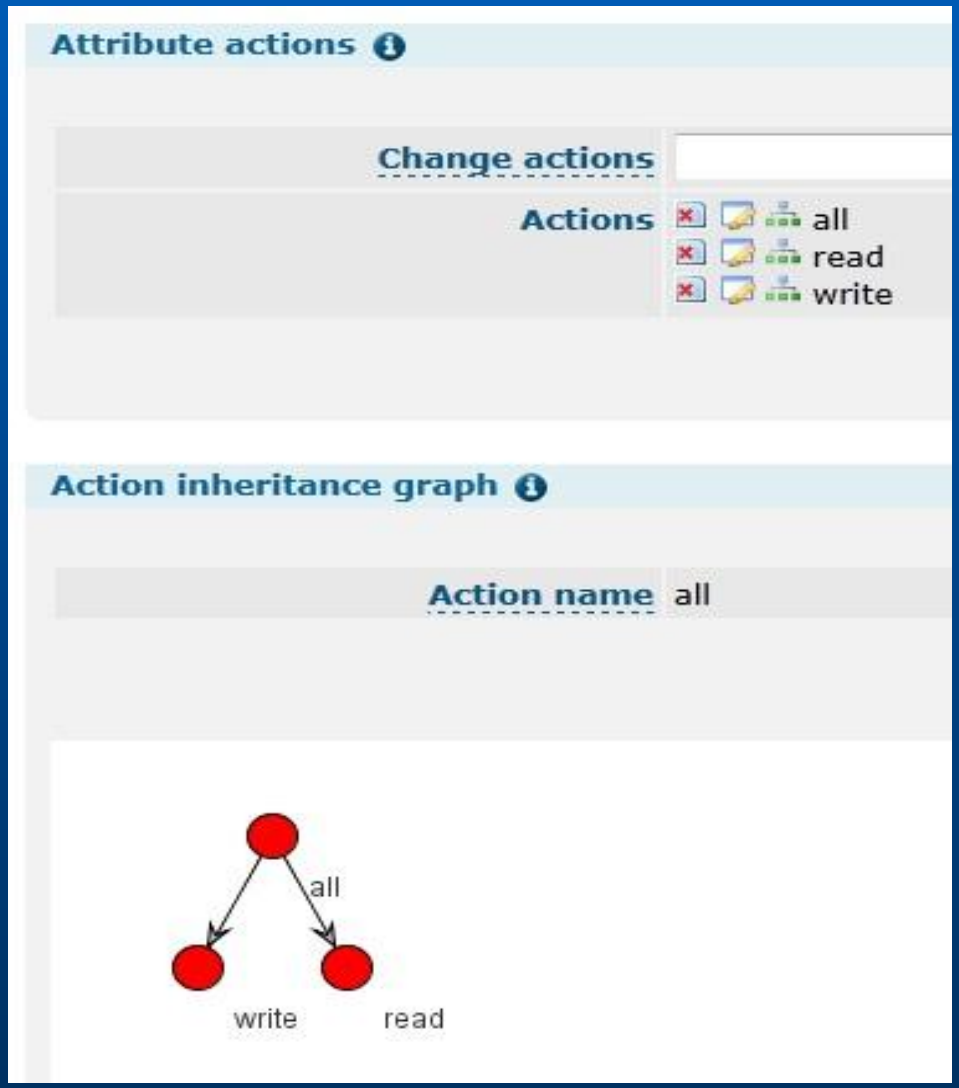


Setup: row/column level permission definition

- Permission definition has configuration and security

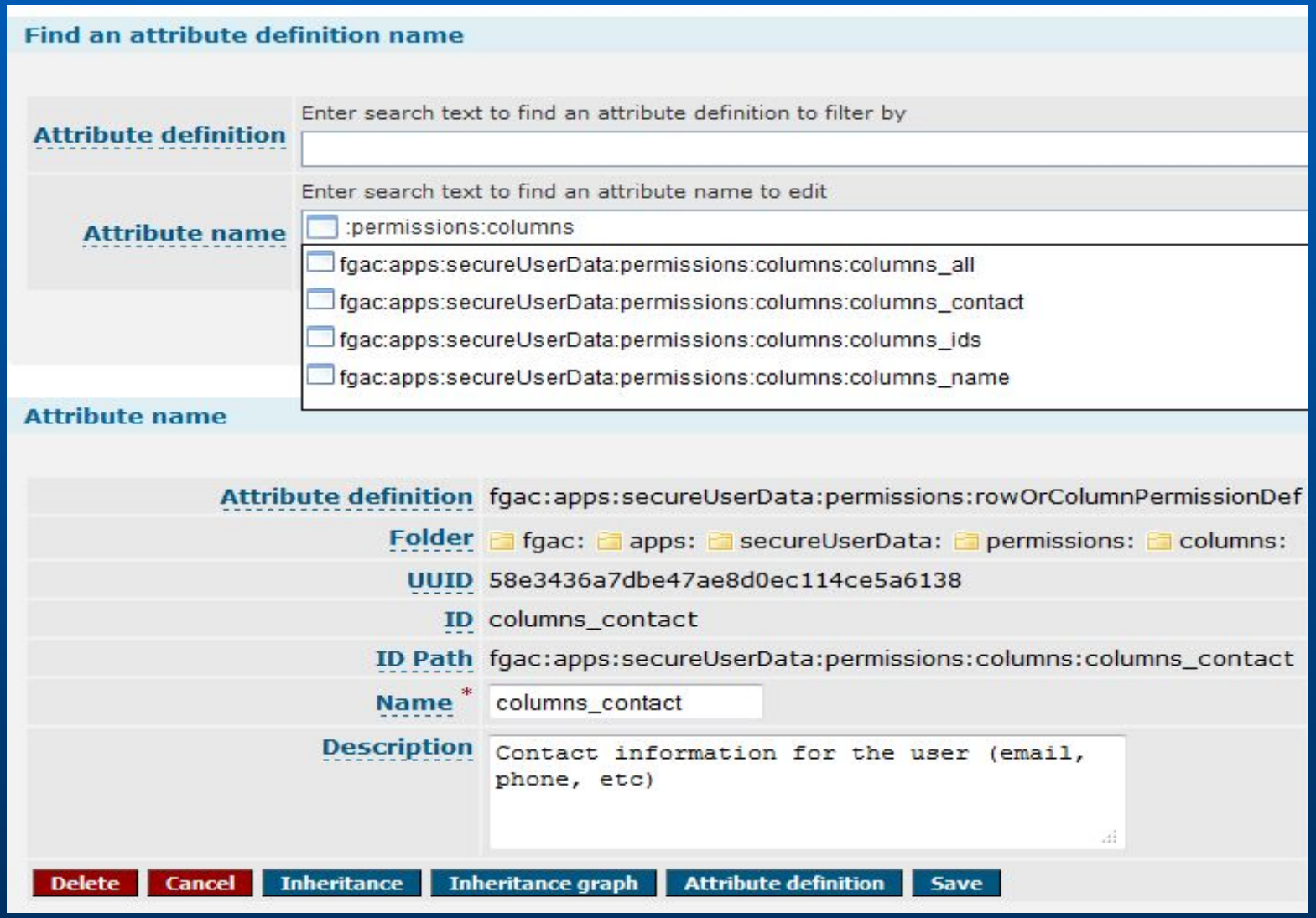


Setup read/write action for this permission def

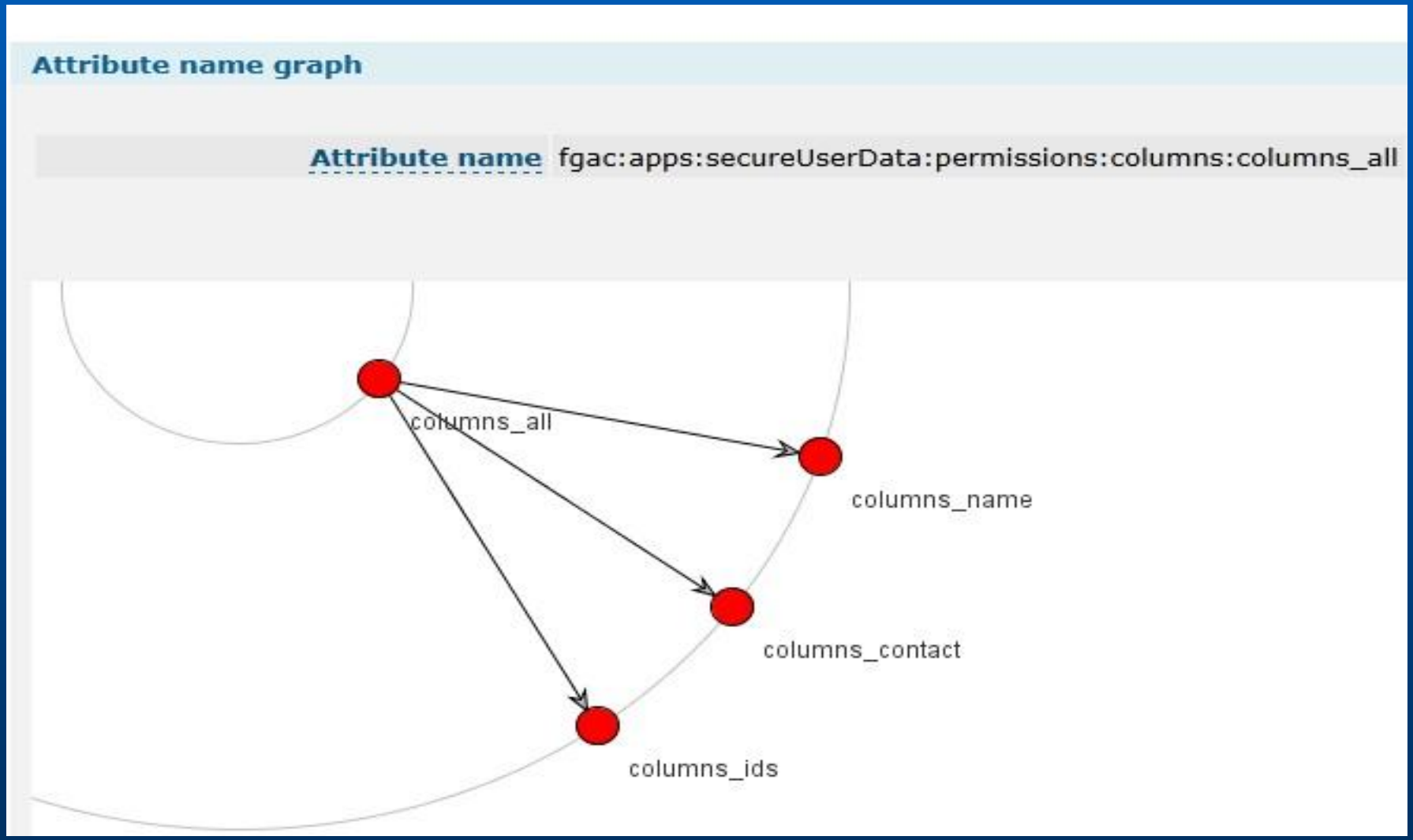


- Include an “all” which implies read and write
- Note: this is specific to this one permission definition, and does not affect other permissions in Grouper

