Grouper in action

PRESENTED BY: **CHRIS HYZER, UNIVERSITY OF PENNSYLVANIA**
BILL THOMPSON, LAFAYETTE COLLEGE
KEITH WESSEL, UNIVERSITY OF ILLINOIS
CHRIS HUBING, INTERNET2

© 2018 Internet2

Agenda

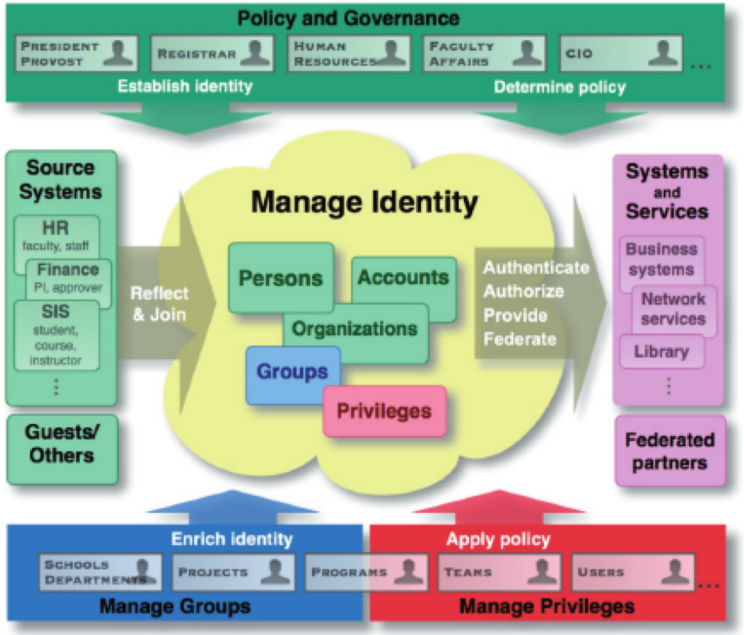
1. Introduction to Grouper (30 min)
2. TIER GDG, GTE, ref groups (45 min)
3. Packaging (15 min)
4. Grouper @ Duke (10 min)
5. Grouper @ Illinois (10 min)
6. Grouper @ Lafayette (10 min)
7. Break (15 min)
8. Open Q&A (15 min)
9. Hands on Grouper (90 min)

 | © 2018 Internet2

Grouper in action

TABLE OF CONTENTS

Access management strategy

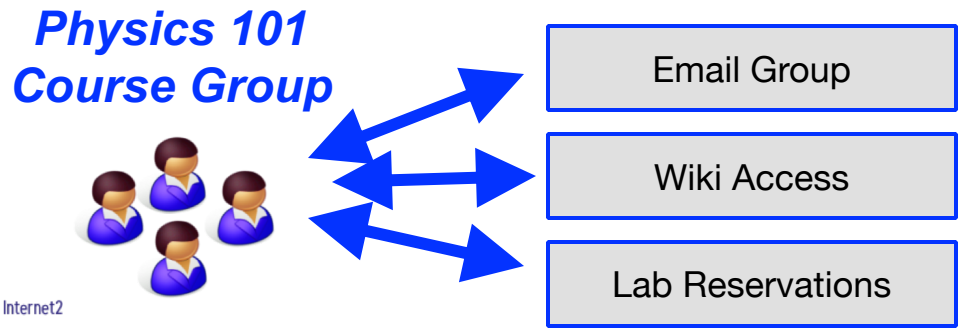


- Tools & processes to translate IAM concepts into typical campus environment
  - Which people?
  - What systems & business processes?
  - What policies?
  - What purposes?
  - Whose authority?

 © 2018 Internet2

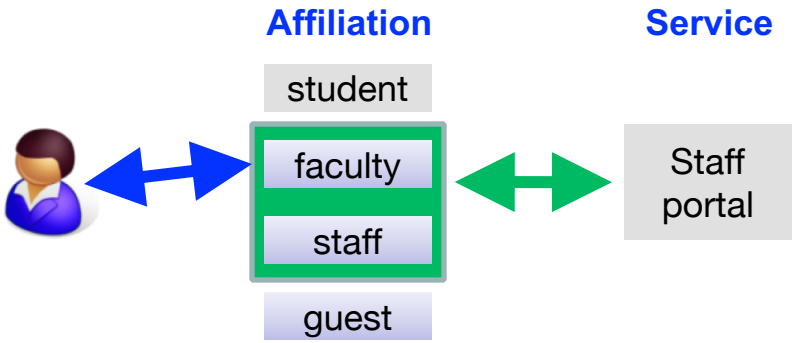
Why have an access management strategy?

- 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 levels of maturity:

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



Access management stages

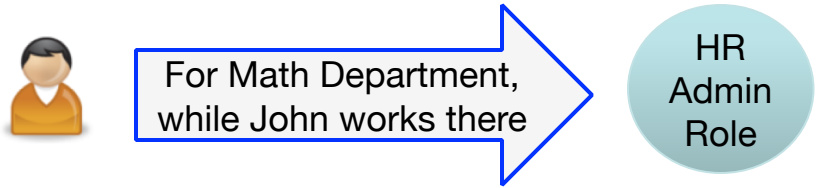
2. Maintain access groups determined from systems of record
   - Courses, departments,…
   - Define service-specific access policies in the centralized access management system

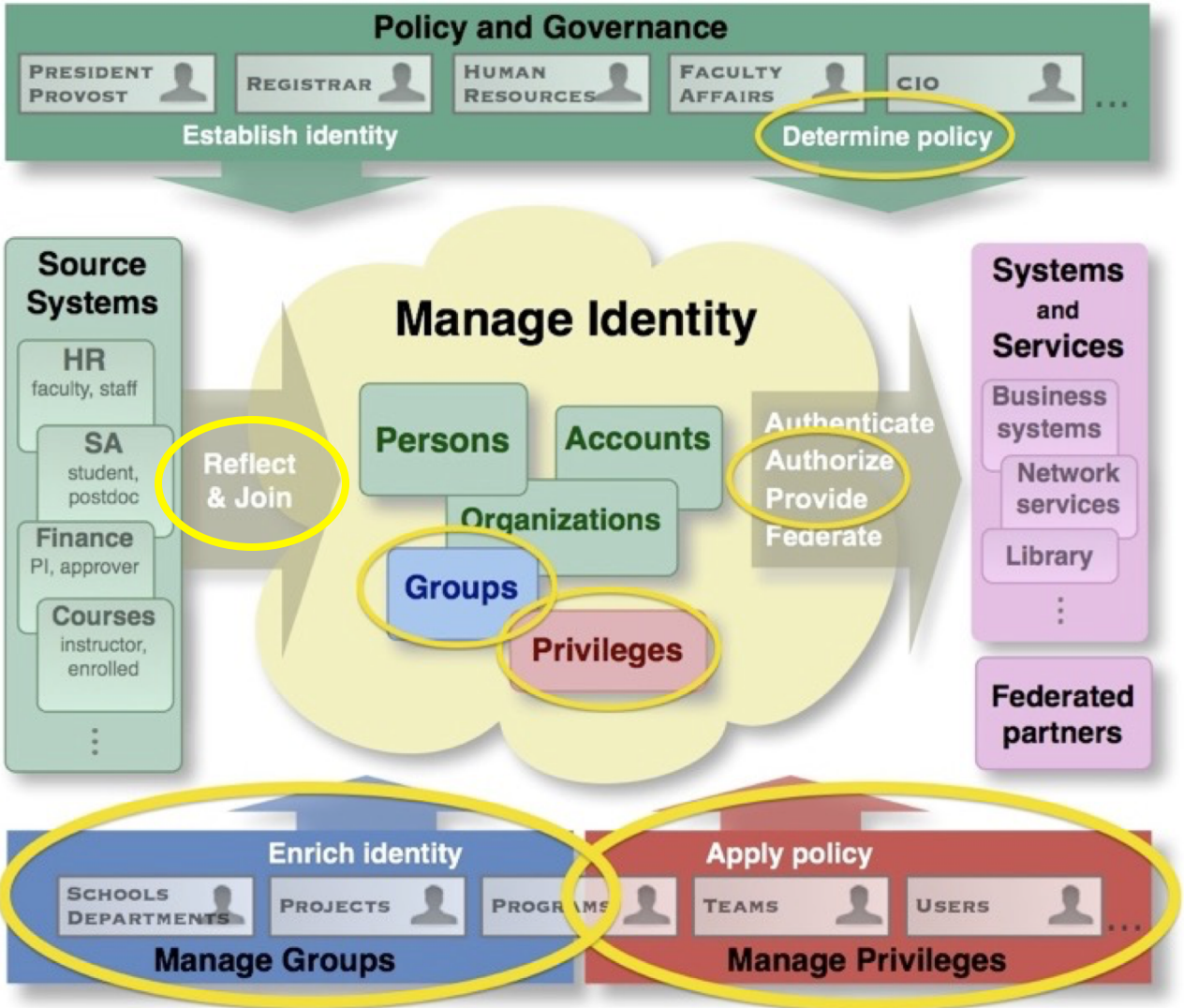
Access management stages

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
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

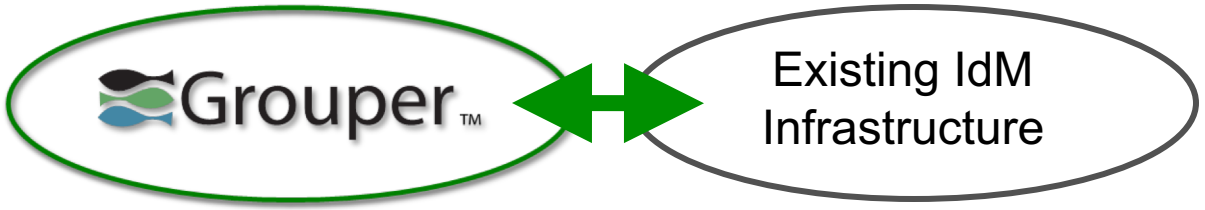
 | © 2018 Internet2

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)

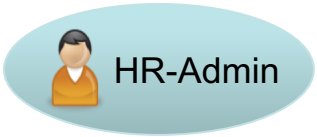
The Grouper Story

- 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

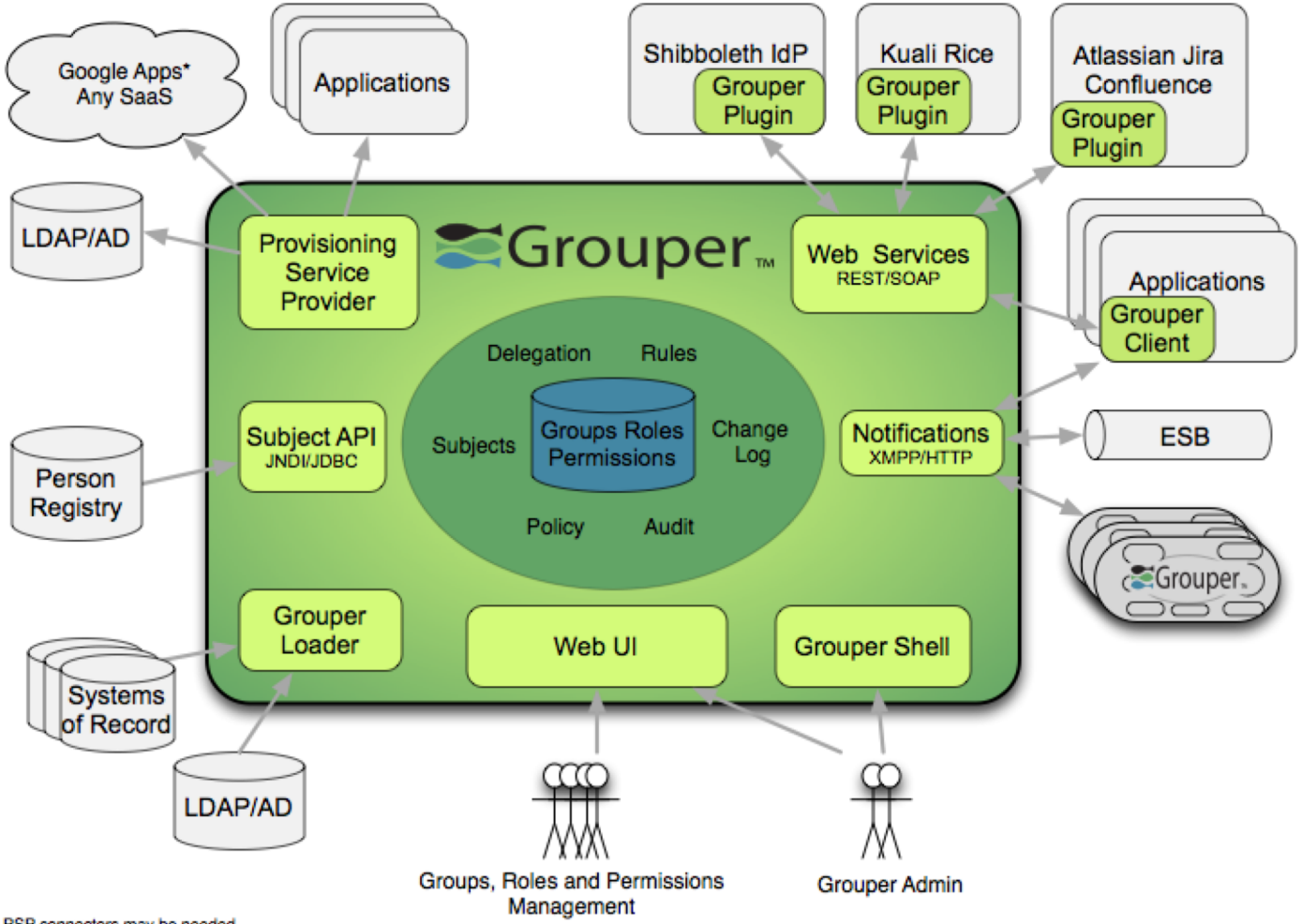
```
-  If
       removed from group A
-  then
       remove from group B
```

*"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

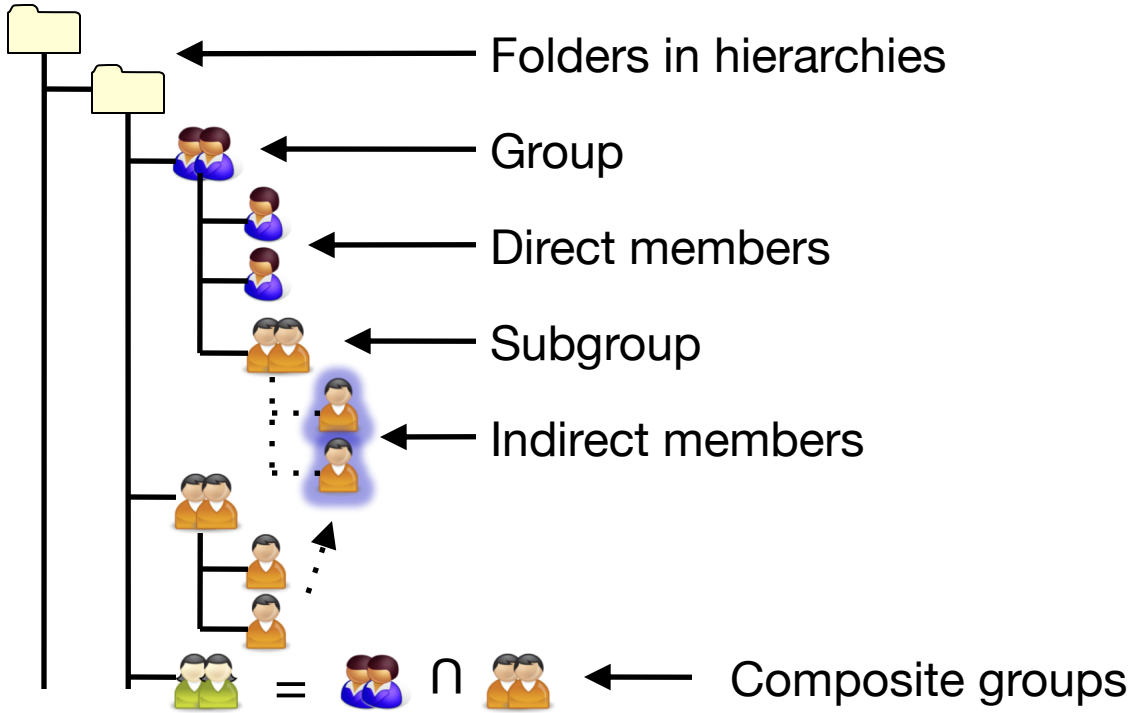
*"It's not just about federation, it's about **enabling high-value collaboration across thousands of disciplines and millions of people.** Hence agreement on attribute and authorization management, application integration, administration procedures,..."*

— RL 'Bob' Morgan



* PSP connectors may be needed

Grouper Concepts



Security and Delegation

- Admin folders
- Create sub - groups/folders/etc

- 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

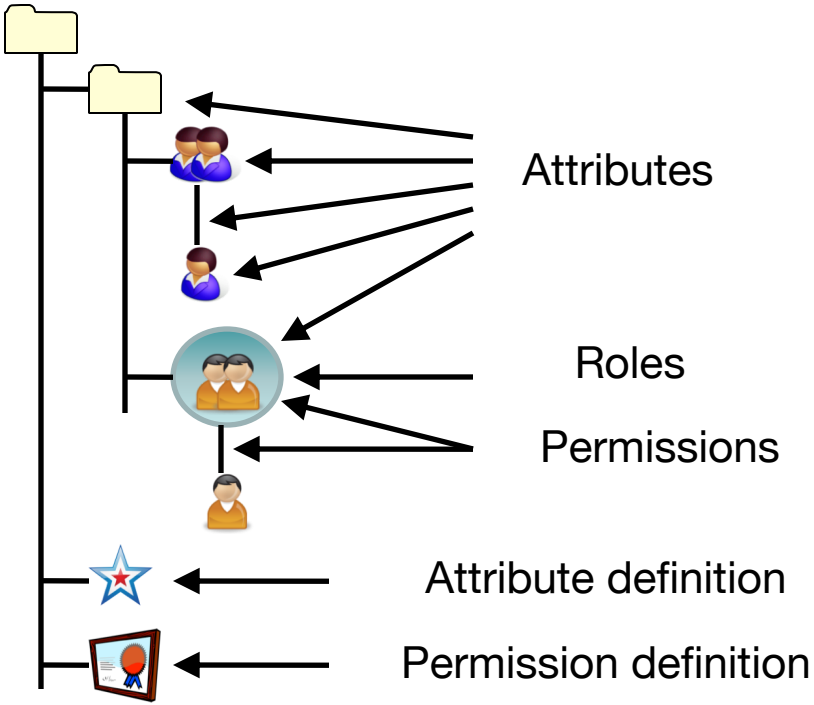
Auditing

- “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 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
- Can be scheduled and/or real-time

Beyond groups...