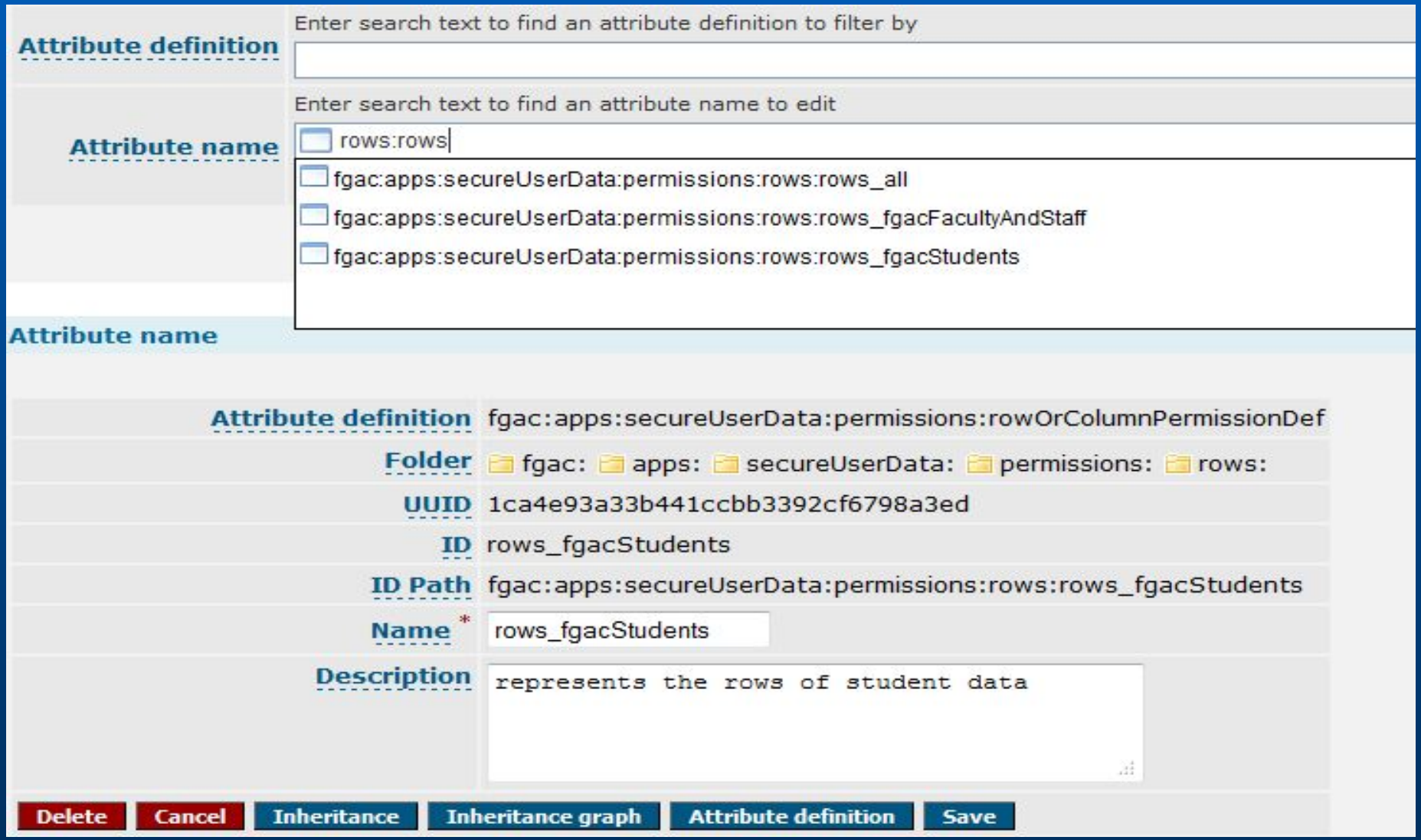
Setup permission name for each set of columns



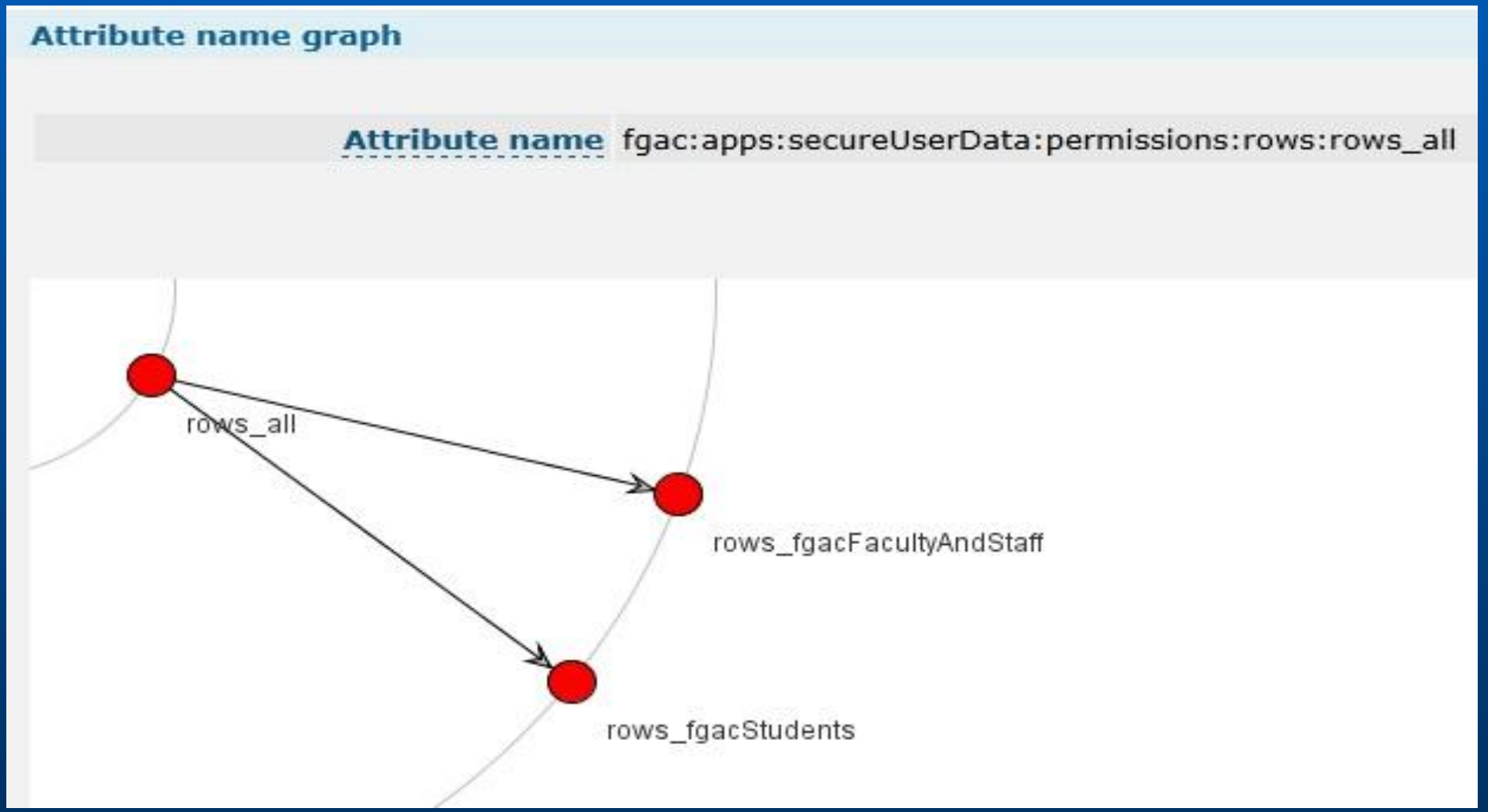
Setup column permission name inheritance



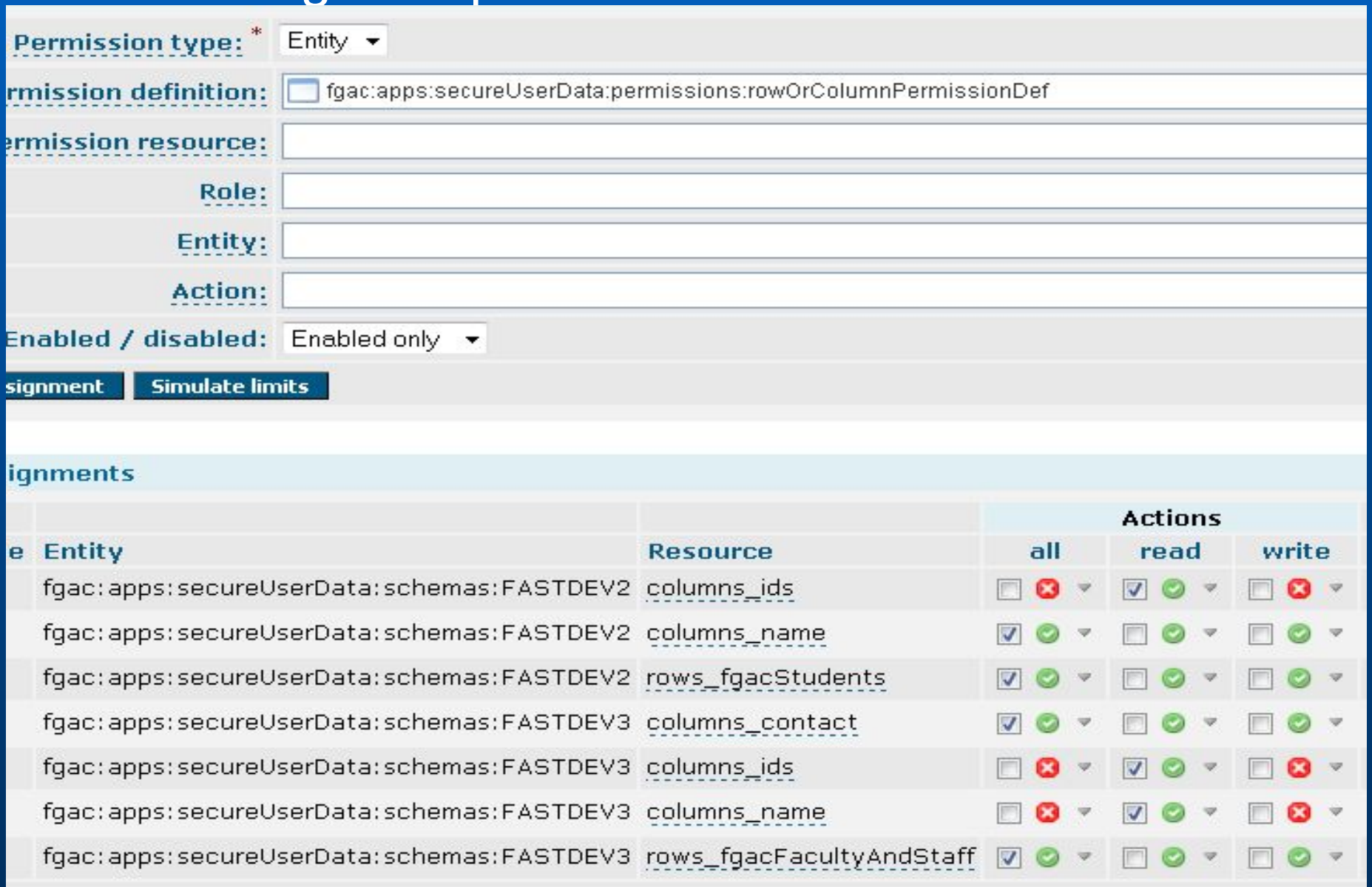
Setup permission name for each group of rows



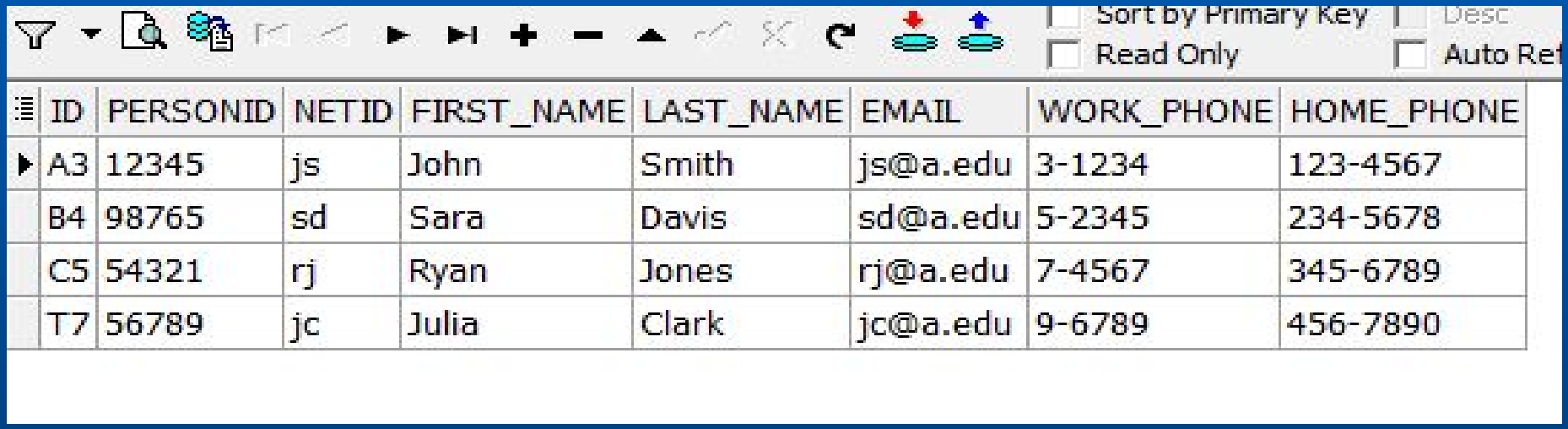
Setup row permission name inheritance



Assign the permissions



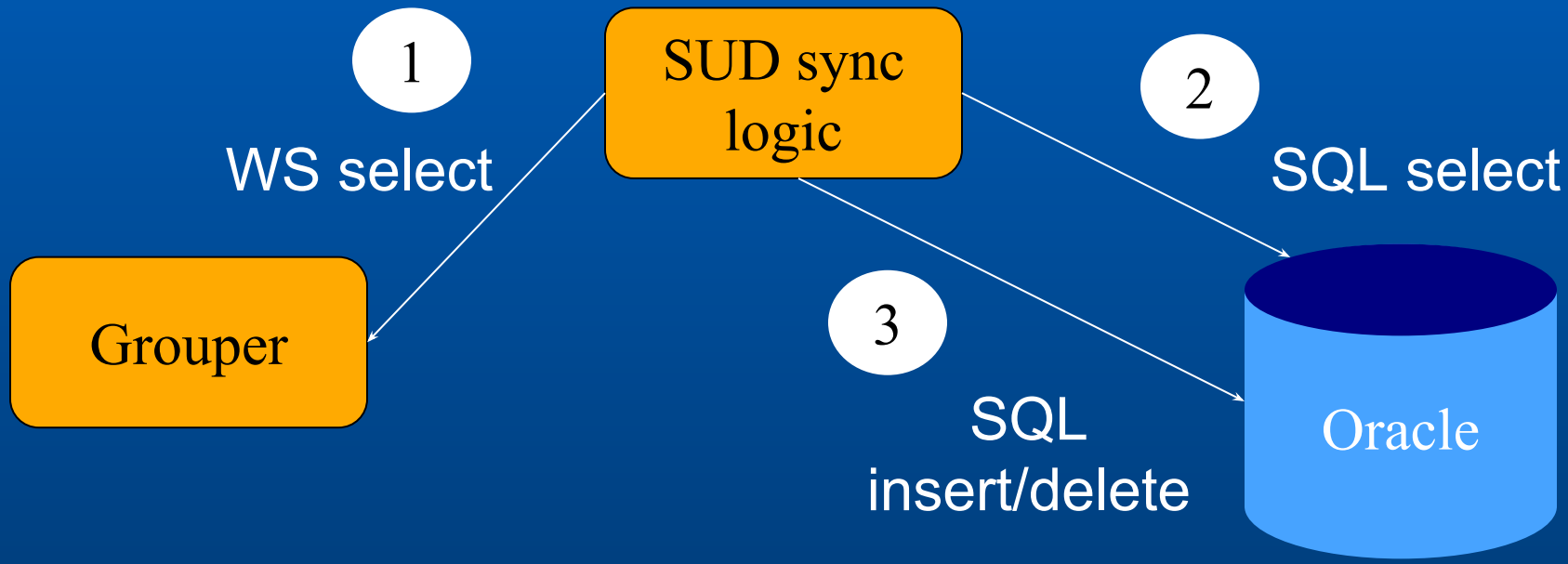
Setup: insert sample data
Table: SECUREUSERDATA_USER



ID	PERSONID	NETID	FIRST_NAME	LAST_NAME	EMAIL	WORK_PHONE	HOME_PHONE
A3	12345	js	John	Smith	js@a.edu	3-1234	123-4567
B4	98765	sd	Sara	Davis	sd@a.edu	5-2345	234-5678
C5	54321	rj	Ryan	Jones	rj@a.edu	7-4567	345-6789
T7	56789	jc	Julia	Clark	jc@a.edu	9-6789	456-7890

Setup: groups without members represent schemas

Full sync Grouper to Oracle security tables



Run the full sync Java program

- Code in SVN:

  http://anonsvn.internet2.edu/svn/i2mi/trunk/grouper-misc/poc_secureUserData/

```
C:\mchyzer\grouper\trunk\poc_secureUserData>java -cp conf;lib\grouperClient.jar;
lib\log4j.jar;lib\ojdbc14.jar;dist\secureUserData.jar edu.internet2.middleware.p
oc_secureUserData.SudFullSync
 - Del 1 mships of group: fgacAlumni
 - Del 1 mships of group: fgacStudents, personid: 98766
 - Add mship for group: fgacStudents, personid: 12345
 - Add mship for group: fgacStudents, personid: 98765
 - Del 1 row permiss schema: FASTDEV2, action: read, group: fgacAlumni
 - Del 1 row permiss schema: FASTDEV4, action: write, group: fgacStudents
 - Del 1 col permiss schema: FASTDEV4, action: read, cols: name
 - Del 1 col permiss schema: FASTDEV2, action: read, cols: ssn
 - Add row permiss schema: FASTDEV2, action: write, group: fgacStudents
 - Add row permiss schema: FASTDEV2, action: read, group: fgacStudents
 - Add col permiss schema: FASTDEV3, action: read, cols: name
 - Add col permiss schema: FASTDEV2, action: read, cols: ids
 - Add col permiss schema: FASTDEV3, action: read, cols: contact

C:\mchyzer\grouper\trunk\poc_secureUserData>_
```

Local cache of security tables and memberships

- SECUREUSERDATA_MEMBERSHIPS

ID	PERSONID	GROUP_EXTENSION
Q2SI0S23	56789	fgacFacultyAndStaff
Q2SI8046	54321	fgacFacultyAndStaff
Q2SJGOZ2	98765	fgacStudents
Q2SJGOZ1	12345	fgacStudents
Q2SI3U8P	98765	fgacFacultyAndStaff