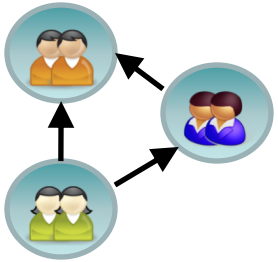
Attributes

Roles

Permissions

Attribute definition

Permission definition



Role inheritance

Delegation model extends that for Groups

Grouper - What's new?

Grouper in Action

 | © 2018 Internet2

Release 2.4.0 new features

See release notes for full list

https://spaces.internet2.edu/display/Grouper/v2.4+Release+Notes

(google “grouper release notes”)

- Migrate to New UI
- TIER instrumentation (with UI)
- Migrate XML config to properties overlays

Release 2.3.0.patch new features (continued)

- Subject API diagnostics
- Grouper loader in UI
- Attestation
- New GSH command line utility
- Messaging implementation, WS, and service bridge
- Many UI usability improvements
- Provisioning fixes and improvements
- Grouper loader improvements for real time updates
- External subject web services
- Find bad memberships daemon
- Lots of other improvements

CC BY NC

Grouper roadmap

- Deprovisioning in UI
- Provisioning in UI
- Other UI features:
  - Membership reports
  - Migrate entitlements from one user to another
- Configuration stored in database
- Improved handling of separation of duties

CC BY NC

Grouper - Hands on Grouper

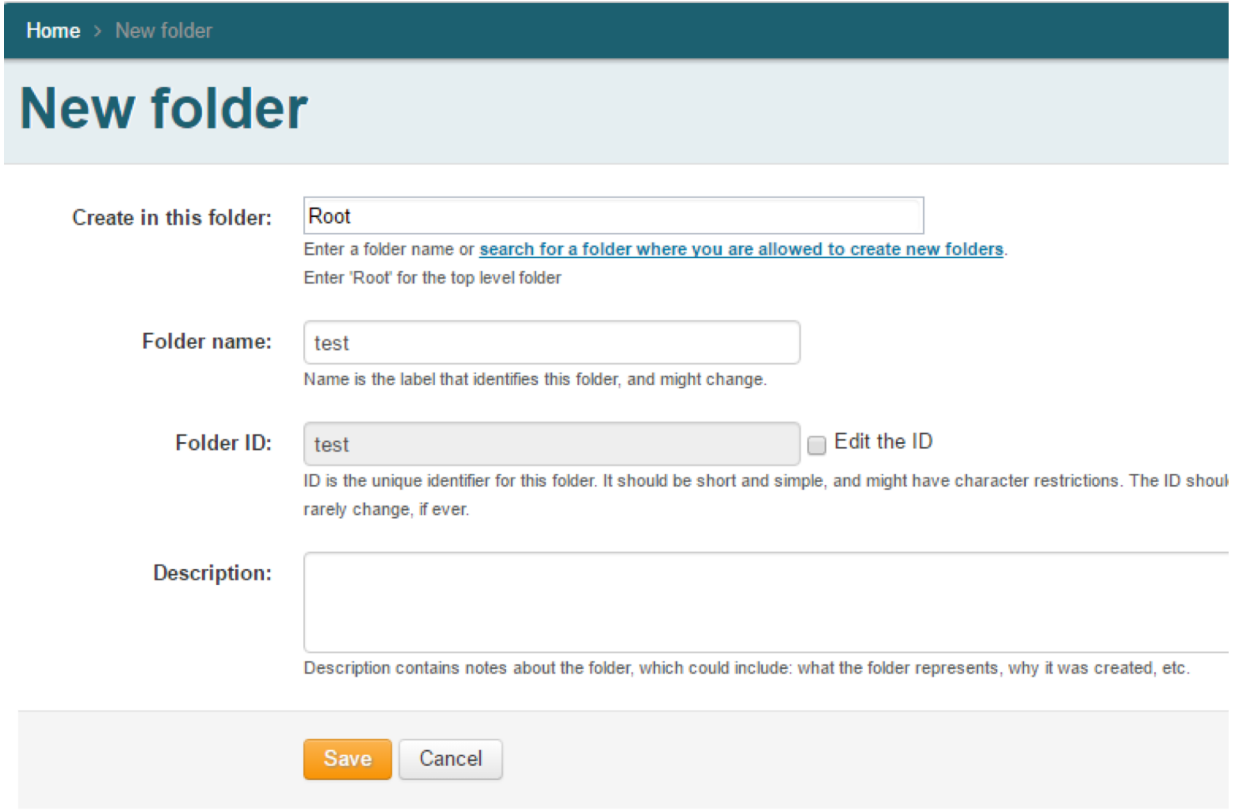
Grouper in Action

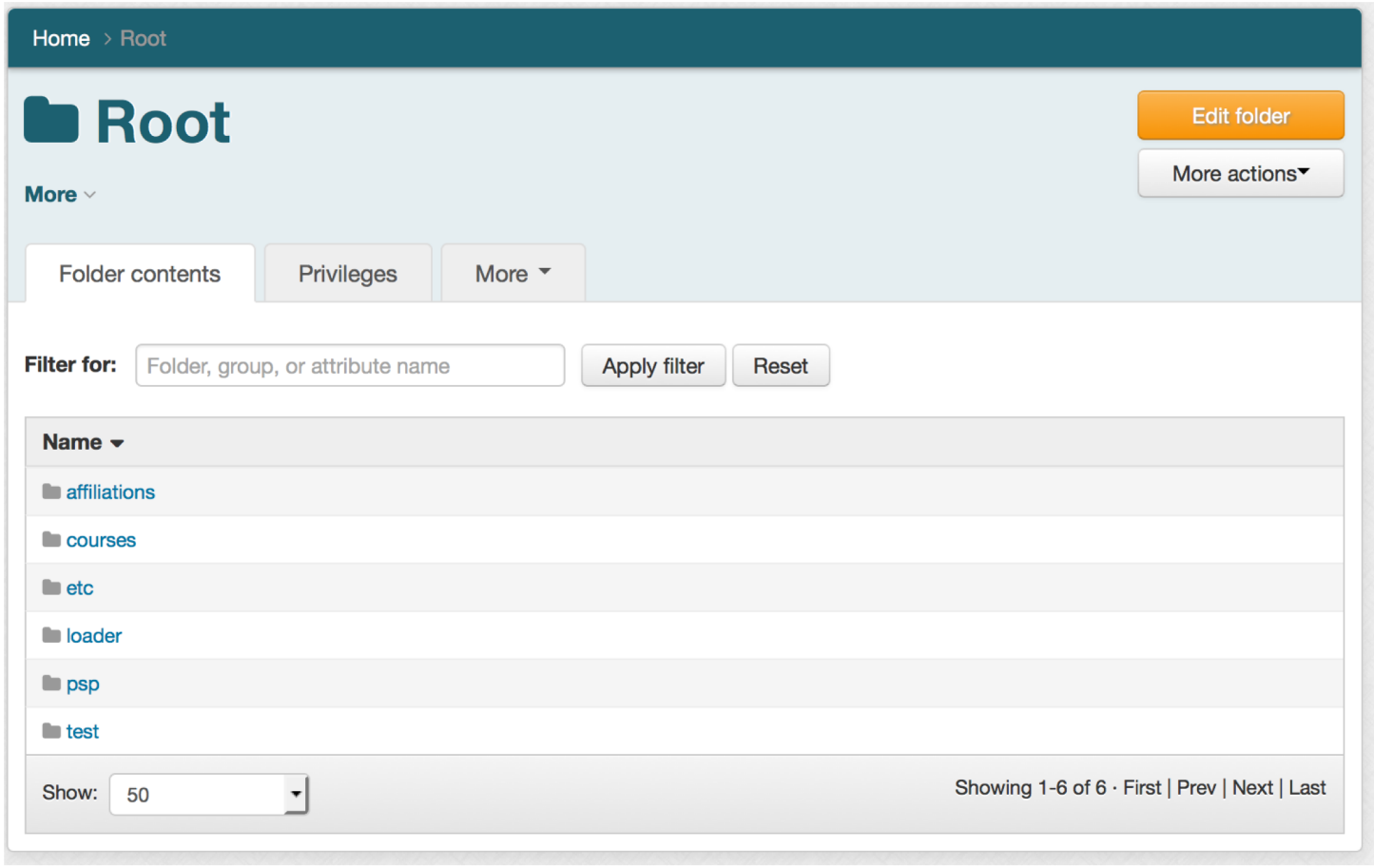
 | © 2018 Internet2

Create new folder

- Go to grouper demo (google “grouper demo”)
- https://grouperdemo.internet2.edu
- Click on UI 2.3
- Go to the folder: training:globalSummit2018
- Create a folder based on your netID (e.g. mchyzer).
  - Dont use special chars except maybe underscore.
- Click into that folder