- SECUREUSERDATA_ROW_PERMISS

ID	GROUP_EXTENSION	SCHEMA_NAME	ACTION
Q2SI805A	fgacFacultyAndStaff	FASTDEV3	read
Q2SI8049	fgacFacultyAndStaff	FASTDEV3	write
Q2SJGOZ4	fgacStudents	FASTDEV2	read
Q2SJGOZ3	fgacStudents	FASTDEV2	write

- SECUREUSERDATA_COL_PERMISS

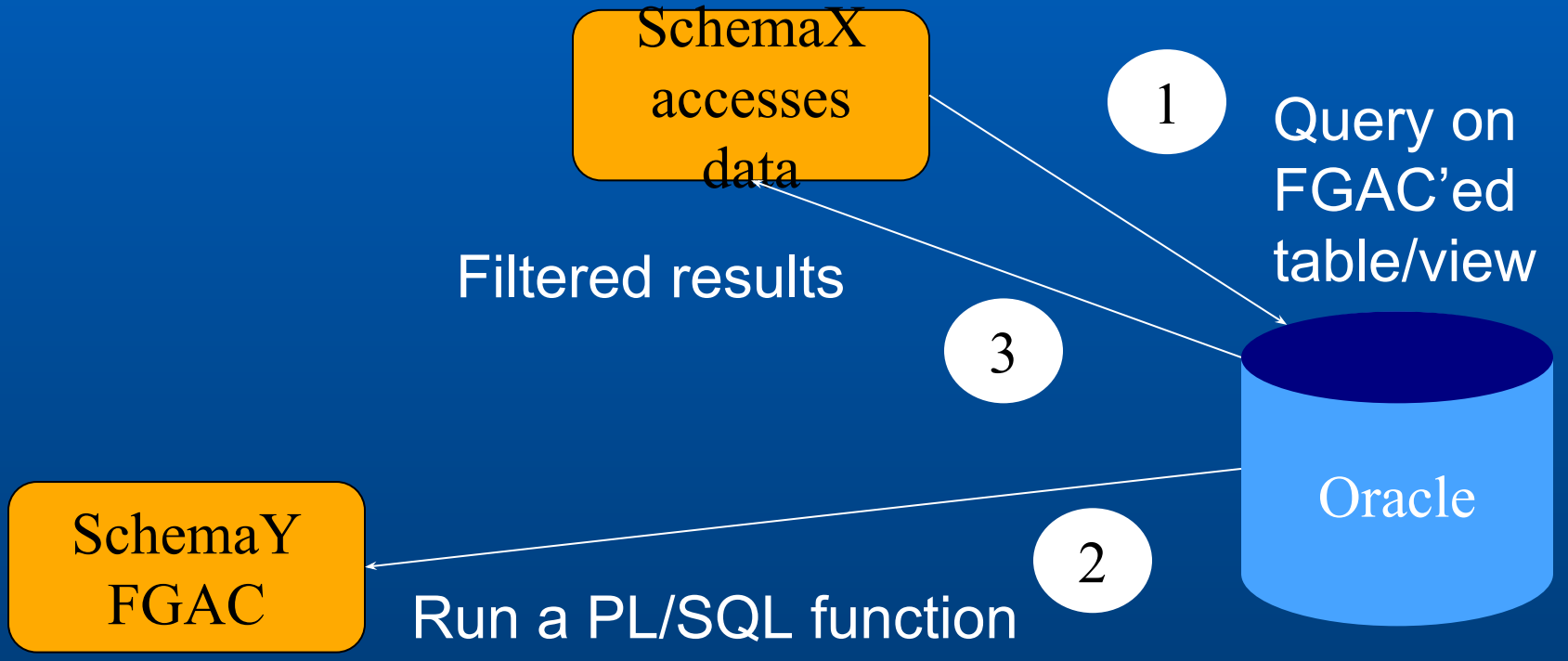
ID	COLSET	SCHEMA_NAME	ACTION
Q2SI805C	name	FASTDEV2	read
Q2SJGOZ7	contact	FASTDEV3	read
Q2SJD6B1	name	FASTDEV2	write
Q2SJD6B2	contact	FASTDEV3	write
Q2SJGOZ5	name	FASTDEV3	read
Q2SJGOZ6	ids	FASTDEV2	read
Q2R69VNA	ids	FASTDEV3	read

*

Oracle FGAC/VPD/RLS

- Oracle Fine Grained Access Control (FGAC) aka: Virtual Private Database (VPD)
  - A way to apply a virtual (hidden to the user) “where clause” to limit rows (Row Level Security (RLS))
  - A way to null-out columns in a way that is hidden to the user
  - Based on schema, or if trusted schema, data in the context
- Note: this part does not have to be FGAC, you could use a view with functions, or something else…
  - With Oracle, FGAC is supposed to perform better than a view with functions

Application schemas accessing FGAC'ed data



Oracle FGAC (continued)

- For performance, cache security in the connection context (similar to ThreadLocal)
  - Only cache for a certain amount of time (5 minutes?)
  - Can cache on connect trigger, or on demand
    - “on demand” might be better if users connect to the DB for things unrelated to the FGAC
  - Cache who the user is, when cache was created, if can read/write all rows, which column sets can read/write

Oracle FGAC queries from owner schema: all data

- Note: there is a short circuit, if owner schema, allow access

```
select * from FASTDEV1.SECUREUSERDATA_USER
```

Data Grid

Messages | Data Grid | Auto Trace | DBMS Output (disabled) | Query Viewer | Expl

ID	PERSONID	NETID	FIRST_NAME	LAST_NAME	EMAIL	WORK_PHONE	HOME_PHONE
A3	12345	js	John	Smith	js@a.edu	3-1234	123-4567
B4	98765	sd	Sara	Davis	sd@a.edu	5-2345	234-5678
C5	54321	rj	Ryan	Jones	rj@a.edu	7-4567	345-6789
T7	56789	jc	Julia	Clark	jc@a.edu	9-6789	456-7890

Oracle FGAC queries from student billing application: sees students and no contact info

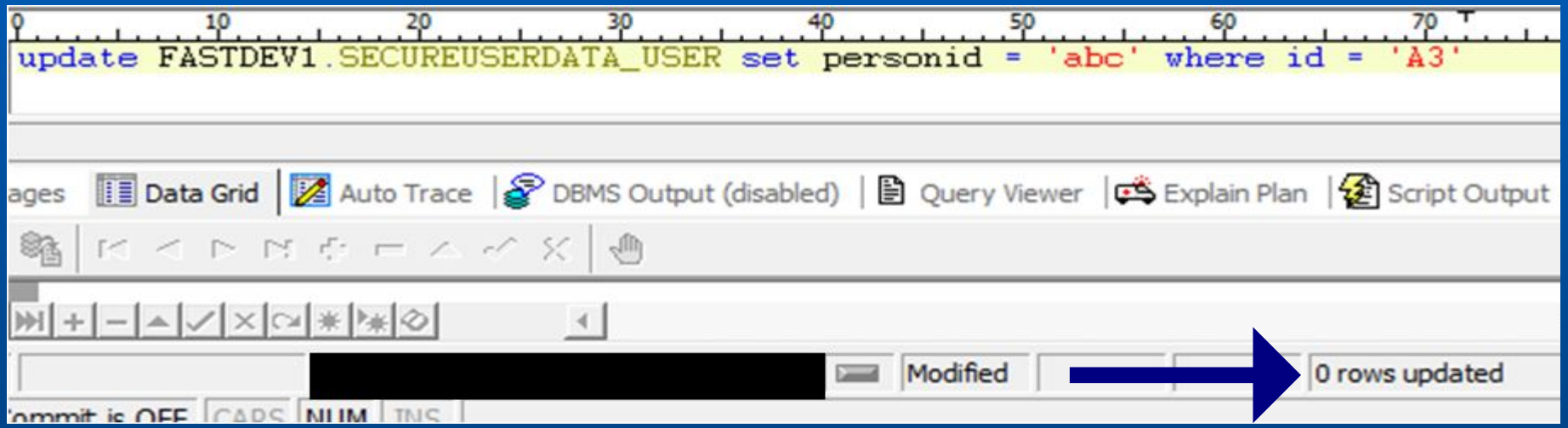
```
1  select * from FASTDEV1.SECUREUSERDATA_USER
```

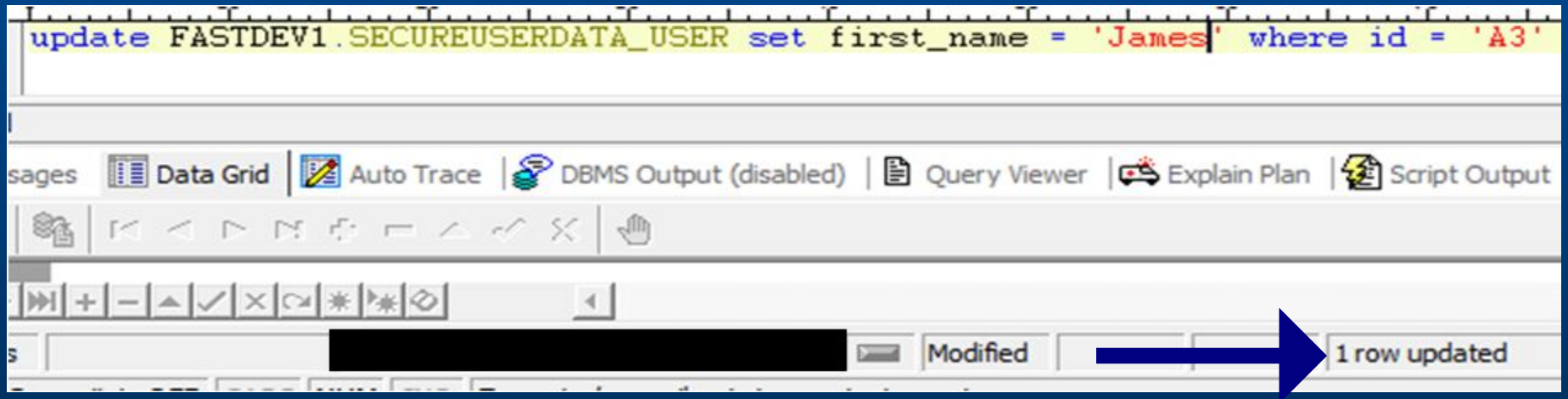
Data Grid

Messages | Data Grid | Auto Trace | DBMS Output (disabled) | Query Viewer | Exp

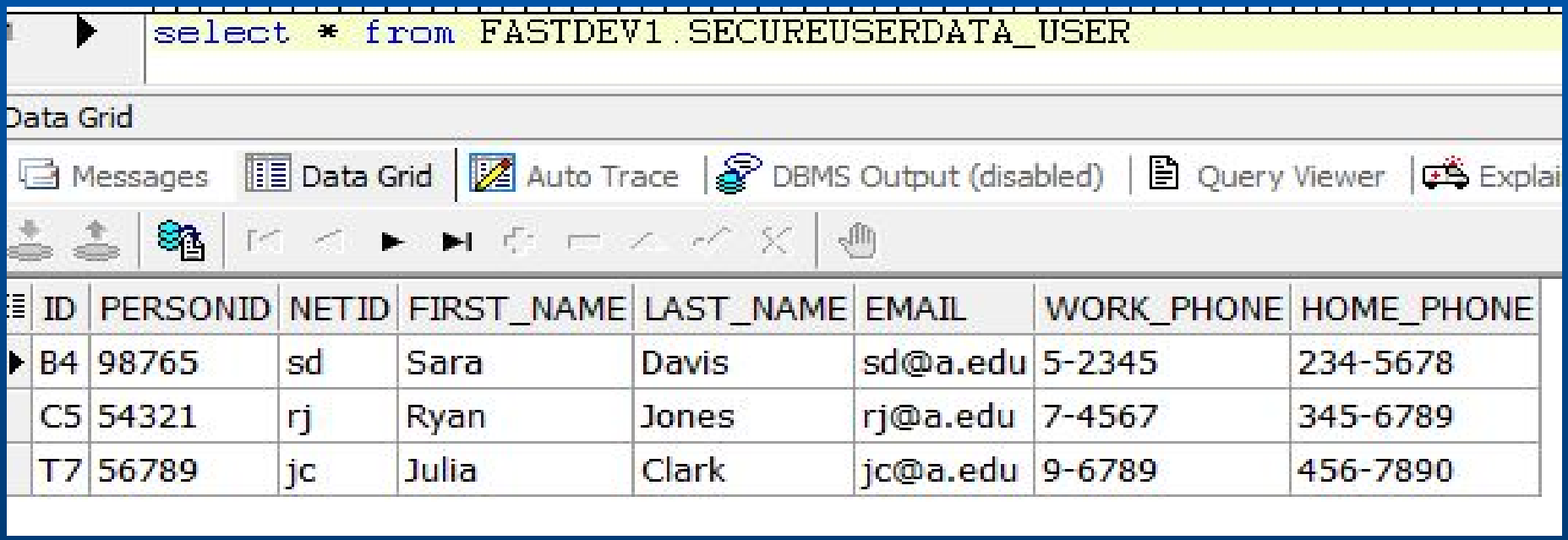
ID	PERSONID	NETID	FIRST_NAME	LAST_NAME	EMAIL	WORK_PHONE	HOME_PHONE
A3	12345	js	John	Smith			
B4	98765	sd	Sara	Davis			

Oracle FGAC queries from student billing application: can update name, not ids





Oracle FGAC queries from faculty/staff file sharing application: sees fac/staff and all columns



```
select * from FASTDEV1.SECUREUSERDATA_USER
```

Data Grid

Messages | Data Grid | Auto Trace | DBMS Output (disabled) | Query Viewer | Explai

ID	PERSONID	NETID	FIRST_NAME	LAST_NAME	EMAIL	WORK_PHONE	HOME_PHONE
B4	98765	sd	Sara	Davis	sd@a.edu	5-2345	234-5678
C5	54321	rj	Ryan	Jones	rj@a.edu	7-4567	345-6789
T7	56789	jc	Julia	Clark	jc@a.edu	9-6789	456-7890

Real-time row membership notification demo

- Start the real time XMPP listener:

```
C:\mchyzer\grouper\trunk\poc_secureUserData>java -cp conf;lib\*;dist\secureUserD
ata.jar edu.internet2.middleware.poc_secureUserData.SudRealTime
```

- Less than 1 minute after Grouper change, XMPP message goes from Grouper to SUD real time logic
- Note, it is configured to only send/receive relevant messages

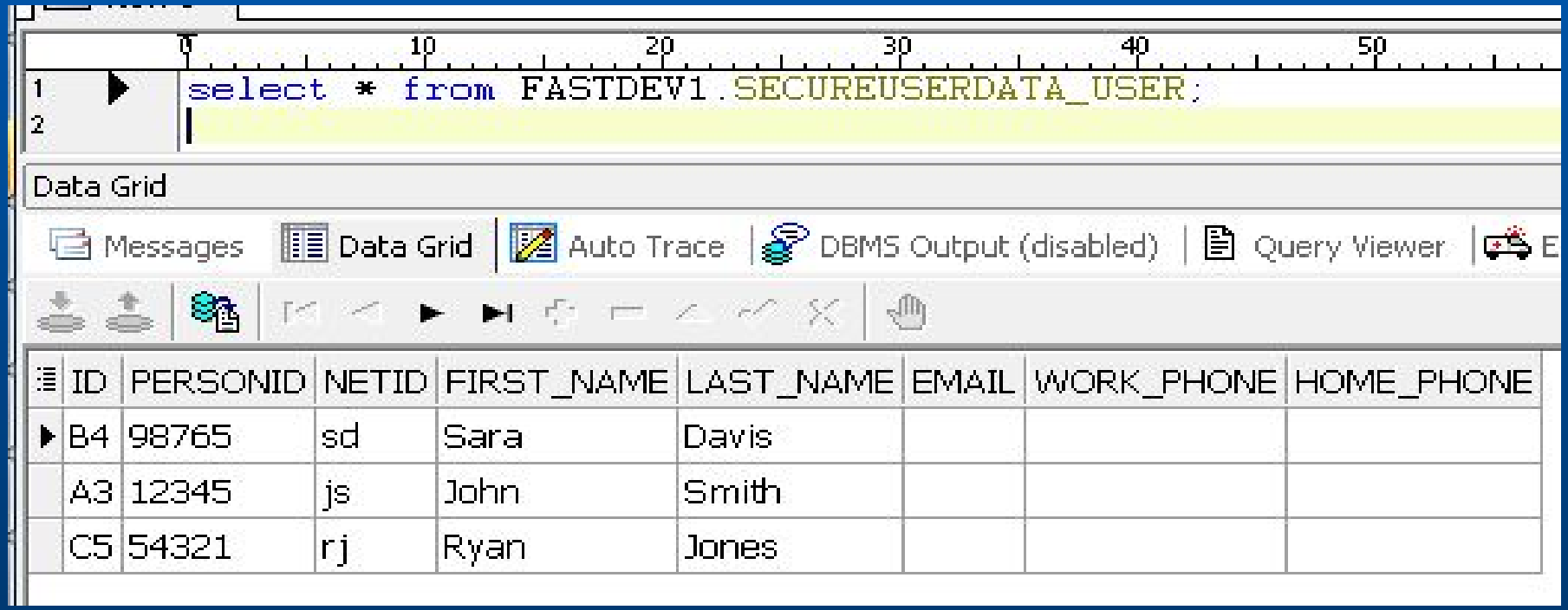
```
(1:01:00 AM) PennGroups: <sudChangeLogMessage><changeType>rowGroupChange</
changeType><rowGroupExtension>fgacStudents</rowGroupExtension><rowSubjectId>54321</rowSubjectId></
sudChangeLogMessage>
```

- See the listener process the message

```
C:\mchyzer\grouper\trunk\poc_secureUserData>java -cp conf;lib\*;dist\secureUserD
ata.jar edu.internet2.middleware.poc_secureUserData.SudRealTime
 - Add mship for group: fgacStudents, personid: 54321
```

Real-time row membership notification demo

- See that Ryan is now a student, select users from fastdev2 (student application)