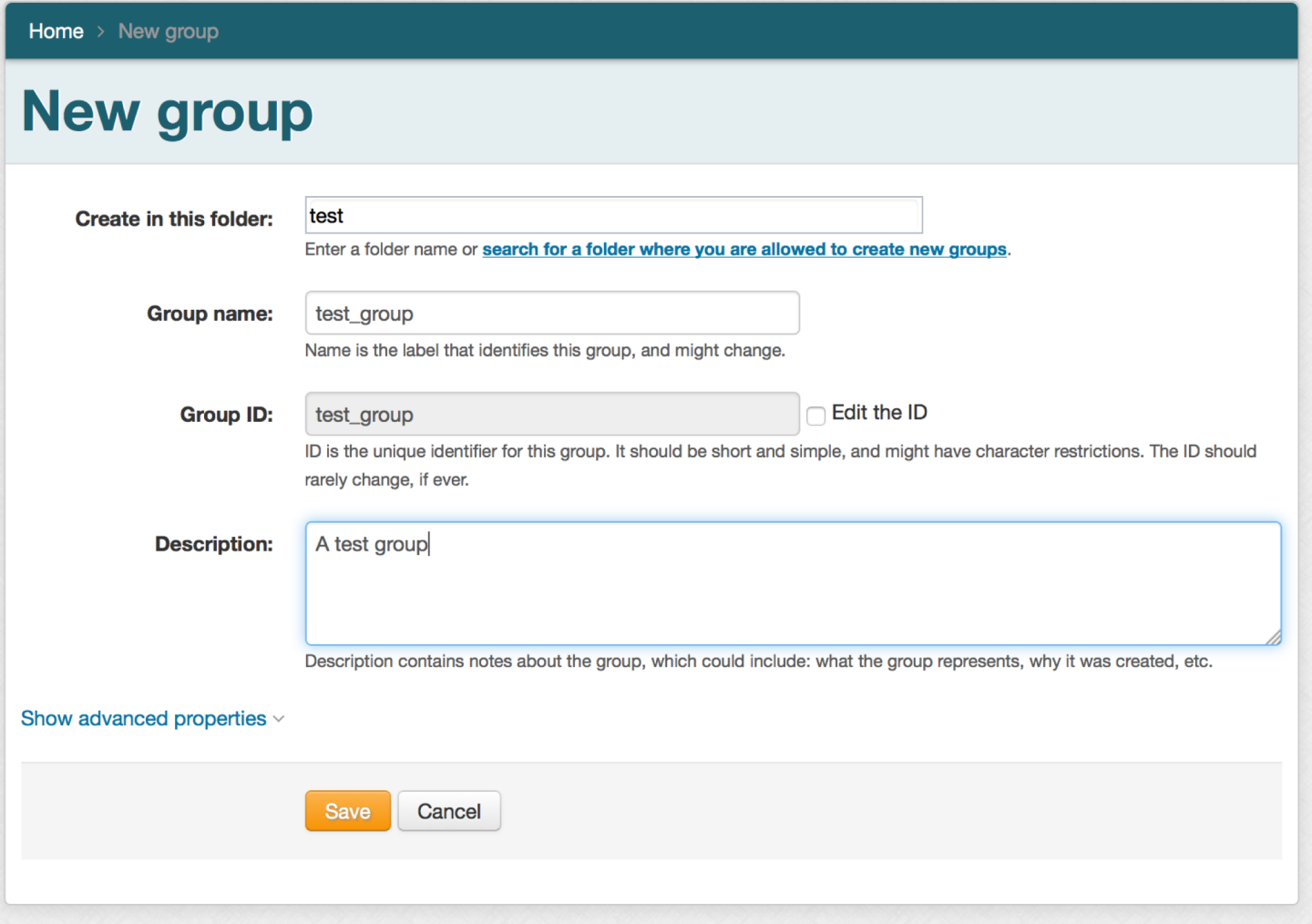
Create new folder

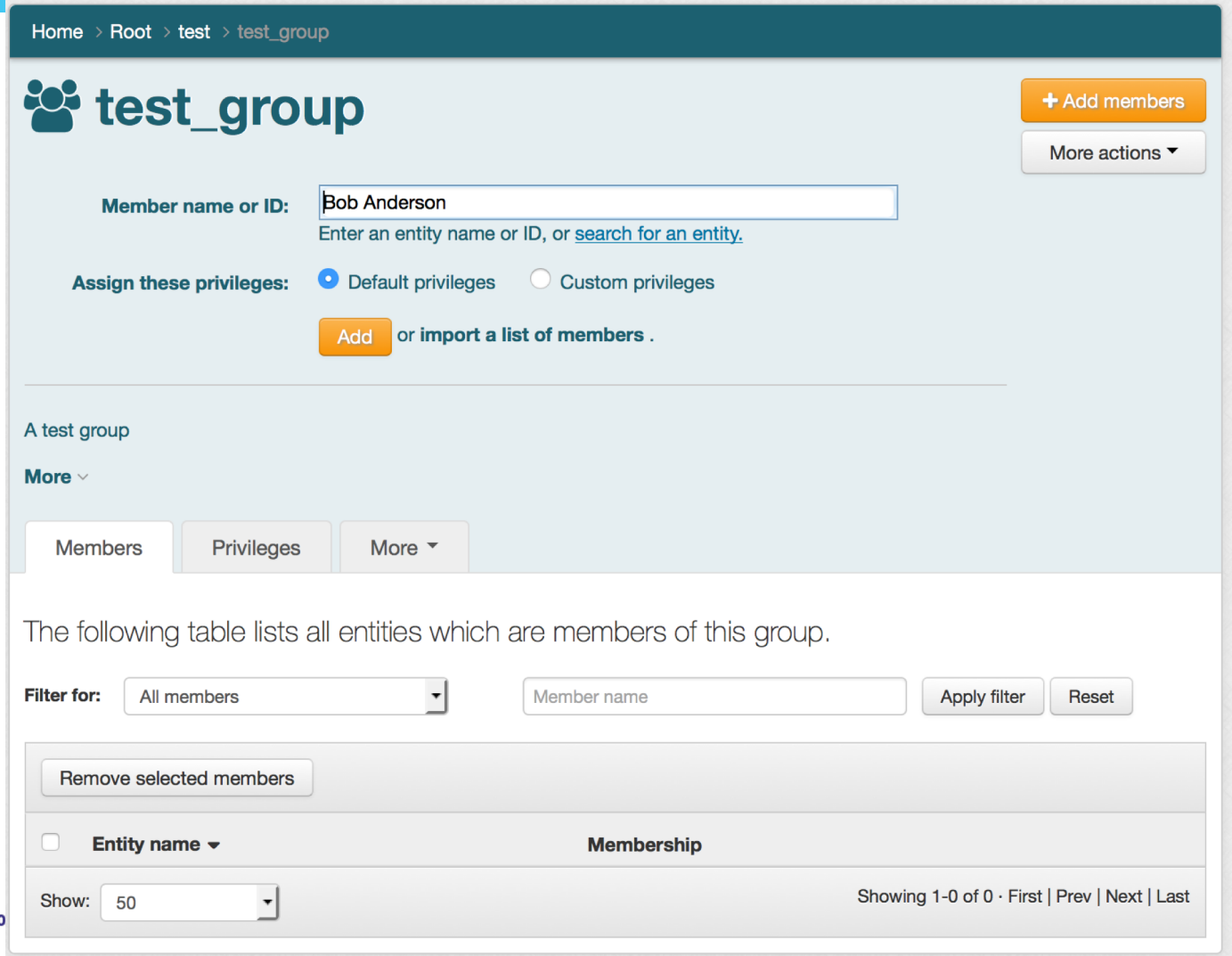


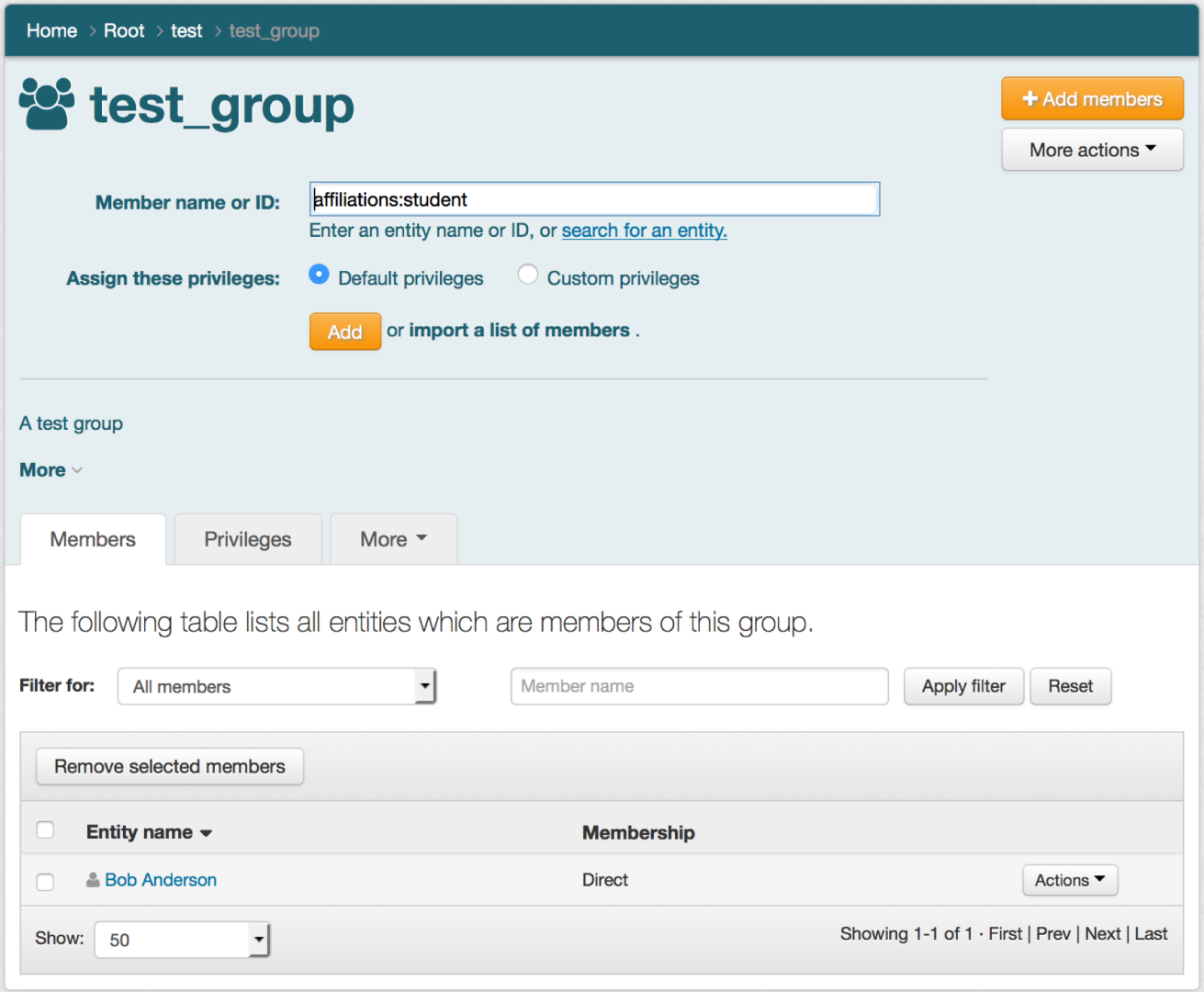

Home › Root
Root
More
Edit folder
More actions
Folder contents
Privileges
More
Filter for:
Folder, group, or attribute name
Apply filter
Reset
Name
affiliations
courses
etc
loader
psp
test
Show:
50
Showing 1-6 of 6 · First | Prev | Next | Last

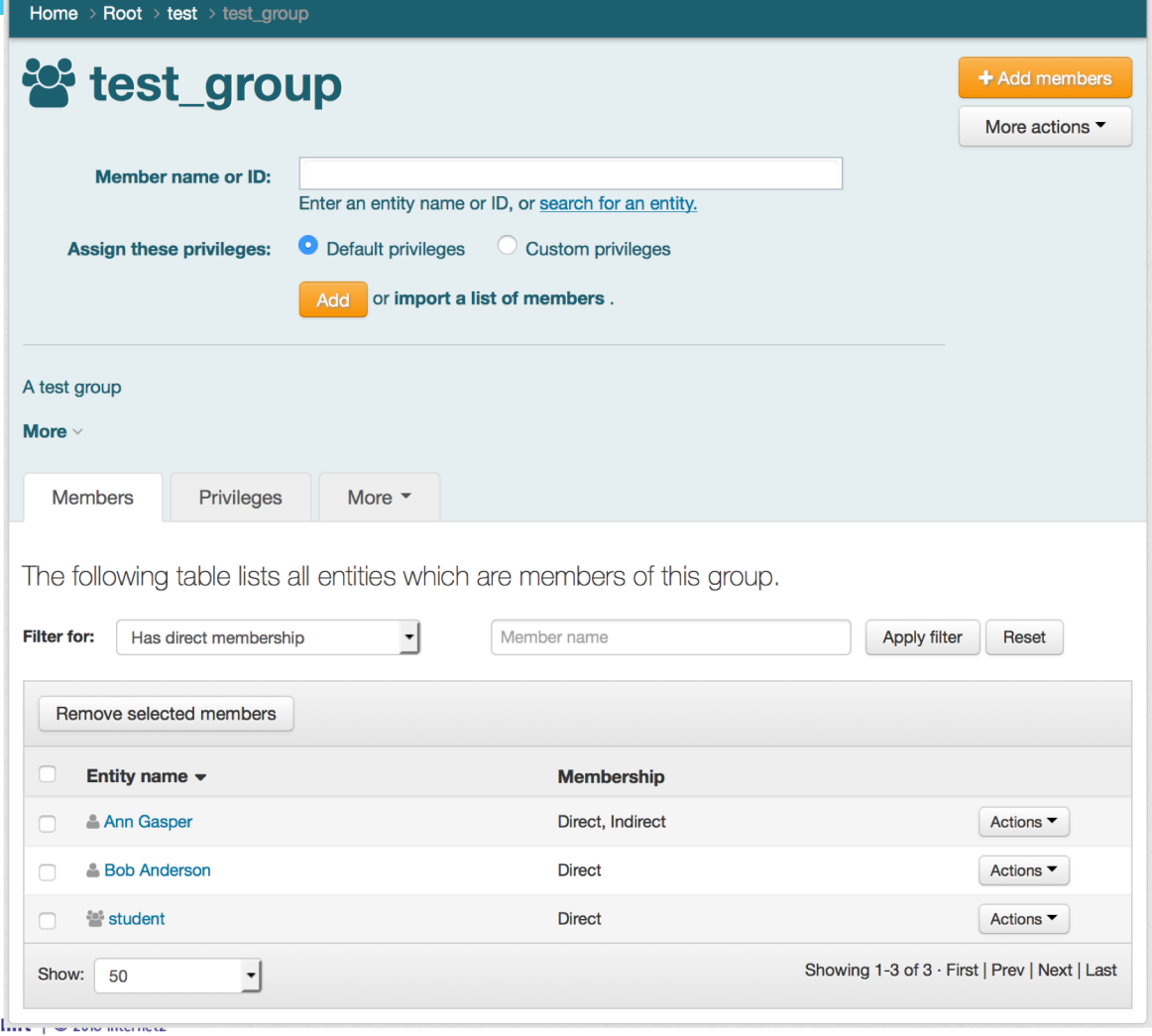
Create an “apps” folder in your folder

- In “apps”, make a “wiki” folder
  - Sometimes the extension of the folder shows in the UI, so something like mchyzerApps might be better
- In “wiki”, make an “etc” folder
  - Sometimes the extension of the folder shows in the UI, so make it unique-ish e.g. “mchyzerWikiEtc”
- In “etc”, make an admins group
  - Sometimes the extension of the group shows in the UI, so make it unique-ish e.g. “mchyzerWikiAdmins”
- Talk to your neighbors, get their name, add them to the wiki admins group


Home › New group
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


Home › Root › test › test_group
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


Home › Root › test › test_group
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

Assign hierarchical privs to wiki folder

- Go to wiki folder
- On the “More” tab
- Click “privileges inherited to objects in folder”
- Add
- Find your wiki admins group
- Assign to all types: ADMIN
- Create a wikiGroups folder under “wiki” (organize things)
- Create a wikiUsers group in wikiGroups
- Have your neighbor verify that they can add/remove members to that group
  - note, everyone’s an admin so not a good test

Turn the group into include/exclude

- This is for groups with a systemOfRecord, and includes list, and excludes list
- This used to be easier in the outdated “Admin UI”
- There will soon be an easier process in the “New UI”
- Find the mchyzerWikiUsers group
- More Actions -> Attribute assignments
- Add: legacyGroupType_addIncludeExclude
- Save
- Browse the mchyzerWikiGroups folder

wikiGroups

Edit folder

More actions

More

Folder contents | Privileges | More

Filter for: Folder, group, or attribute name | Apply filter | Reset

Name
Up one folder
wikiUsers
wikiUsers excludes
wikiUsers includes
wikiUsers system of record
wikiUsers system of record and includes