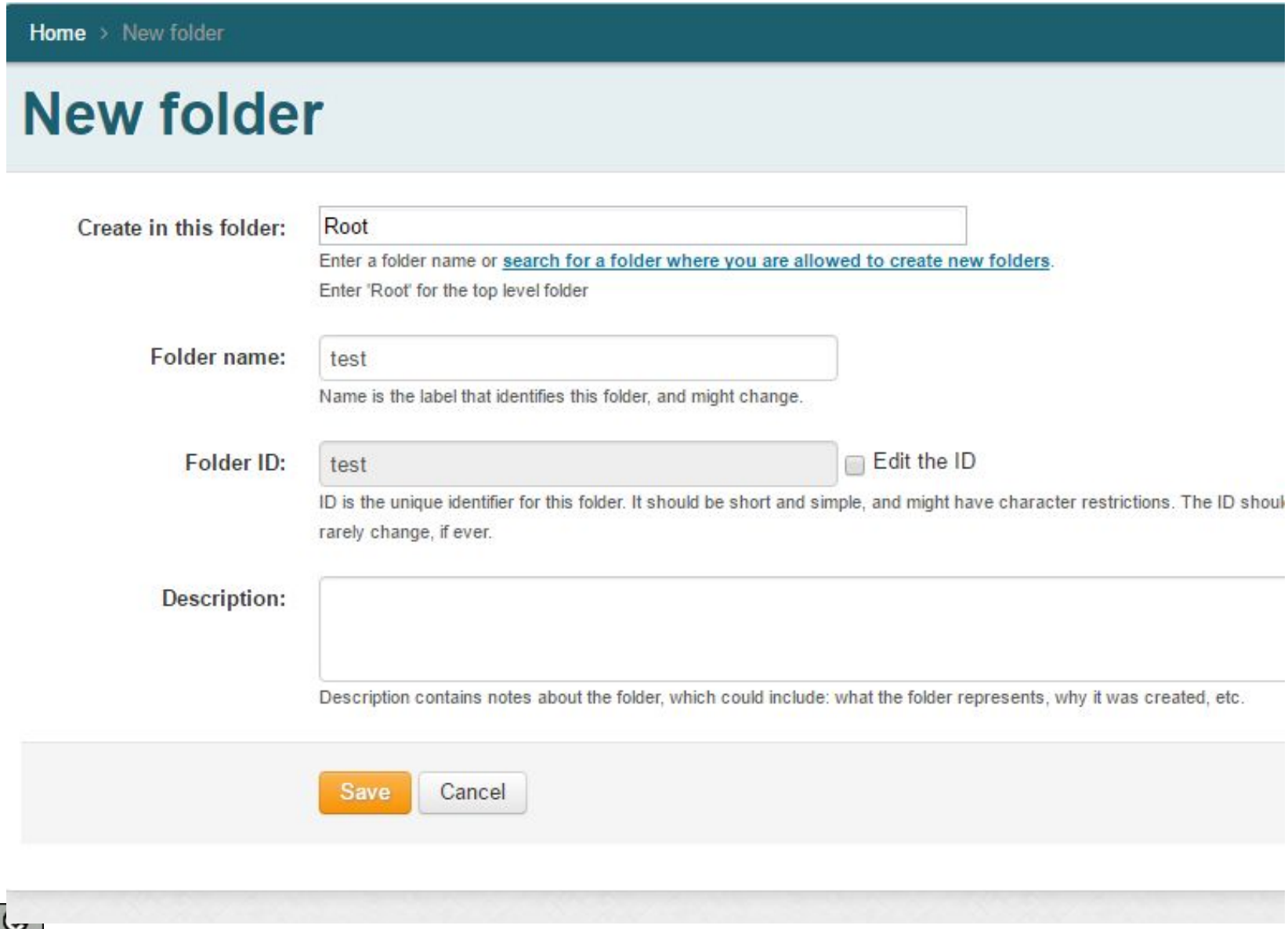
ID	PERSONID	NETID	FIRST_NAME	LAST_NAME	EMAIL	WORK_PHONE	HOME_PHONE
B4	98765	sd	Sara	Davis			
A3	12345	js	John	Smith			
C5	54321	rj	Ryan	Jones			

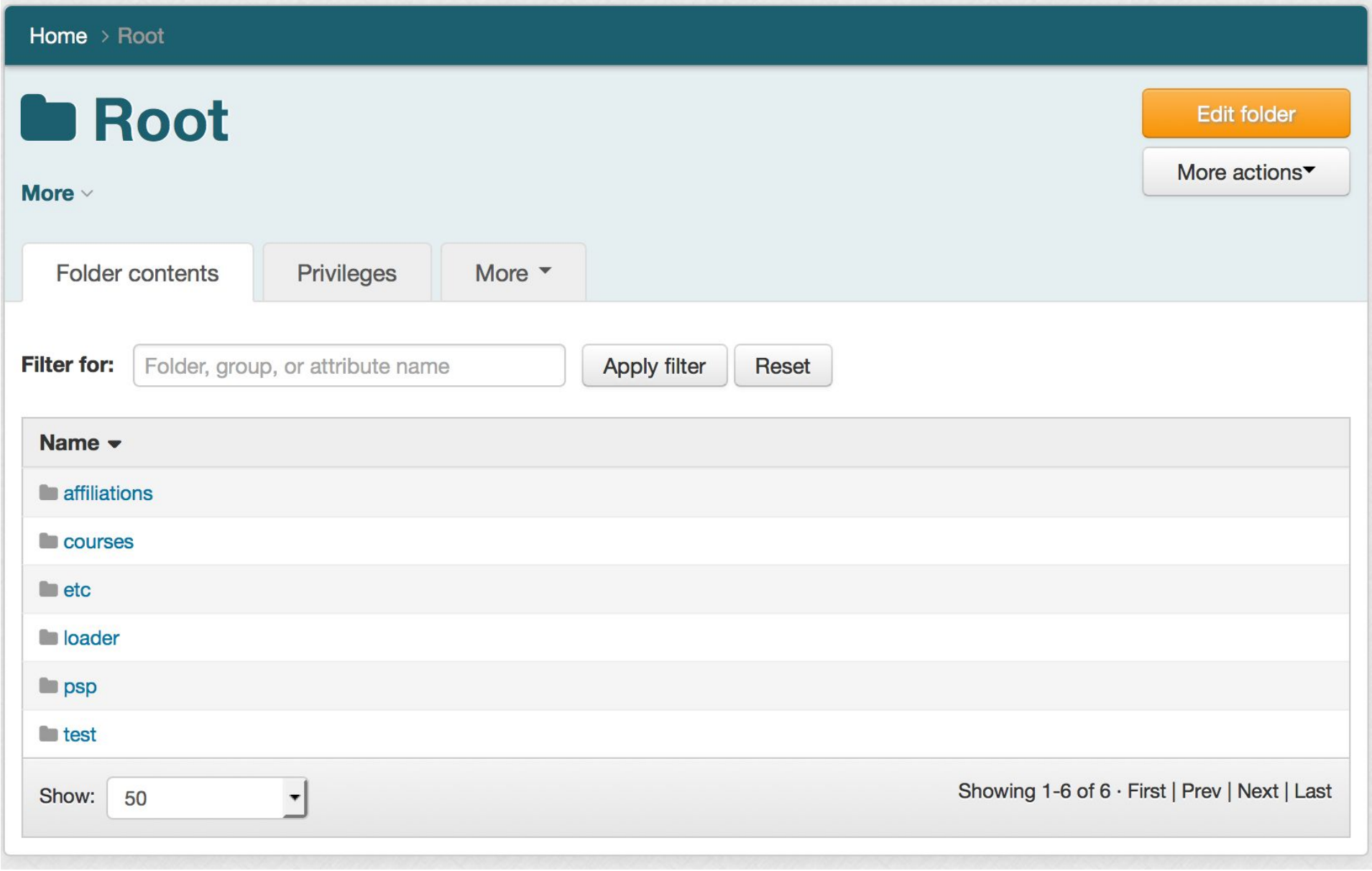
Open Apereo 2016

100% Open for Education

Grouper - Hands on exercises

Create new folder




Home › Root
Root
More
Edit folder
More actions
Folder contents
Privileges
More
Filter for:
Folder, group, or attribute name
Apply filter
Reset
Name
affiliations
courses
etc
loader
psp
test
Show:
50
Showing 1-6 of 6 · First | Prev | Next | Last

New group

Create in this folder: test

Enter a folder name or **search for a folder where you are allowed to create new groups**.

Group name: test_group

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

Group ID: test_group ☐ Edit the ID

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.

Description: A test group

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

Show advanced properties

Save Cancel

test_group

+ Add members

More actions

Member name or ID: Bob Anderson

Enter an entity name or ID, or search for an entity.

Assign these privileges: Default privileges Custom privileges

Add or **import a list of members** .

A test group

More

Members | Privileges | More

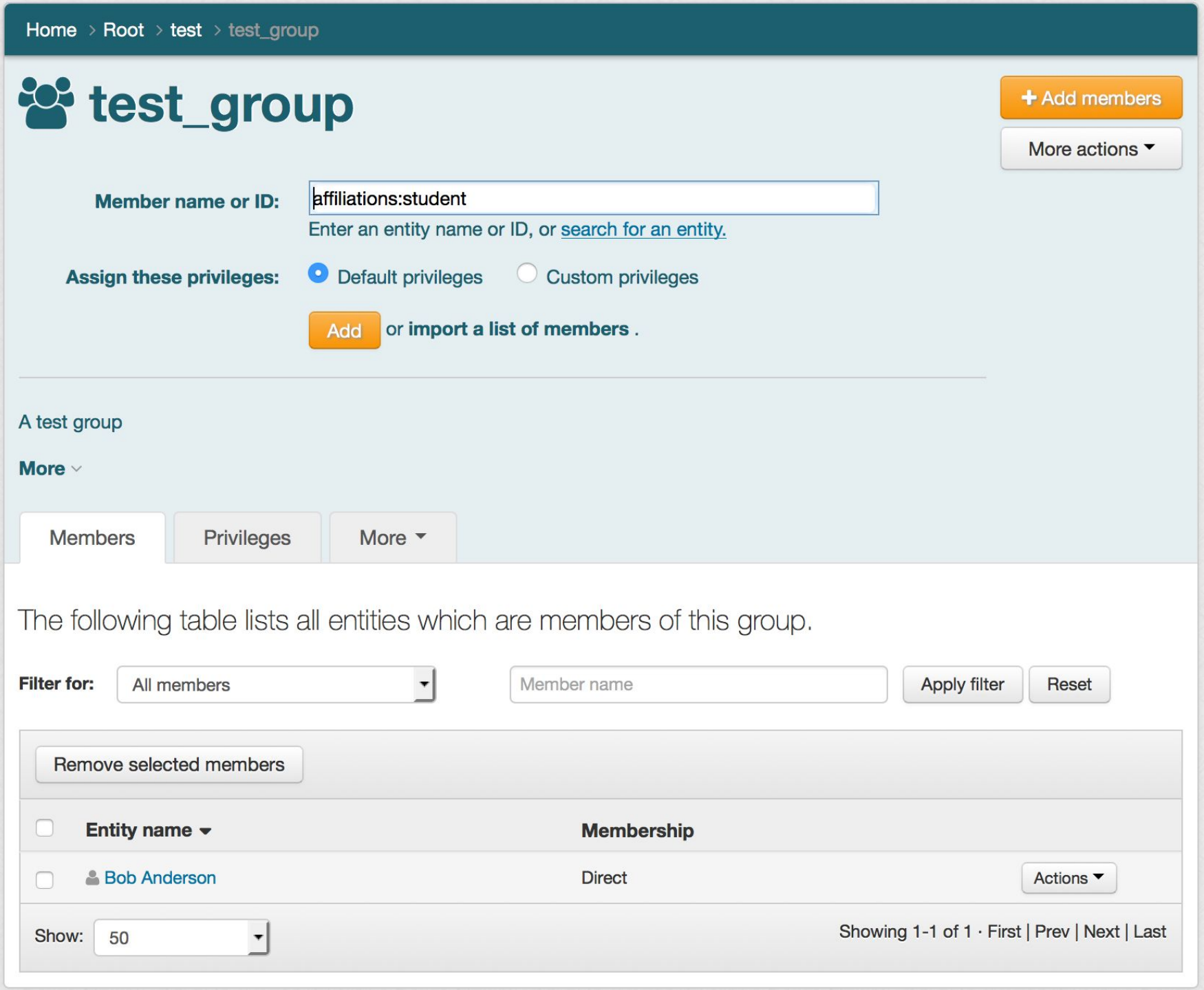
The following table lists all entities which are members of this group.