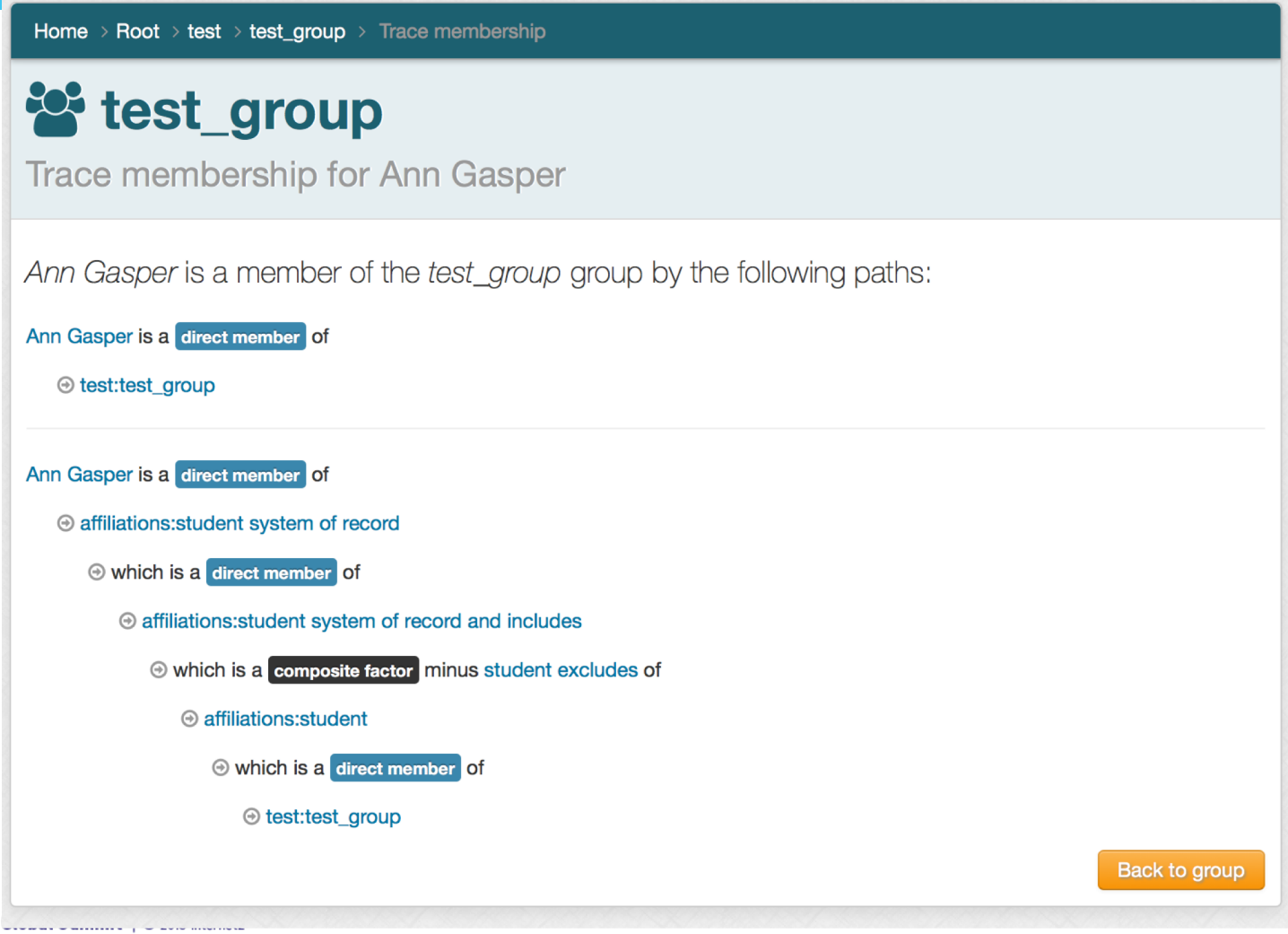
Show: 50

Showing 1-5 of 5 · First | Prev | Next | Last

Go back to New UI, analyze membership

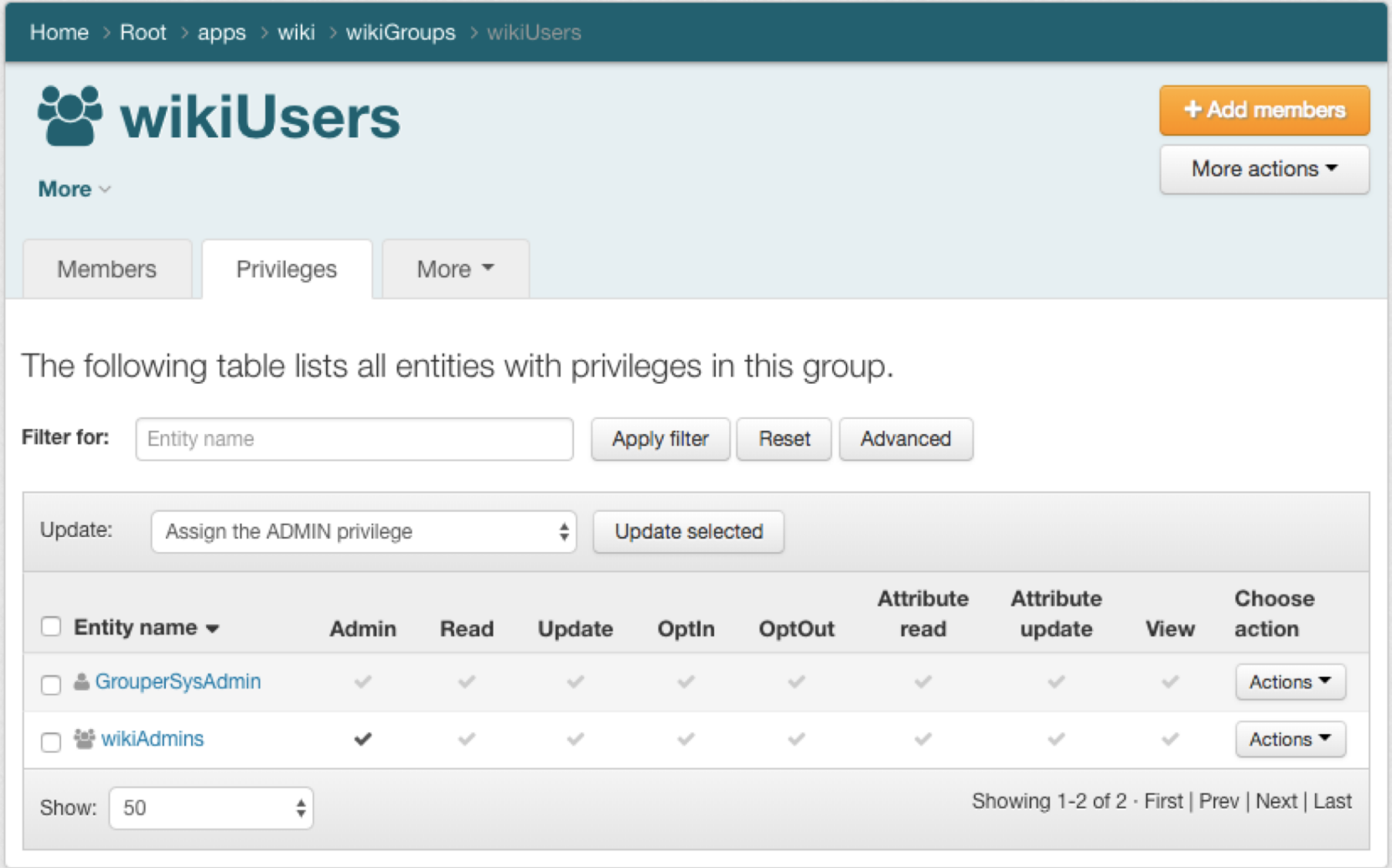
- Go to overall group
- See a membership
  - If none there, then add one to the system of record
- Actions -> trace membership

CC BY NC


Home › Root › test › test_group › Trace membership
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

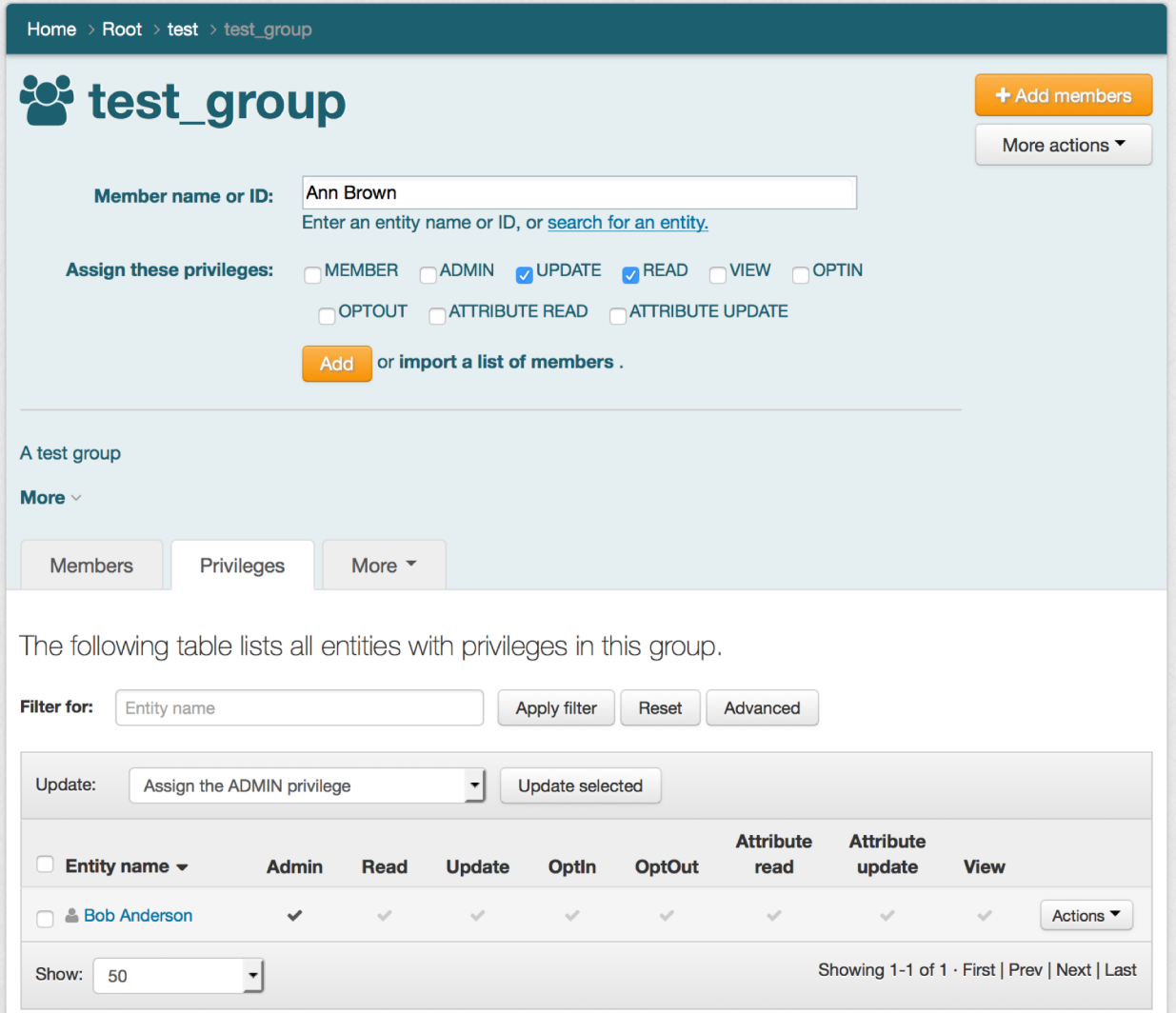
Look at the direct and indirect privileges

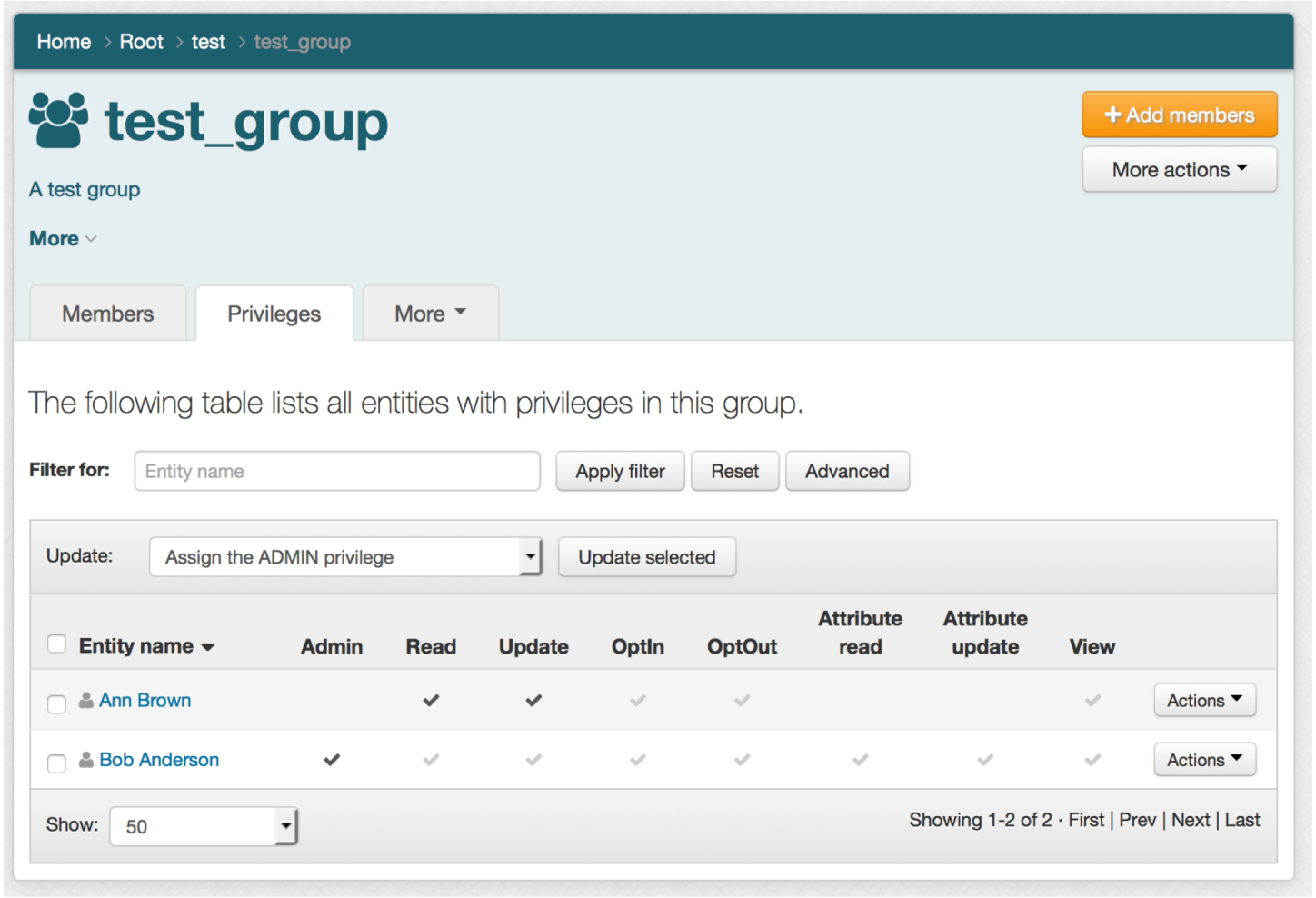
- Go to mchyzerWikiUsers
- Click on the privileges tab
- Dark checkboxes are direct assignments
- Light checkboxes are inherited


Home › Root › apps › wiki › wikiGroups › wikiUsers
wikiUsers
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
Choose action
GrouperSysAdmin
wikiAdmins
Actions
Actions
Show:
50
Showing 1-2 of 2 · First | Prev | Next | Last

Privileges best practices

- Generally privileges should be assigned to groups
- Generally privileges should be inherited
  - Can be inherited due to group in group
  - Can be inherited due to privilege inheritance (e.g. READ implies VIEW. If you can READ a group you can VIEW it)
- Decide which privileges should be system-wide
  - Can everyone VIEW which groups exist?
  - Can everyone READ memberships for all groups?
- Add a direct privilege for someone or a 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

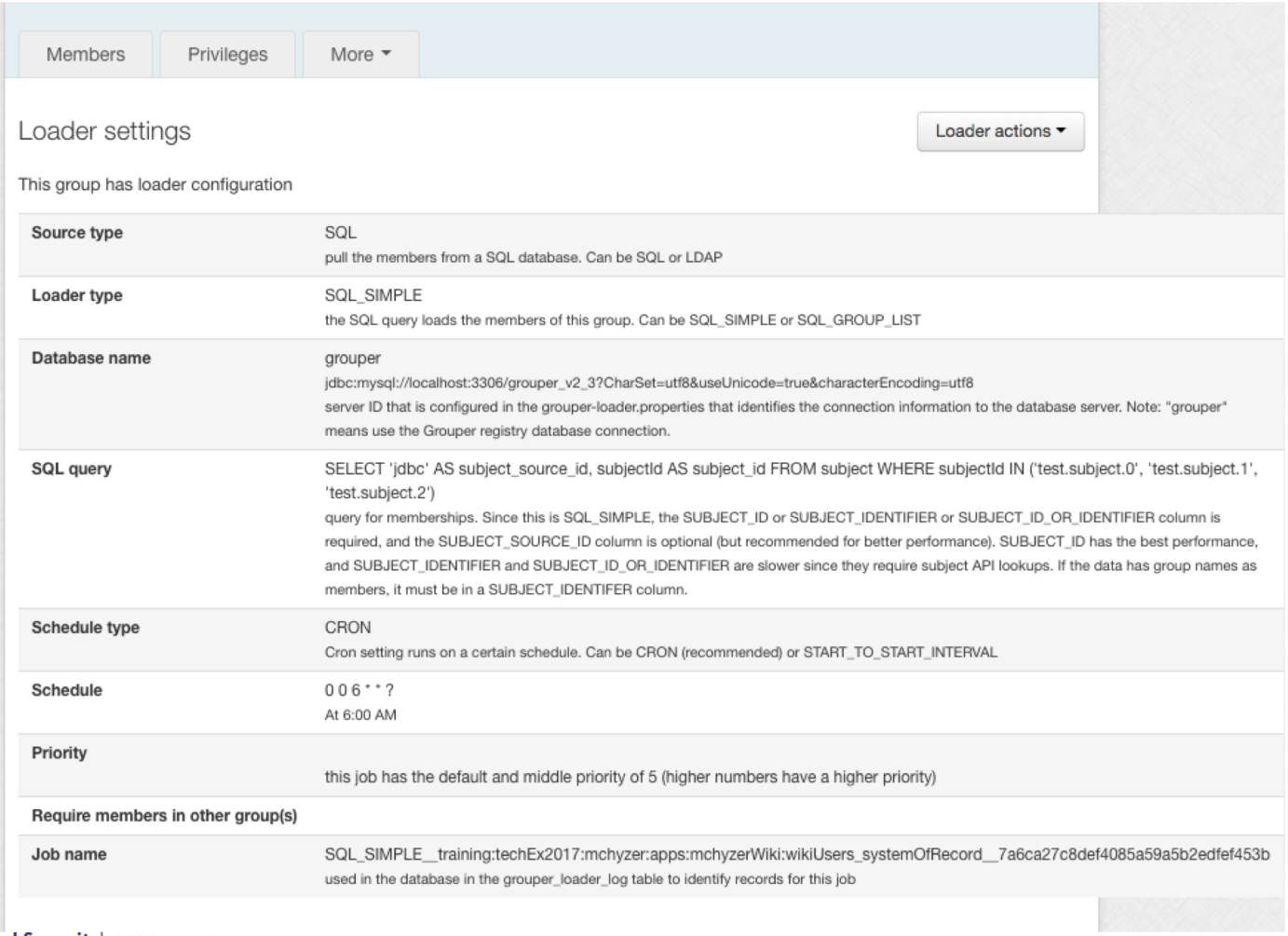

Home › Root › test › test_group
test_group
A test group
More
+ Add members
More actions
Members
Privileges
More
The following table lists all entities with privileges in this group.
Filter for:
Entity name
Apply filter
Reset
Advanced
Update:
Assign the ADMIN privilege
Update selected
Entity name
Admin
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