Filter for: All members Member name Apply filter Reset

Remove selected members

Entity name	Membership

Show: 50 Showing 1-0 of 0 · First | Prev | Next | Last


Home > Root > test > test_group
test_group
+ Add members
More actions
Member name or ID:
affiliations:student
Enter an entity name or ID, or search for an entity.
Assign these privileges:
Default privileges
Custom privileges
Add
or import a list of members .
A test group
More
Members
Privileges
More
The following table lists all entities which are members of this group.
Filter for:
All members
Member name
Apply filter
Reset
Remove selected members
Entity name
Membership
Bob Anderson
Direct
Actions
Show:
50
Showing 1-1 of 1 · First | Prev | Next | Last

test_group

+ Add members

More actions

Member name or ID:

Enter an entity name or ID, or search for an entity.

Assign these privileges: Default privileges Custom privileges

Add or **import a list of members** .

A test group

More

Members | Privileges | More

The following table lists all entities which are members of this group.

Filter for: Has direct membership | Member name | Apply filter | Reset

Remove selected members

Entity name	Membership	
Ann Gasper	Direct, Indirect	Actions
Bob Anderson	Direct	Actions
student	Direct	Actions

Show: 50

Showing 1-3 of 3 · First | Prev | Next | Last

test_group

Trace membership for Ann Gasper

Ann Gasper is a member of the *test_group* group by the following paths:

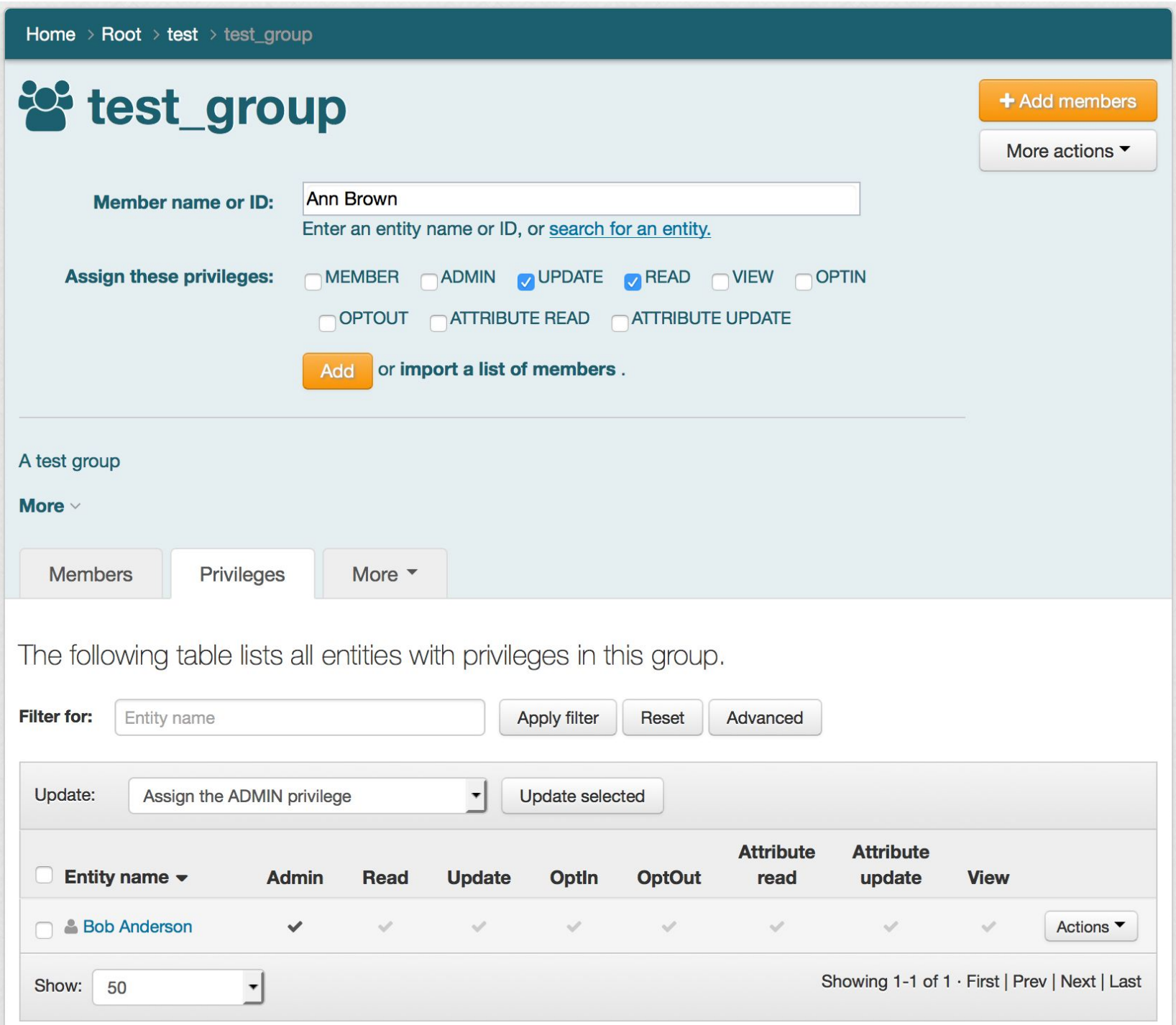
Ann Gasper is a **direct member** of

- test:test_group

Ann Gasper is a **direct member** of

- affiliations:student system of record
  - which is a **direct member** of
    - affiliations:student system of record and includes
      - which is a **composite factor** minus student excludes of
        - affiliations:student
          - which is a **direct member** of
            - test:test_group

Back to group


Home › Root › test › test_group
test_group
+ Add members
More actions
Member name or ID:
Ann Brown
Enter an entity name or ID, or search for an entity.
Assign these privileges:
MEMBER ADMIN UPDATE READ VIEW OPTIN
OPTOUT ATTRIBUTE READ ATTRIBUTE UPDATE
Add or import a list of members .
A test group
More
Members
Privileges
More
The following table lists all entities with privileges in this group.
Filter for:
Entity name
Apply filter
Reset
Advanced
Update:
Assign the ADMIN privilege
Update selected
Entity name
Admin
Read
Update
OptIn
OptOut
Attribute read
Attribute update
View
Bob Anderson
Actions
Show:
50
Showing 1-1 of 1 · First | Prev | Next | Last

Home > Root > test > test_group

test_group

A test group

More

+ Add members

More actions

Members | Privileges | More

The following table lists all entities with privileges in this group.

Filter for: Entity name | Apply filter | Reset | Advanced

Update: Assign the ADMIN privilege | Update selected

Entity name	Admin	Read	Update	OptIn	OptOut	Attribute read	Attribute update	View	
Ann Brown		✔	✔	✔	✔			✔	Actions
Bob Anderson	✔	✔	✔	✔	✔	✔	✔	✔	Actions

Show: 50

Showing 1-2 of 2 · First | Prev | Next | Last

EXPLORE

Edit group

Current location is:

Root: test: **all_the_anns**

Name	all_the_anns
ID	all_the_anns
Alternate ID Path	
Description	
Assign privileges to everyone	☐ Read ☐ View ☐ Optin ☐ Optout ☐ Attribute read
Select group types	☐ addIncludeExclude ☑ grouperLoader ☐ requireInGroups

Save

Back to group summary

Edit attributes

Current location is:

Root: test: **all_the_anns**

Group type	Attribute	Value
grouperLoader		
	grouperLoaderAndGroups	
	grouperLoaderDbName	grouper
	grouperLoaderGroupQuery	
	grouperLoaderGroupTypes	
	grouperLoaderGroupsLike	
	grouperLoaderIntervalSeconds	
	grouperLoaderPriority	
	grouperLoaderQuartzCron	0 0 * * * ?
	grouperLoaderQuery	d as subject_id from SIS_COURSES where givenName = "Ann"
	grouperLoaderScheduleType	CRON
	grouperLoaderType	SQL_SIMPLE