Go to system of record, make loader

- Go to wiki system of record group
- More tab - > Loader
- Edit
- Copy settings from

  https://spaces.internet2.edu/display/Grouper/Grouper+loader+SQL+simple+example

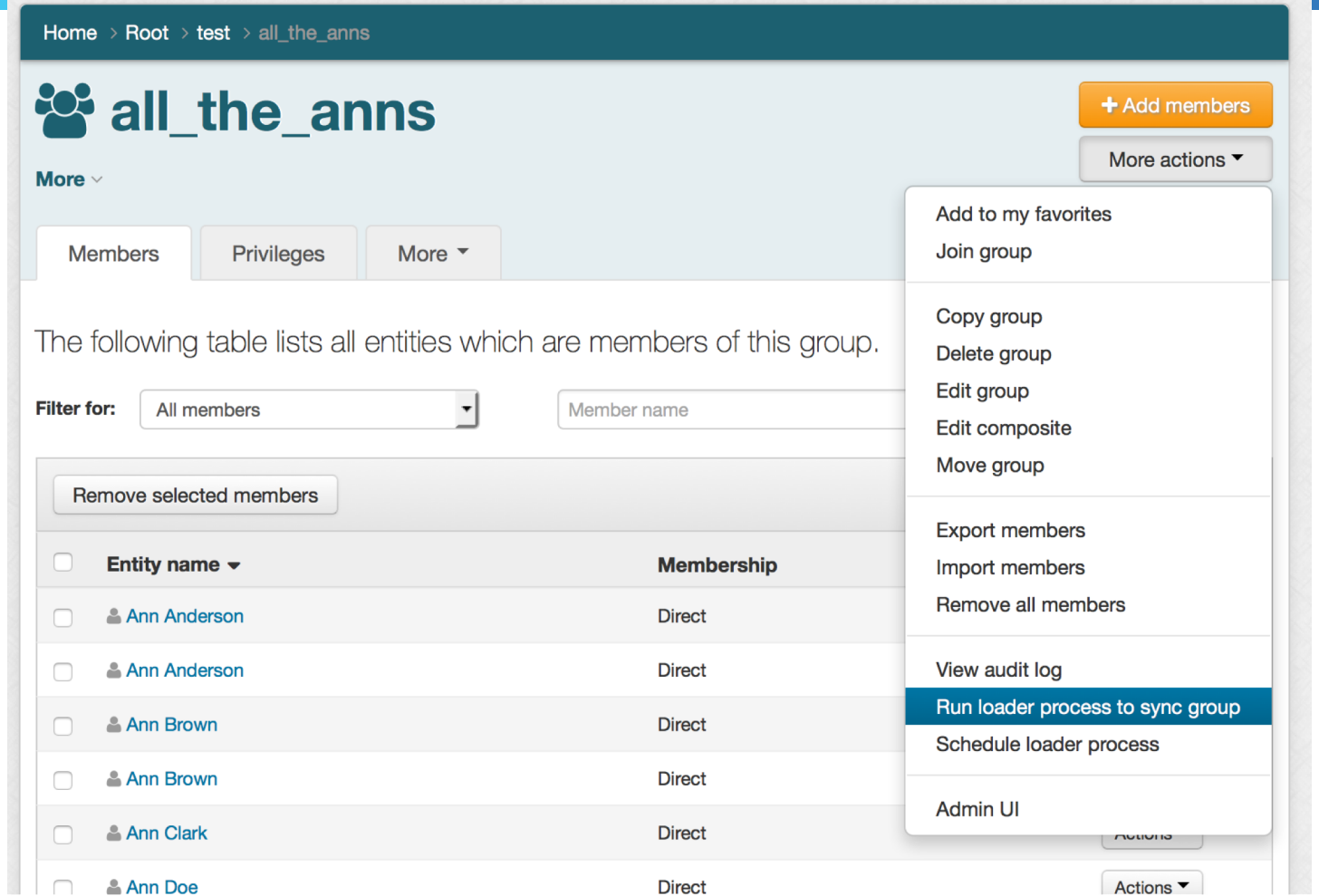
- Can google “grouper loader SQL simple loader”
- SELECT 'jdbc' AS subject_source_id, subjectId AS subject_id FROM subject WHERE subjectId IN ('test.subject.0', 'test.subject.1', 'test.subject.2')


Members
Privileges
More
Loader settings
Loader actions
This group has loader configuration
Source type
SQL
pull the members from a SQL database. Can be SQL or LDAP
Loader type
SQL_SIMPLE
the SQL query loads the members of this group. Can be SQL_SIMPLE or SQL_GROUP_LIST
Database name
grouper
jdbc:mysql://localhost:3306/grouper_v2_3?CharSet=utf8&useUnicode=true&characterEncoding=utf8
server ID that is configured in the grouper-loader.properties that identifies the connection information to the database server. Note: "grouper" means use the Grouper registry database connection.
SQL query
SELECT 'jdbc' AS subject_source_id, subjectId AS subject_id FROM subject WHERE subjectId IN ('test.subject.0', 'test.subject.1', 'test.subject.2')
query for memberships. Since this is SQL_SIMPLE, the SUBJECT_ID or SUBJECT_IDENTIFIER or SUBJECT_ID_OR_IDENTIFIER column is required, and the SUBJECT_SOURCE_ID column is optional (but recommended for better performance). SUBJECT_ID has the best performance, and SUBJECT_IDENTIFIER and SUBJECT_ID_OR_IDENTIFIER are slower since they require subject API lookups. If the data has group names as members, it must be in a SUBJECT_IDENTIFER column.
Schedule type
CRON
Cron setting runs on a certain schedule. Can be CRON (recommended) or START_TO_START_INTERVAL
Schedule
0 0 6 * * ?
At 6:00 AM
Priority
this job has the default and middle priority of 5 (higher numbers have a higher priority)
Require members in other group(s)
Job name
SQL_SIMPLE__training:techEx2017:mchyzer:apps:mchyzerWiki:wikiUsers_systemOfRecord__7a6ca27c8def4085a59a5b2edfef453b
used in the database in the grouper_loader_log table to identify records for this job

Run loader features

- Schedule the job
- Run the job
- Run diagnostics
- See members
- See overall members
- Add one of them to the excludes group
- See the overall group

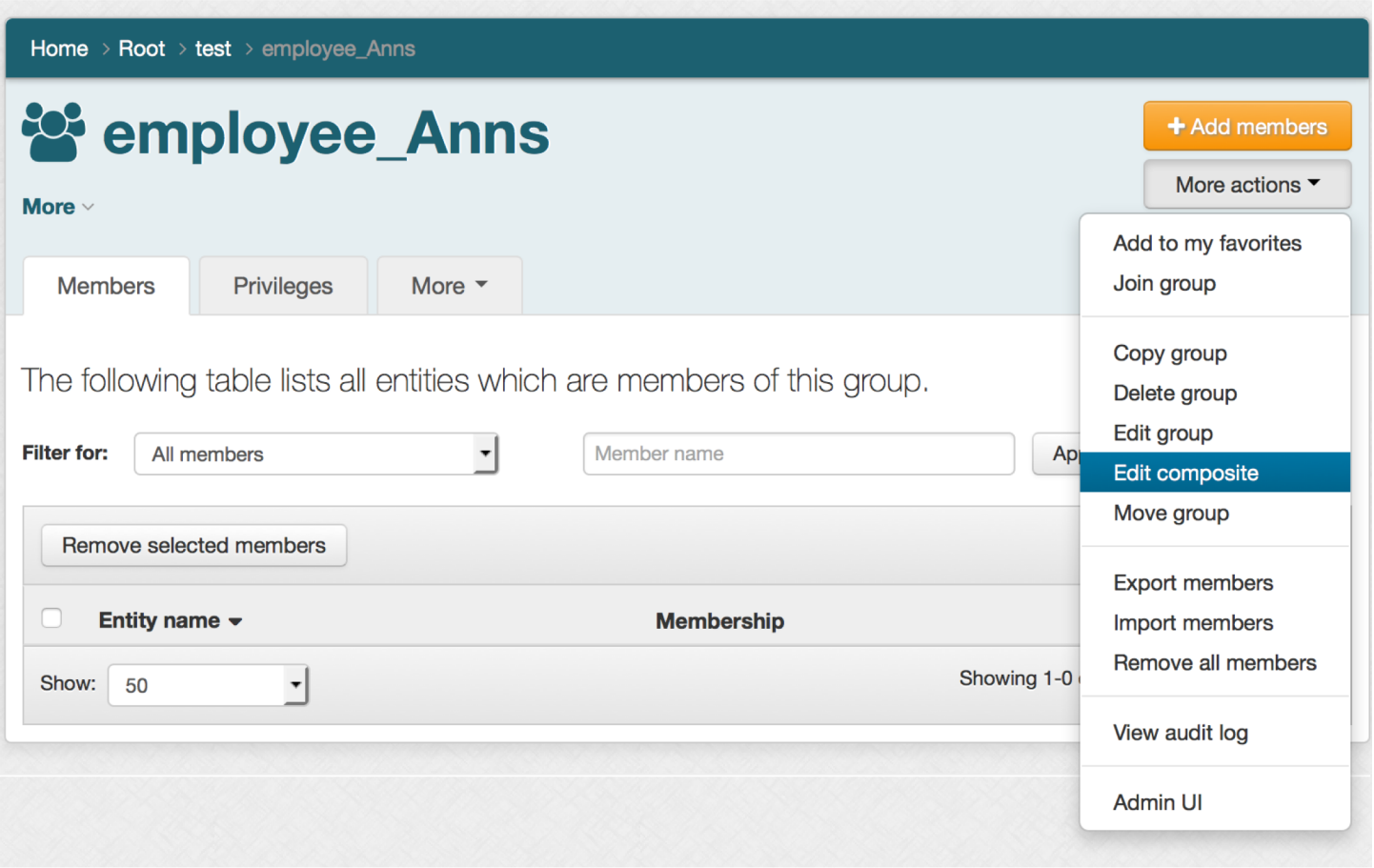
CC BY NC

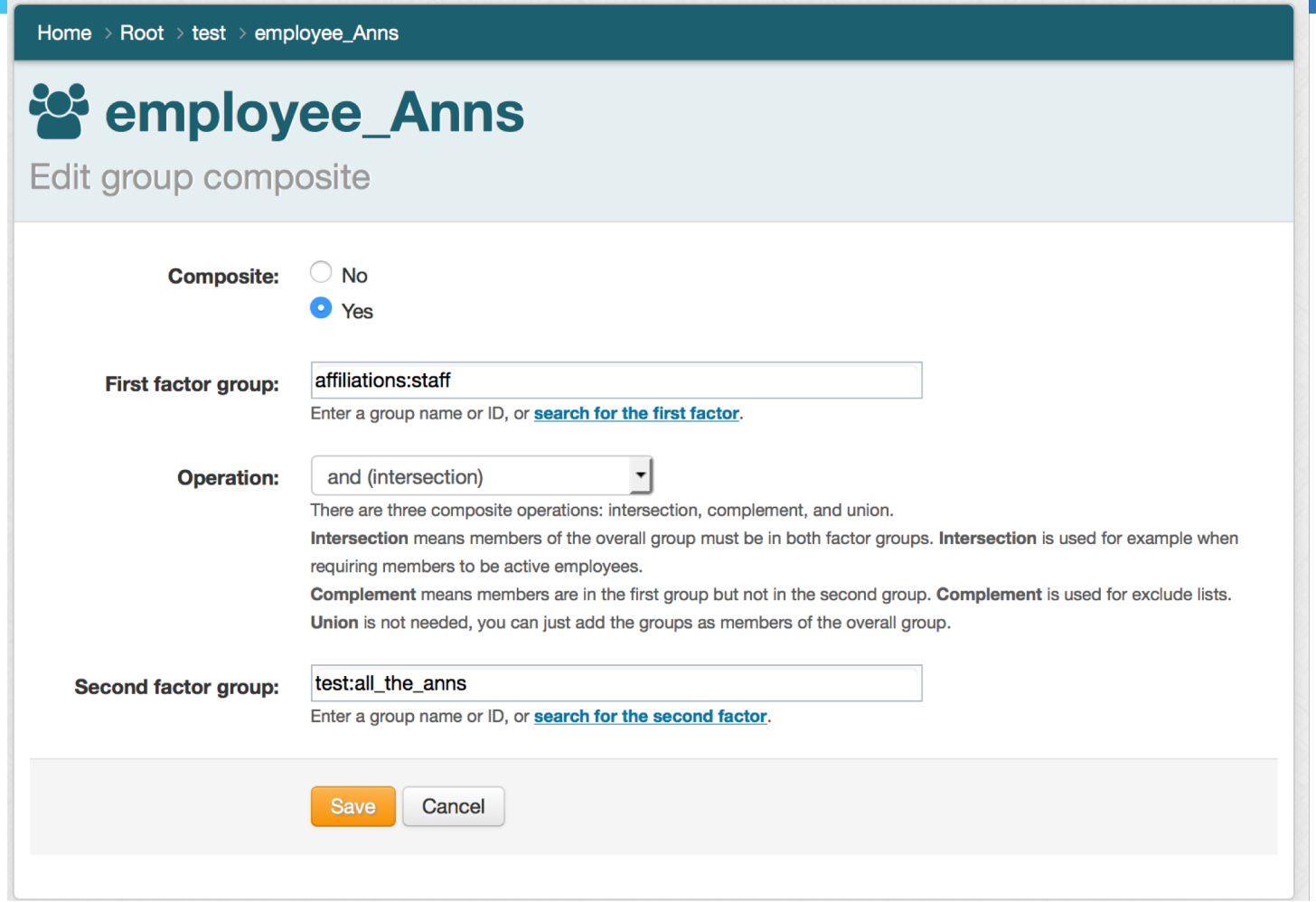

Home › Root › test › all_the_anns
all_the_anns
+ Add members
More actions
More
Members
Privileges
More
The following table lists all entities which are members of this group.
Filter for:
All members
Member name
Remove selected members
Entity name
Membership
Ann Anderson
Direct
Ann Anderson
Direct
Ann 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

See composite

- Go to some of the groups
- More actions, edit composite
- Dont make changes, but see which groups are composites
- Draw out how the groups are related
- Which takes precedence, includes or excludes
  - I.e. if someone were in both, would they be in the overall?

 | © 2018 Internet2


Home > Root > test > employee_Anns
employee_Anns
More
+ Add members
More 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
Admin UI
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
Show:
50
Showing 1-0


Home > Root > test > employee_Anns
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

Make the excludes group attestable

- Go to the excludes group
- More actions -> attestation
- Edit attestation
- Yes, has attestation
- Dont set as attested (or clear it afterwards if you set it)
- Save
- Should say needs attestation
- Maybe you will get an email
  - If you registered your credential with an email address

See more attestation screens

- Global attestation
- Global settings
- Folder attestation
- Folder settings
- Group audit history
- Set an attestation
- See the history again
- Go to Lite UI and see attributes

View or assign attributes

Filter or assign attributes

Owner type: * Group

Attribute definition:

Attribute name: Grouper Administration:attribute:attestation:attestation

Owner group:

Enabled / disabled: Enabled only

Filter Assign

Attribute assignments

	Owner group	Attribute name	Enabled?	Assignment values	Attribute definition	Assignment UUID
	testB	attestation	enabled		attestationDef	0084f...
Metadata on assignment		attestationLastEmailedDate	enabled	2017/10/15	attestationValueDef	95145...
	inheritAttestGroup	attestation	enabled		attestationDef	170b0...
Metadata on assignment		attestationCalculatedDaysLeft	enabled	0	attestationValueDef	24ed6...
Metadata on assignment		attestationDirectAssignment	enabled	false	attestationValueDef	c45d4...
Metadata on assignment		attestationLastEmailedDate	enabled	2017/10/15	attestationValueDef	cb9ad...
	testAttest	attestation	enabled		attestationDef	22f74...
Metadata on assignment		attestationEmailAddresses	enabled		attestationValueDef	0b5e7...
Metadata on assignment		attestationDateCertified	enabled	2017/10/15	attestationValueDef	428be...
Metadata on assignment		attestationSendEmail	enabled	true	attestationValueDef	4aa59...
Metadata on assignment		attestationCalculatedDaysLeft	enabled	180	attestationValueDef	8e361...
Metadata on assignment		attestationDaysBeforeToRemind	enabled		attestationValueDef	98e05...
Metadata on assignment		attestationDirectAssignment	enabled	true	attestationValueDef	c83f6...
Metadata on assignment		attestationDaysUntilRecertify	enabled		attestationValueDef	eb6c6...
	overallgroup	attestation	enabled		attestationDef	65381...
Metadata on assignment		attestationLastEmailedDate	enabled	2017/10/15	attestationValueDef	a8e8e...

CC BY NC

Attributes

- Attributes have two parts
  - Definition
  - Name
- Each part is an object in the Grouper folder namespace
- Anyone who can create objects in a folder can create and use attributes
- Definition
  - Privileges
  - Settings
- Name
  - What is assigned to an object

CC BY NC

Attribute assignments

- An attribute name assigned to an owners is an attribute assignment
- Owner can be:
  - Group, folder, entity, membership (direct or indirect), attribute definition
  - You can also assign attributes to attributes assignments one level deep
- An attribute assignment can have 0, 1, or many values
- Multi-assign vs multi-value

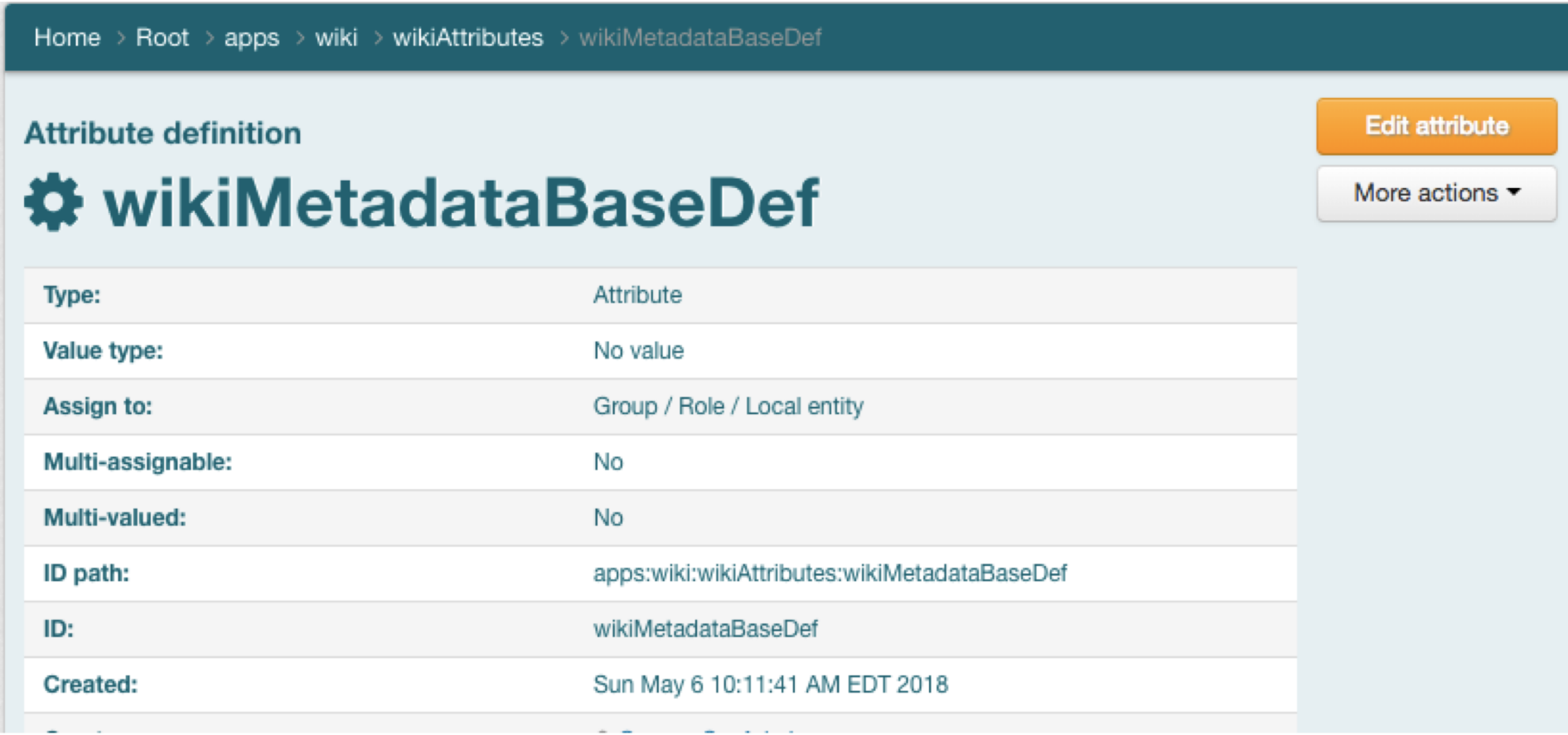
“Set of values” attribute pattern

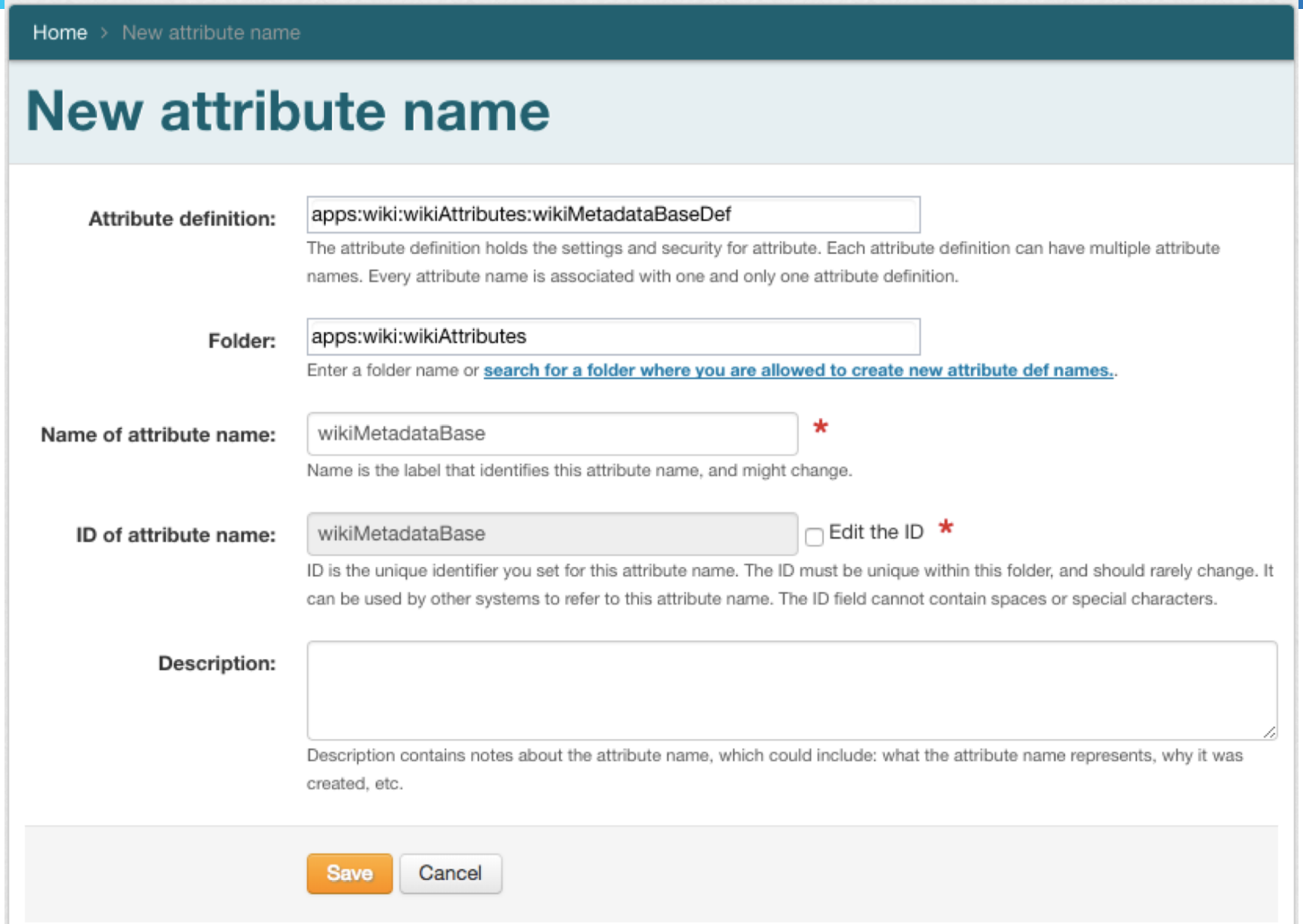
- When we have a set of values
- Generally we have two attribute definitions
  - Base definition single assigned to owner (e.g. group), marker
    - Base definition has one name
  - Value definition is single assigned to group assignments, string
    - Has multiple names

 | © 2018 Internet2

Create and use some attributes

- We want to store department name and department affiliation on the wiki groups
- Create a folder in the wiki folder: wikiAttributes
- Create an attribute definition: wikiMetadataBaseDef
  - Assignable to groups
  - Marker value type (no value)
- Create an attribute name: wikiMetadataBase
  - Attribute definition: wikiMetadataBaseDef

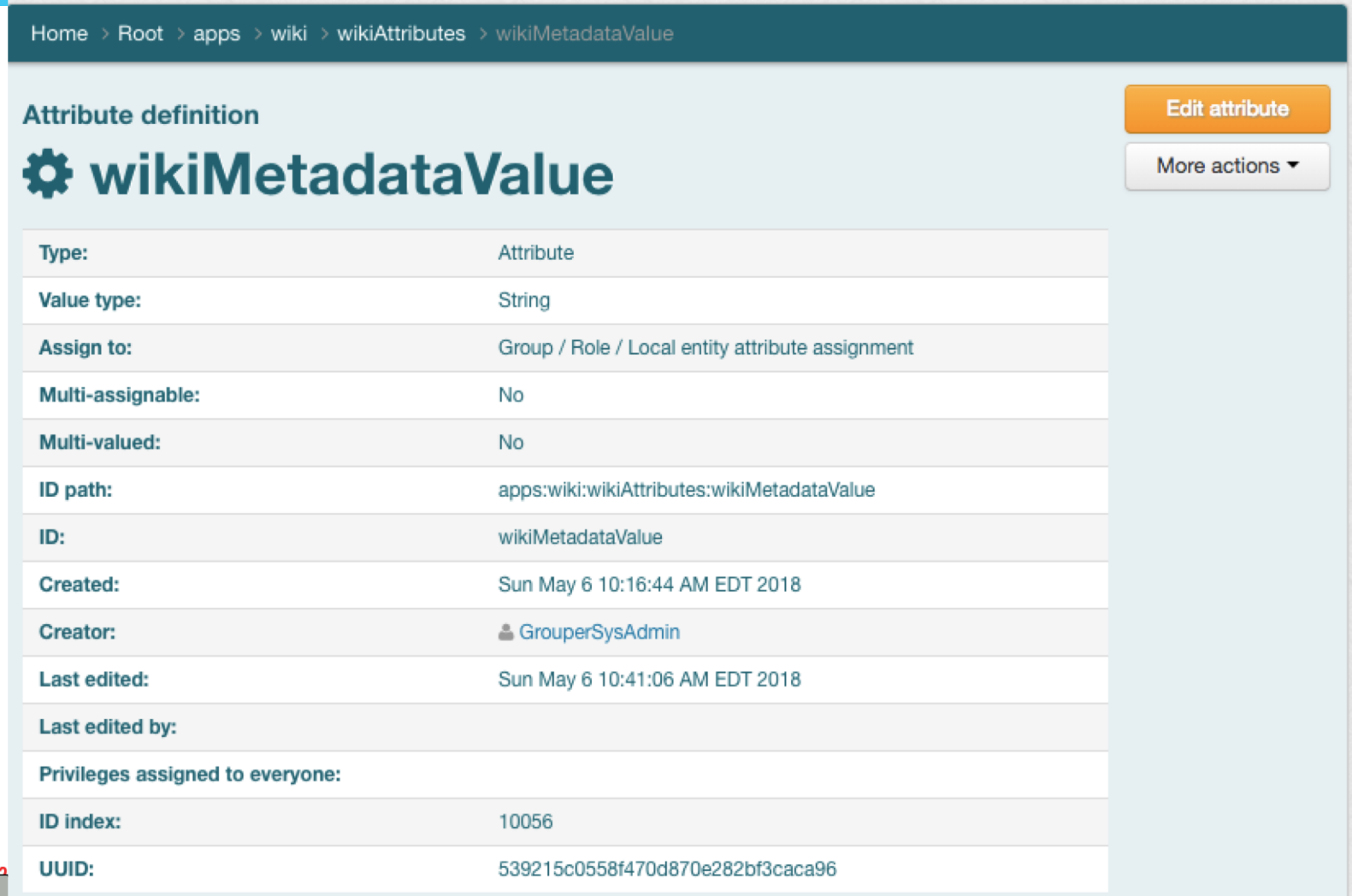

Home › Root › apps › wiki › wikiAttributes › wikiMetadataBaseDef
Attribute definition
wikiMetadataBaseDef
Edit attribute
More actions
Type: Attribute
Value type: No value
Assign to: Group / Role / Local entity
Multi-assignable: No
Multi-valued: No
ID path: apps:wiki:wikiAttributes:wikiMetadataBaseDef
ID: wikiMetadataBaseDef
Created: Sun May 6 10:11:41 AM EDT 2018

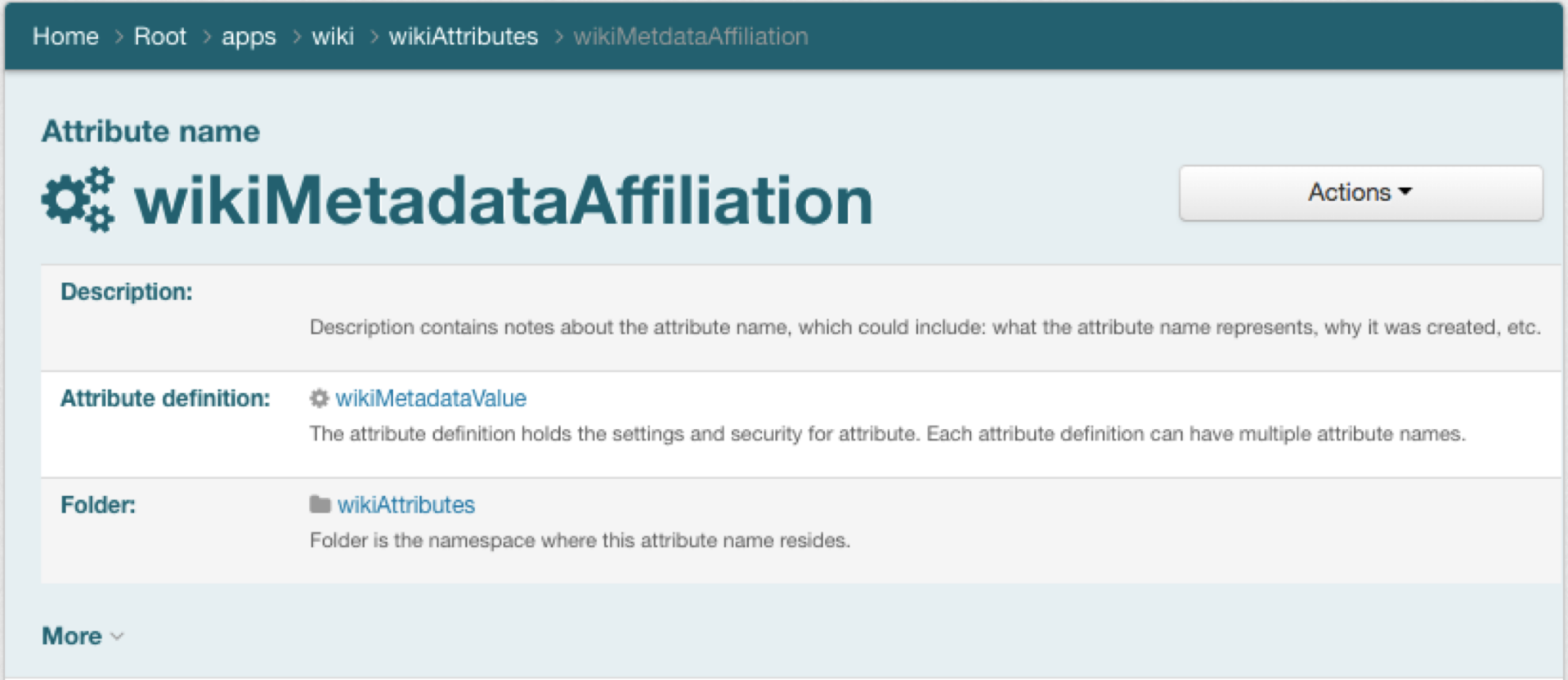

Home › New attribute name
New attribute name
Attribute definition:
apps:wiki:wikiAttributes:wikiMetadataBaseDef
The attribute definition holds the settings and security for attribute. Each attribute definition can have multiple attribute names. Every attribute name is associated with one and only one attribute definition.
Folder:
apps:wiki:wikiAttributes
Enter a folder name or search for a folder where you are allowed to create new attribute def names..
Name of attribute name:
wikiMetadataBase
*
Name is the label that identifies this attribute name, and might change.
ID of attribute name:
wikiMetadataBase
Edit the ID
*
ID is the unique identifier you set for this attribute name. The ID must be unique within this folder, and should rarely change. It can be used by other systems to refer to this attribute name. The ID field cannot contain spaces or special characters.
Description:
Description contains notes about the attribute name, which could include: what the attribute name represents, why it was created, etc.
Save
Cancel

CC BY NC

Create metadata attributes

- Create an attribute definition: wikiMetadataValue
  - Assignable to group assignments
  - String value
  - Single assign, single value
- Create an attribute name: wikiMetadataDepartment
  - Attribute definition: wikiMetadataValue
- Create an attribute name: wikiMetadataAffiliation
  - Attribute definition: wikiMetadataValue


Home › Root › apps › wiki › wikiAttributes › wikiMetadataValue
Attribute definition
wikiMetadataValue
Edit attribute
More actions
Type: Attribute
Value type: String
Assign to: Group / Role / Local entity attribute assignment
Multi-assignable: No
Multi-valued: No
ID path: apps:wiki:wikiAttributes:wikiMetadataValue
ID: wikiMetadataValue
Created: Sun May 6 10:16:44 AM EDT 2018
Creator: GrouperSysAdmin
Last edited: Sun May 6 10:41:06 AM EDT 2018
Last edited by:
Privileges assigned to everyone:
ID index: 10056
UUID: 539215c0558f470d870e282bf3caca96


Home › Root › apps › wiki › wikiAttributes › wikiMetdataAffiliation
Attribute name
wikiMetadataAffiliation
Actions
Description:
Description contains notes about the attribute name, which could include: what the attribute name represents, why it was created, etc.
Attribute definition:
wikiMetadataValue
The attribute definition holds the settings and security for attribute. Each attribute definition can have multiple attribute names.
Folder:
wikiAttributes
Folder is the namespace where this attribute name resides.
More

CC BY NC

Assign attributes and values

- Open the wikiUsers group
- Click More actions -> Attribute assignments
- Assign the wikiMetadataBase attribute
- Assign metadata on assignments
- Assign the wikiMetadataDepartment attribute
  - Assign “math” as the value
- Assign the wikiMetadataAffiliation attribute
  - Assign ”faculty” as the value

Home > Root > apps > wiki > wikiGroups > wikiUsers

wikiUsers

More actions

Group containing list of wikiUsers after adding the includes and subtracting the excludes

More

Members | Privileges | More

Attribute assignments

+ Assign attribute

The following table lists all attributes assigned to this group

Assignment type	Attribute name	Enabled?	Assignment values	Attribute definition	Choose action
Direct assignment	wikiMetadataBase	enabled		wikiMetadataBaseDef	Actions
Metadata on assignment	wikiMetadataDepartment	enabled	math	wikiMetdataValue	Actions
Metadata on assignment	wikiMetadataAffiliation	enabled	faculty	wikiMetdataValue	Actions
Direct assignment	legacyGroupType_addIncludeExclude	enabled		legacyGroupTypeDef_addIncludeExclude	Actions

Permissions

- Groups identify a set of entities
- The application is use that to mean what the people can do
- Can make it more dynamic with Grouper permissions
- Another level of access management maturity

 | © 2018 Internet2

What is a permission?