Save attributes and finish | Save attributes and add members

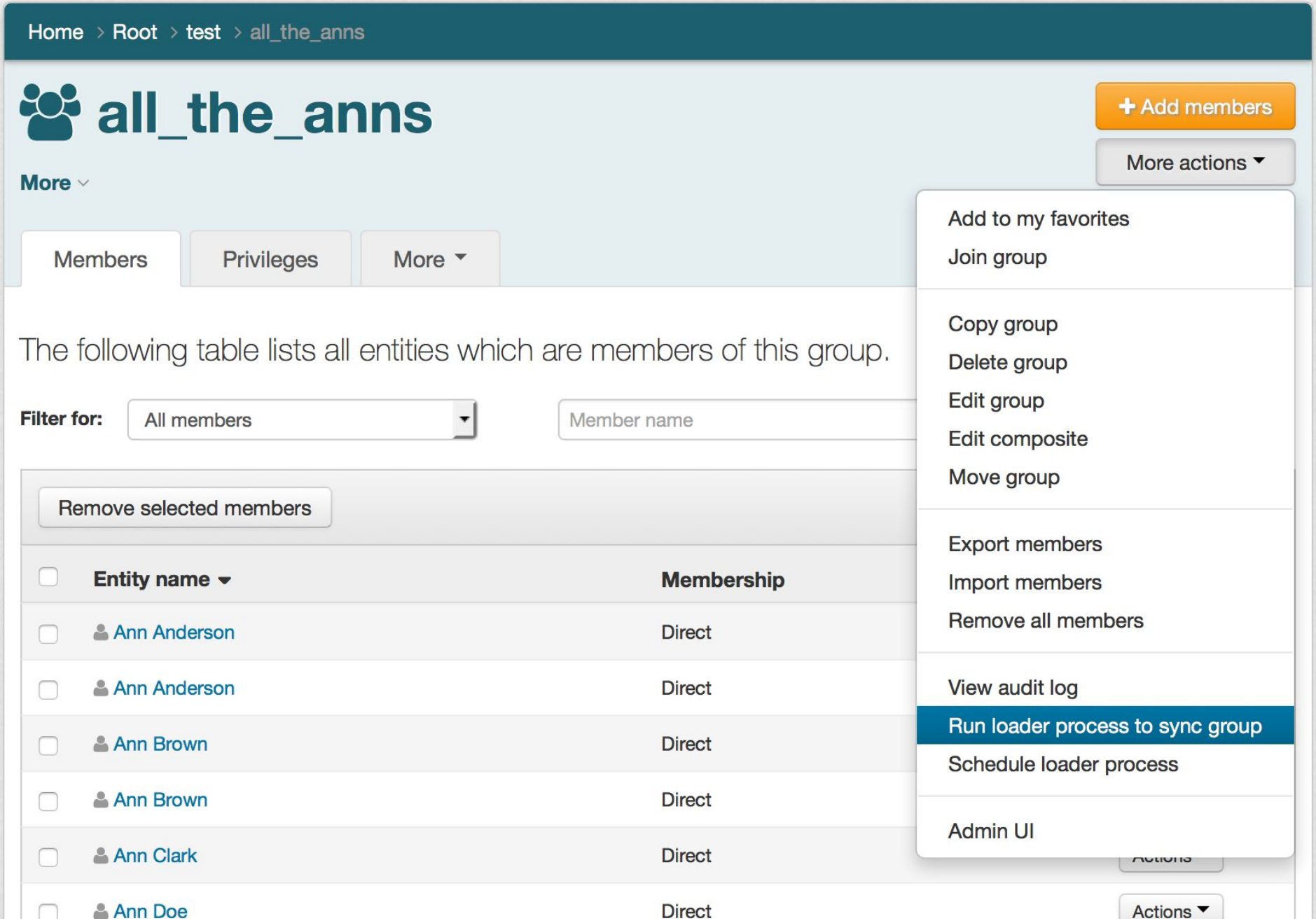
```
select SIS_COURSES.uid as subject_id from SIS_COURSES
    where givenName = "Ann"
```

Current location is:

Root: test: **all_the_anns**

Name	all_the_anns
Path	test:all_the_anns
Description	
ID	all_the_anns
ID Path	test:all_the_anns
Alternate ID Path	
UUID	d8d464b45a8e4526a054ac2608312837
Types	**grouperLoader**

grouperLoaderAndGroups	
grouperLoaderDbName	grouper
grouperLoaderGroupQuery	
grouperLoaderGroupTypes	
grouperLoaderGroupsLike	
grouperLoaderIntervalSeconds	
grouperLoaderPriority	
grouperLoaderQuartzCron	0 0 * * * ?
grouperLoaderQuery	select SIS_COURSES.uid as subject_id from SIS_COURSES where givenName = "Ann"
grouperLoaderScheduleType	CRON
grouperLoaderType	SQL_SIMPLE


Home › Root › test › all_the_anns
all_the_anns
More
+ Add members
More actions
Members
Privileges
More
The following table lists all entities which are members of this group.
Filter for:
All members
Member name
Remove selected members
Entity name
Membership
Ann Anderson
Direct
Ann Anderson
Direct
Ann Brown
Direct
Ann Brown
Direct
Ann Clark
Direct
Ann Doe
Direct
Actions
Add to my favorites
Join group
Copy group
Delete group
Edit group
Edit composite
Move group
Export members
Import members
Remove all members
View audit log
Run loader process to sync group
Schedule loader process
Admin UI

New group

Create in this folder: test

Enter a folder name or **search for a folder where you are allowed to create new groups**.

Group name: employee_Anns

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

Group ID: employee_Anns ☐ Edit the ID

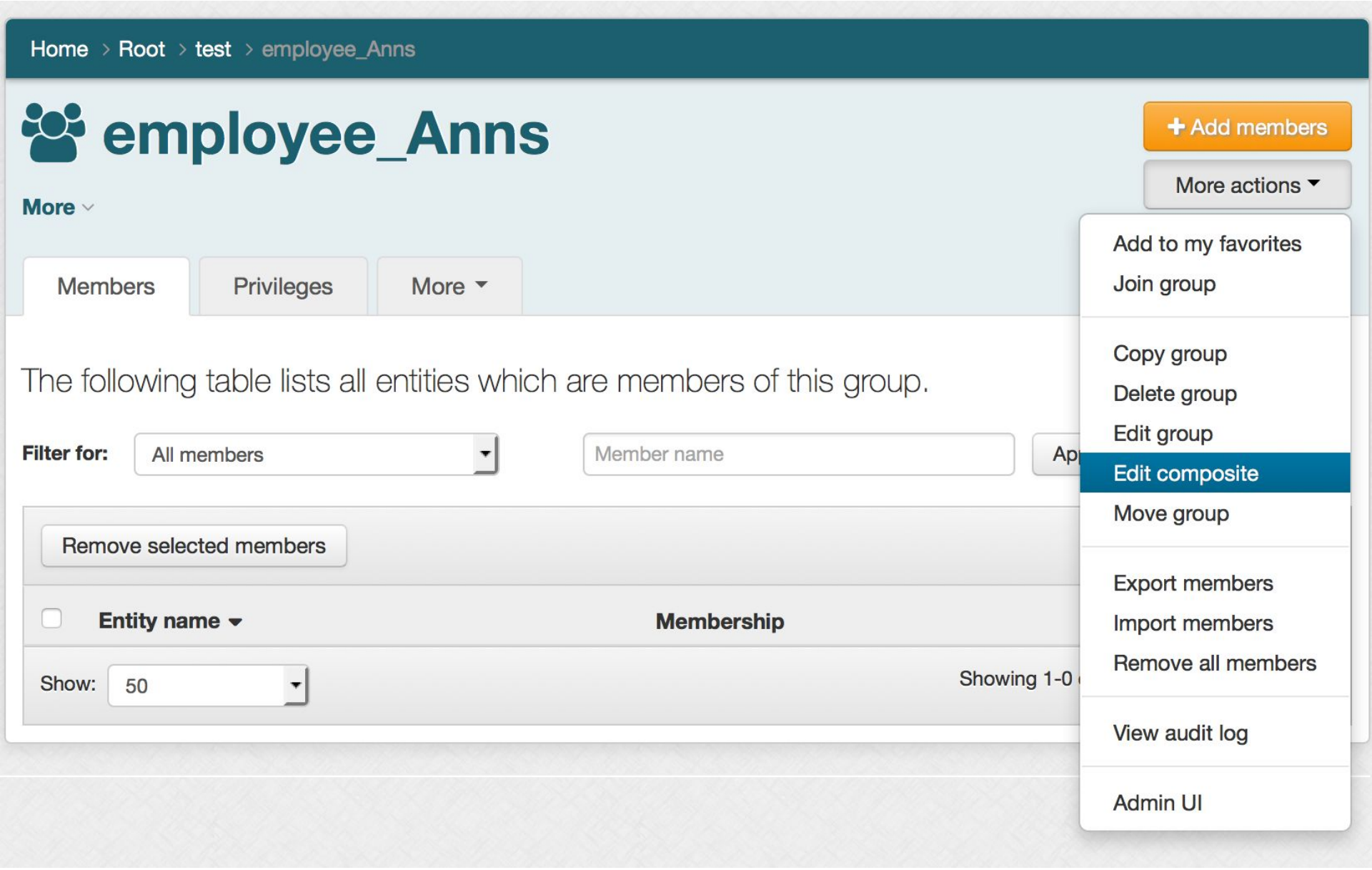
ID is the unique identifier for this group. It should be short and simple, and might have character restrictions. The ID should rarely change, if ever.

Description:

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

Show advanced properties

Save Cancel


Home > Root > test > employee_Anns
employee_Anns
+ Add members
More actions
More
Members
Privileges
More
Add to my favorites
Join group
Copy group
Delete group
Edit group
Edit composite
Move group
Export members
Import members
Remove all members
View audit log
Admin UI
The following table lists all entities which are members of this group.
Filter for:
All members
Member name
Remove selected members
Entity name
Membership
Show:
50
Showing 1-0

employee_Anns

Edit group composite

Composite: ○ No ◉ Yes

First factor group: affiliations:staff

Enter a group name or ID, or search for the first factor.

Operation: and (intersection)

There are three composite operations: intersection, complement, and union.
Intersection means members of the overall group must be in both factor groups. **Intersection** is used for example when requiring members to be active employees.
Complement means members are in the first group but not in the second group. **Complement** is used for exclude lists.
Union is not needed, you can just add the groups as members of the overall group.

Second factor group: test:all_the_anns

Enter a group name or ID, or search for the second factor.

Save Cancel

Home › Root › test › employee_Anns

employee_Anns

+ Add members

More actions

More

Members | Privileges | More

The following table lists all entities which are members of this group.

Note: this group is a composite owner: employee_Anns is a composite intersection of staff and all_the_anns

Filter for: All members | Member name | Apply filter | Reset

Remove selected members

	Entity name	Membership	
☐	Ann Langenberg	Indirect	Actions
☐	Ann Smith	Indirect	Actions

Show: 50

Showing 1-2 of 2 · First | Prev | Next | Last

Apereo 2016 Grouper Sessions

Exploring Internet2 Grouper & NIST RBAC/ABAC

Time: May 25, 2016, 10:45 AM - 11:30 AM

Location: KC 907

Misagh Moayyed - Software Engineer, Unicon

Bill Thompson - Lafayette College

Scriptable Grouper - Lafayette College's Big Fish Story

Title: Scriptable Grouper - Lafayette College's Big Fish Story

Time: May 24, 2016, 3:00 PM - 3:45 PM

Location: KC 907

Carl Waldbieser - Lafayette College

Thanks!

Further information:

Infosheets, mail lists, wiki, downloads, etc:
www.internet2.edu/grouper

Grouper demo server:
https://grouperdemo.internet2.edu/