- Attribute name (ahem: permission name)
- Assignable only to:
  - Role
    - Special type of group
    - Can have role inheritance
  - Entity
    - In the context of a role
    - If the user loses the role, they lose the permission

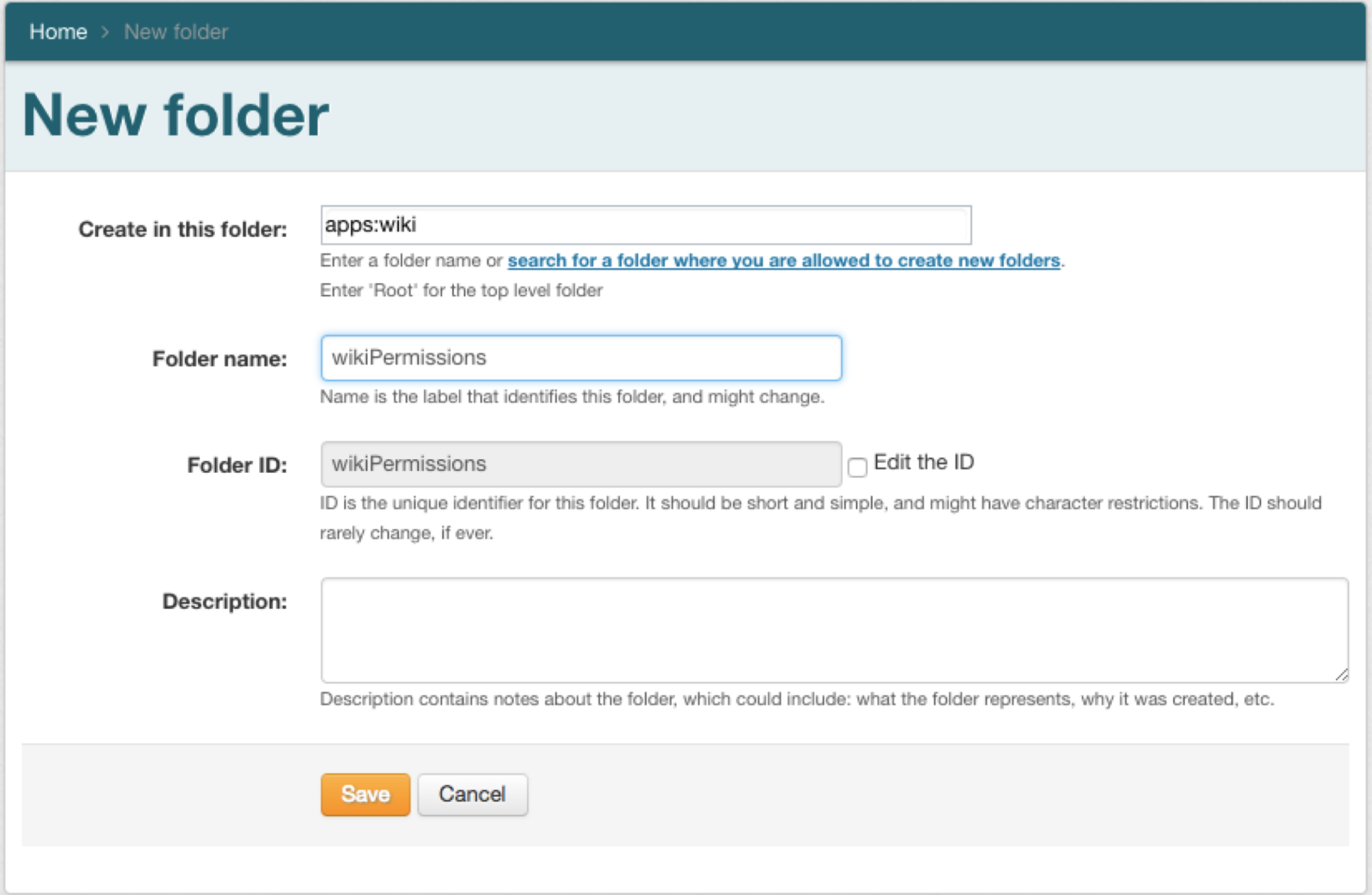
What is a permission? (continued)

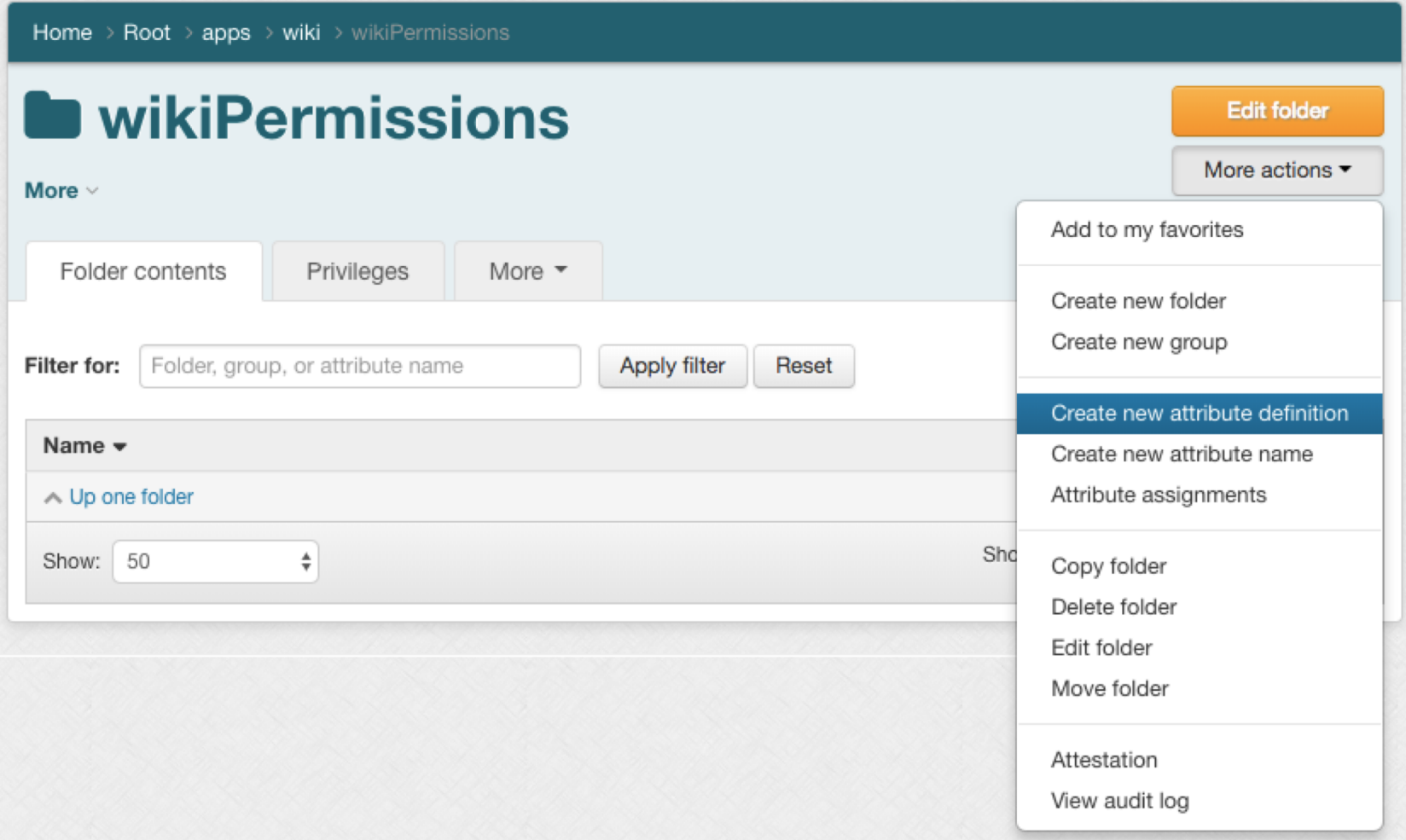
- Permissions are a three part assignment
  - Has an action (e.g. read, write, admin)
- Instead of asking Grouper if a user is a wiki user, ask if the user can login
- Permissions can have limits
  - Metadata on permission assignments
  - E.g. only at certain times of day
  - E.g. only a certain max dollar amount

 | © 2018 Internet2

Create some permissions

- Create a wikiPermissions folder in the wiki folder
- Create a wikiPermissionDef in that folder
  - Type of permission
  - Assignable to role and membership
  - Permissions cannot have a value, so “No value”


Home > New folder
New folder
Create in this folder:
apps:wiki
Enter a folder name or search for a folder where you are allowed to create new folders.
Enter 'Root' for the top level folder
Folder name:
wikiPermissions
Name is the label that identifies this folder, and might change.
Folder ID:
wikiPermissions
Edit the ID
ID is the unique identifier for this folder. It should be short and simple, and might have character restrictions. The ID should rarely change, if ever.
Description:
Description contains notes about the folder, which could include: what the folder represents, why it was created, etc.
Save
Cancel


Home › Root › apps › wiki › wikiPermissions
wikiPermissions
Edit folder
More actions
More
Add to my favorites
Folder contents
Privileges
More
Create new folder
Create new group
Filter for:
Folder, group, or attribute name
Apply filter
Reset
Create new attribute definition
Create new attribute name
Name
Attribute assignments
Up one folder
Copy folder
Show:
50
Delete folder
Edit folder
Move folder
Attestation
View audit log

New attribute definition

Create in this folder: apps:wiki:wikiPermissions

Enter a folder name or search for a folder where you are allowed to create new attribute definitions.

Attribute definition ID: wikiPermissionDef

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

Description:

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

Type: Permission

Attribute definition type describes the attribute definition. Generally it will be attribute or permission. Type is used for templates, limit describes a permission, and service identifies which application the object refers to.

Assign to:

- [x] Group / Role / Local entity
- [x] Membership

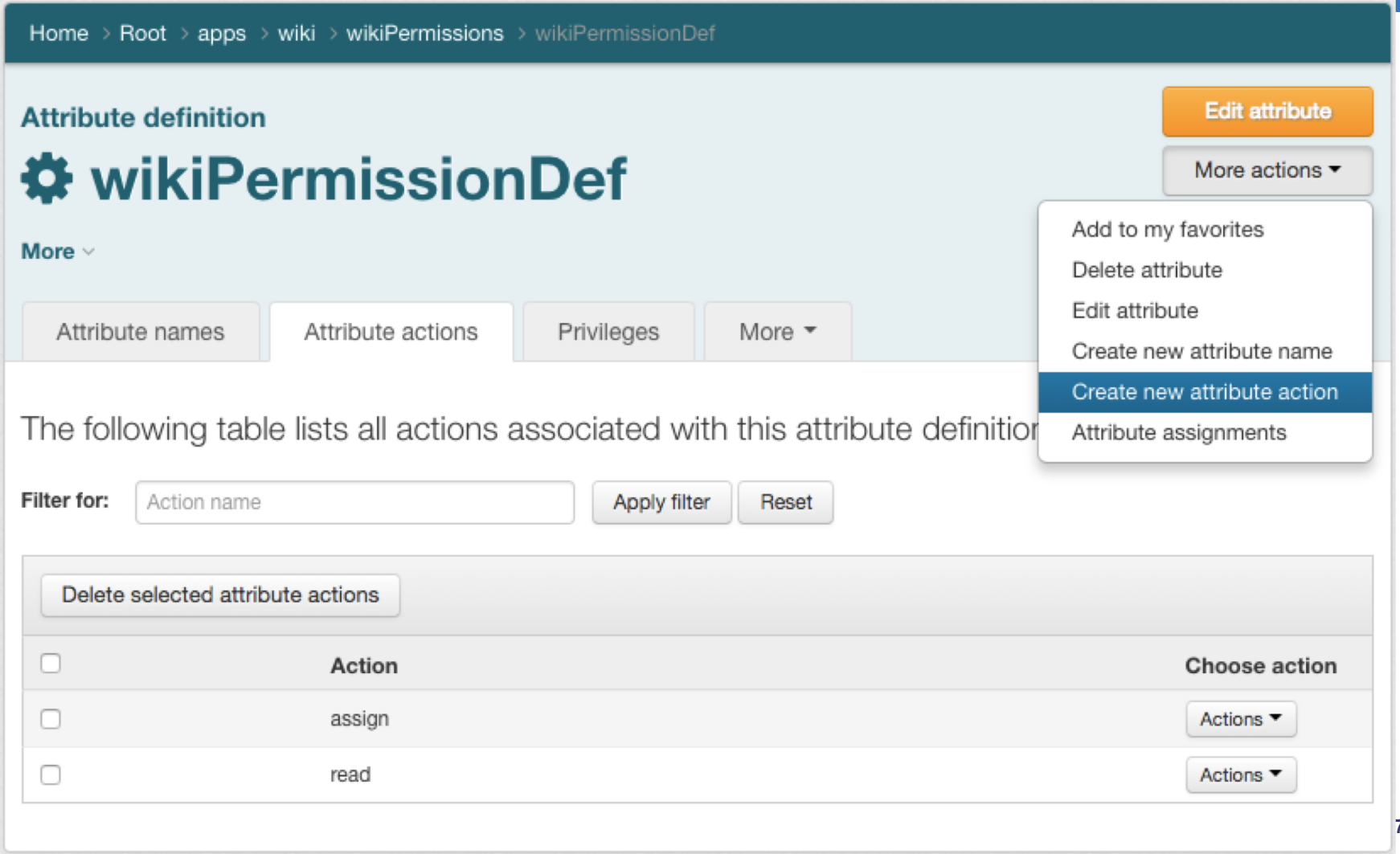
Designate which types of objects that this definition can be assigned to. There are six base object types, or you can assign attributes to the assignment of attributes to those base object types. Membership can be assigned to an immediate or an effective membership, and will still exist as an orphan if the membership is unassigned until the membership is reassigned. Immediate membership attribute assignments are only assignable to immediate memberships and are automatically deleted once the membership is unassigned.

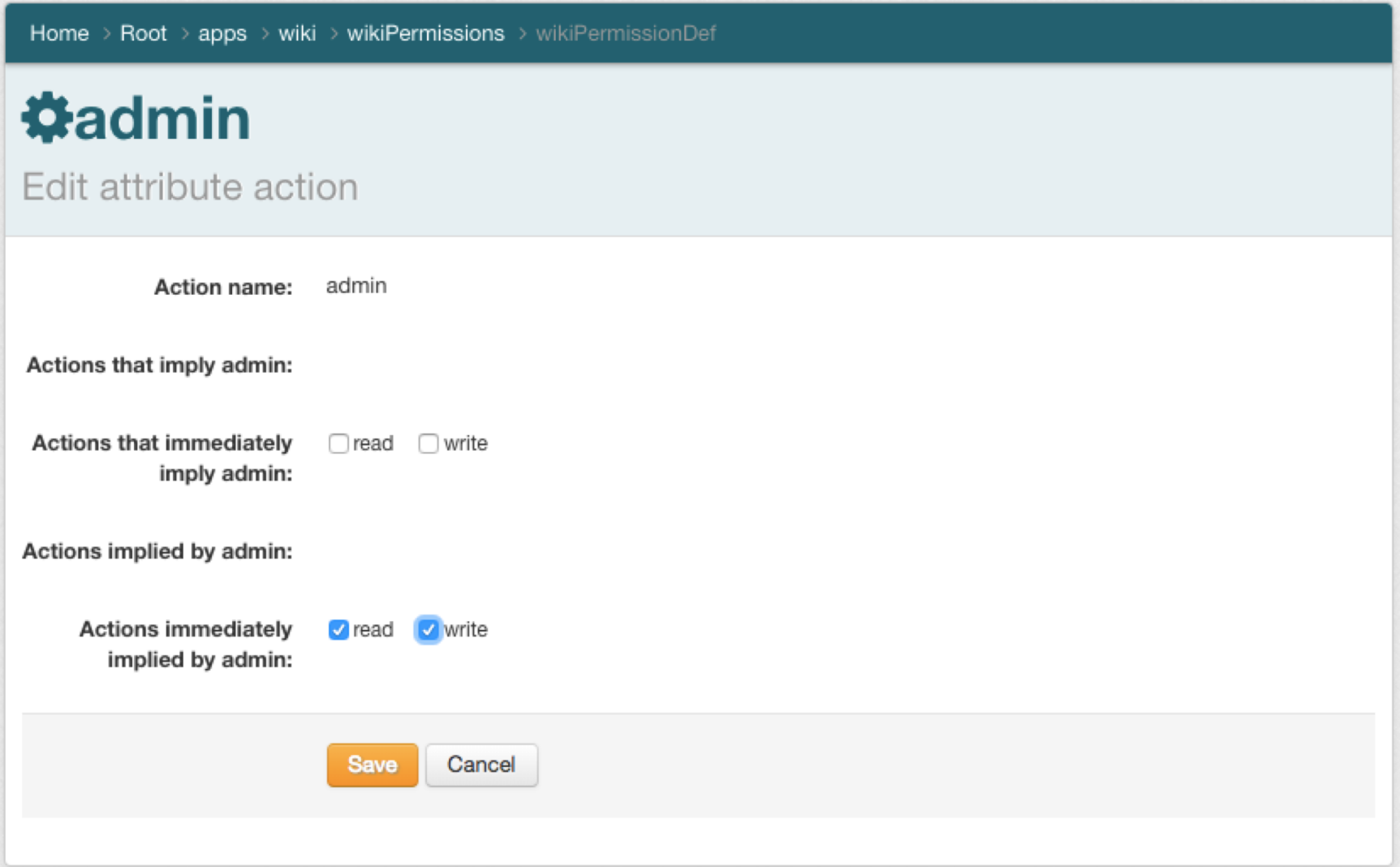
CC BY NC

Create some actions

- Sometimes this will just be a tuple with the “assign” action
- Create some actions:
  - read
  - write
  - admin implies read and write
  - Delete “assign”

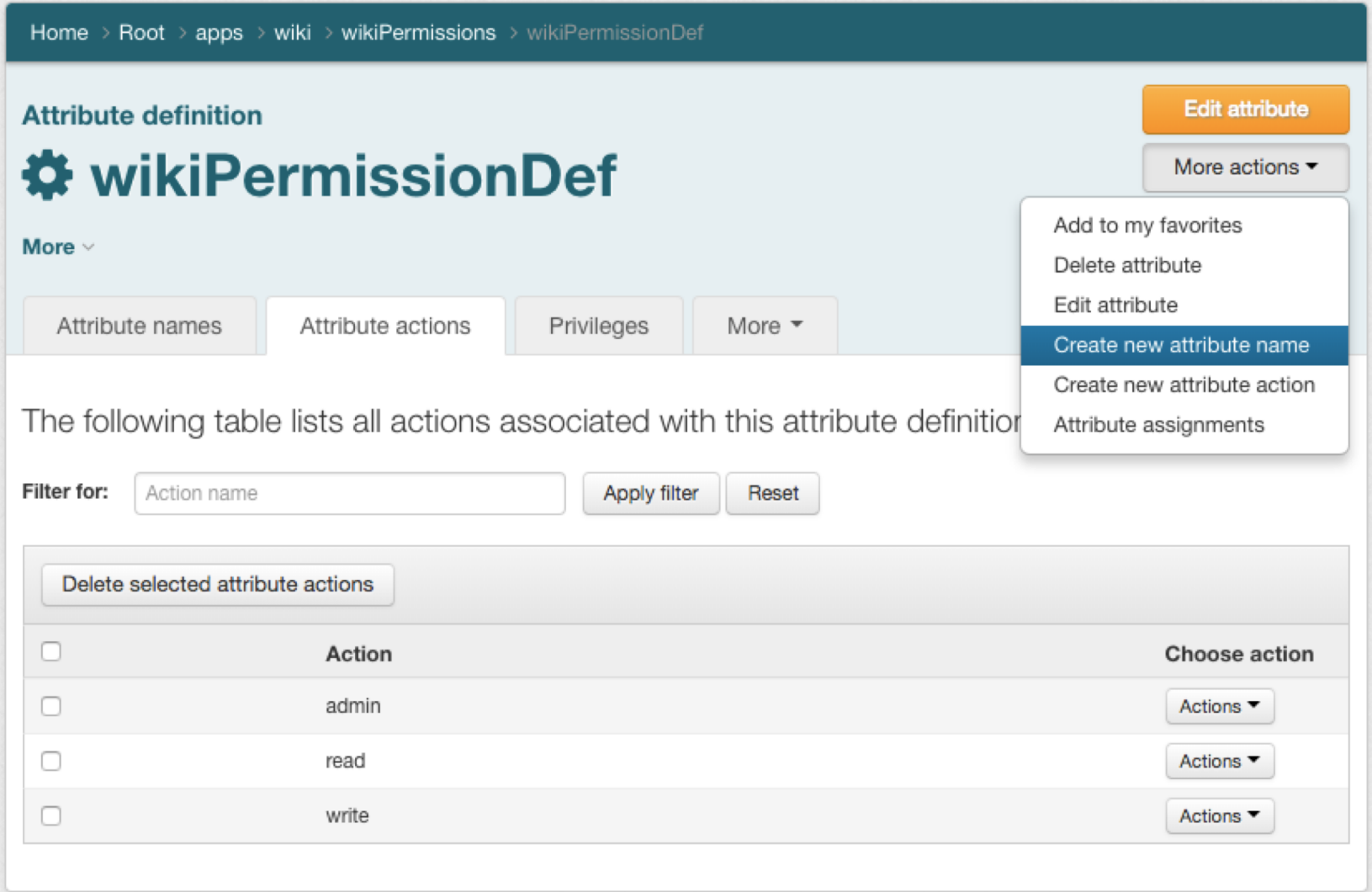
CC BY NC

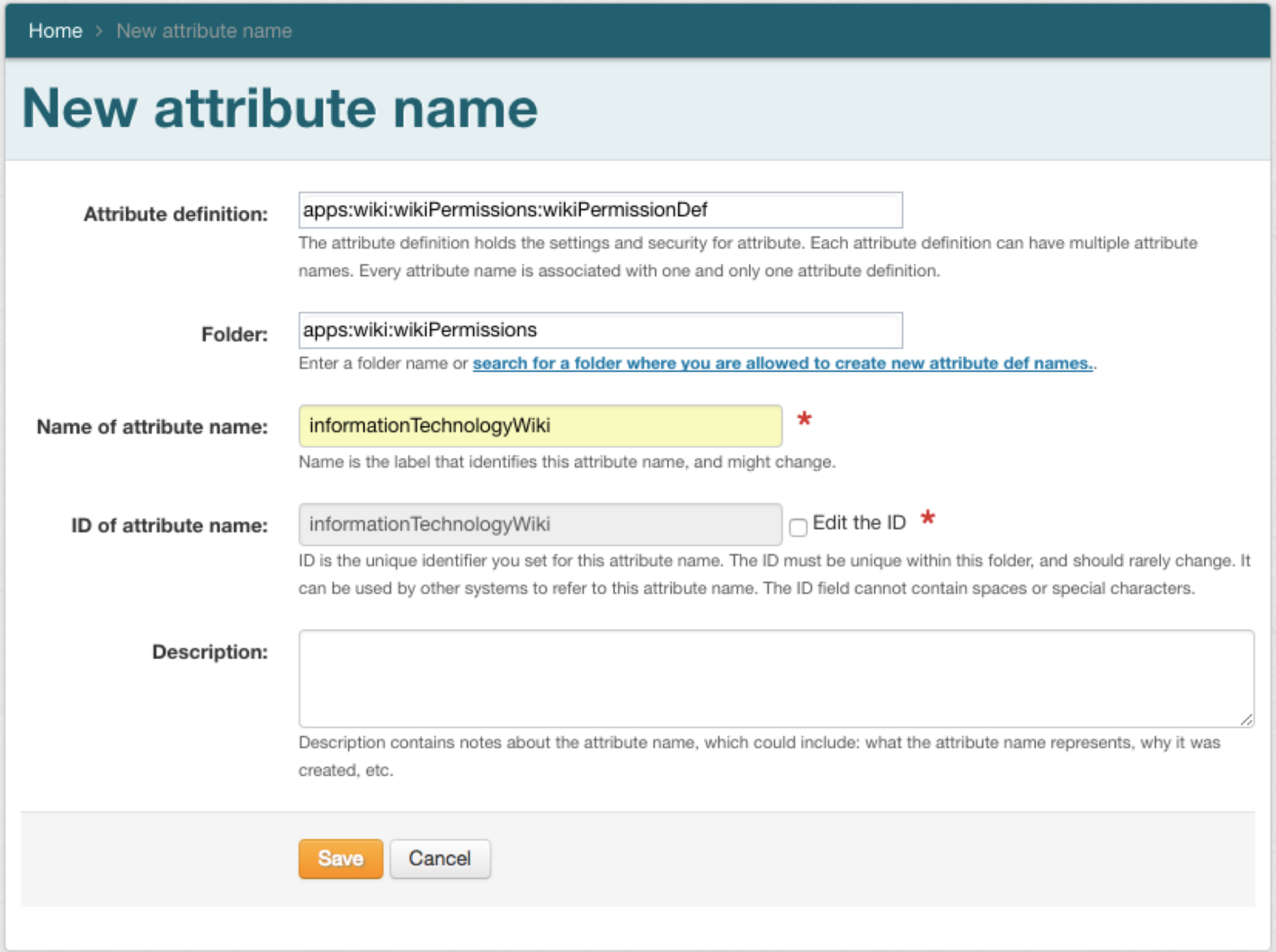

Home › Root › apps › wiki › wikiPermissions › wikiPermissionDef
Attribute definition
wikiPermissionDef
More
Edit attribute
More actions
Add to my favorites
Delete attribute
Edit attribute
Create new attribute name
Create new attribute action
Attribute assignments
Attribute names
Attribute actions
Privileges
More
The following table lists all actions associated with this attribute definitio
Filter for:
Action name
Apply filter
Reset
Delete selected attribute actions
Action
Choose action
assign
Actions
read
Actions


Home › Root › apps › wiki › wikiPermissions › wikiPermissionDef
admin
Edit attribute action
Action name:
admin
Actions that imply admin:
Actions that immediately imply admin:
read
write
Actions implied by admin:
Actions immediately implied by admin:
read
write
Save
Cancel

Make permission names

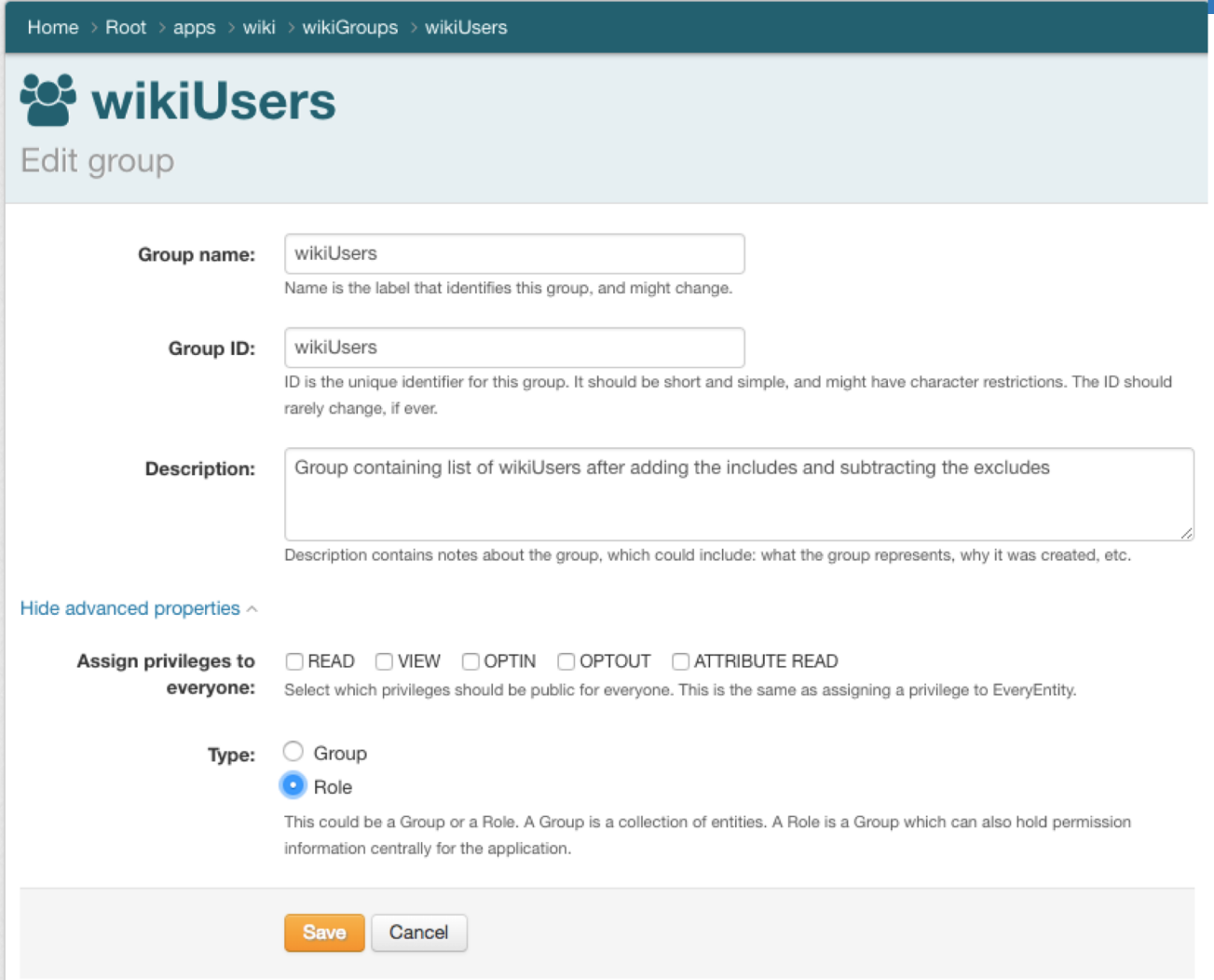
- Permissions in this case represent wikis
- Make one for:
  - mathWiki
  - informationTechnologyWiki


Home › Root › apps › wiki › wikiPermissions › wikiPermissionDef
Attribute definition
wikiPermissionDef
More
Edit attribute
More actions
Add to my favorites
Delete attribute
Edit attribute
Create new attribute name
Create new attribute action
Attribute assignments
Attribute names
Attribute actions
Privileges
More
The following table lists all actions associated with this attribute definitio
Filter for:
Action name
Apply filter
Reset
Delete selected attribute actions
Action
Choose action
admin
Actions
read
Actions
write
Actions


Home › New attribute name
New attribute name
Attribute definition:
apps:wiki:wikiPermissions:wikiPermissionDef
The attribute definition holds the settings and security for attribute. Each attribute definition can have multiple attribute names. Every attribute name is associated with one and only one attribute definition.
Folder:
apps:wiki:wikiPermissions
Enter a folder name or search for a folder where you are allowed to create new attribute def names..
Name of attribute name:
informationTechnologyWiki
*
Name is the label that identifies this attribute name, and might change.
ID of attribute name:
informationTechnologyWiki
Edit the ID
*
ID is the unique identifier you set for this attribute name. The ID must be unique within this folder, and should rarely change. It can be used by other systems to refer to this attribute name. The ID field cannot contain spaces or special characters.
Description:
Description contains notes about the attribute name, which could include: what the attribute name represents, why it was created, etc.
Save
Cancel

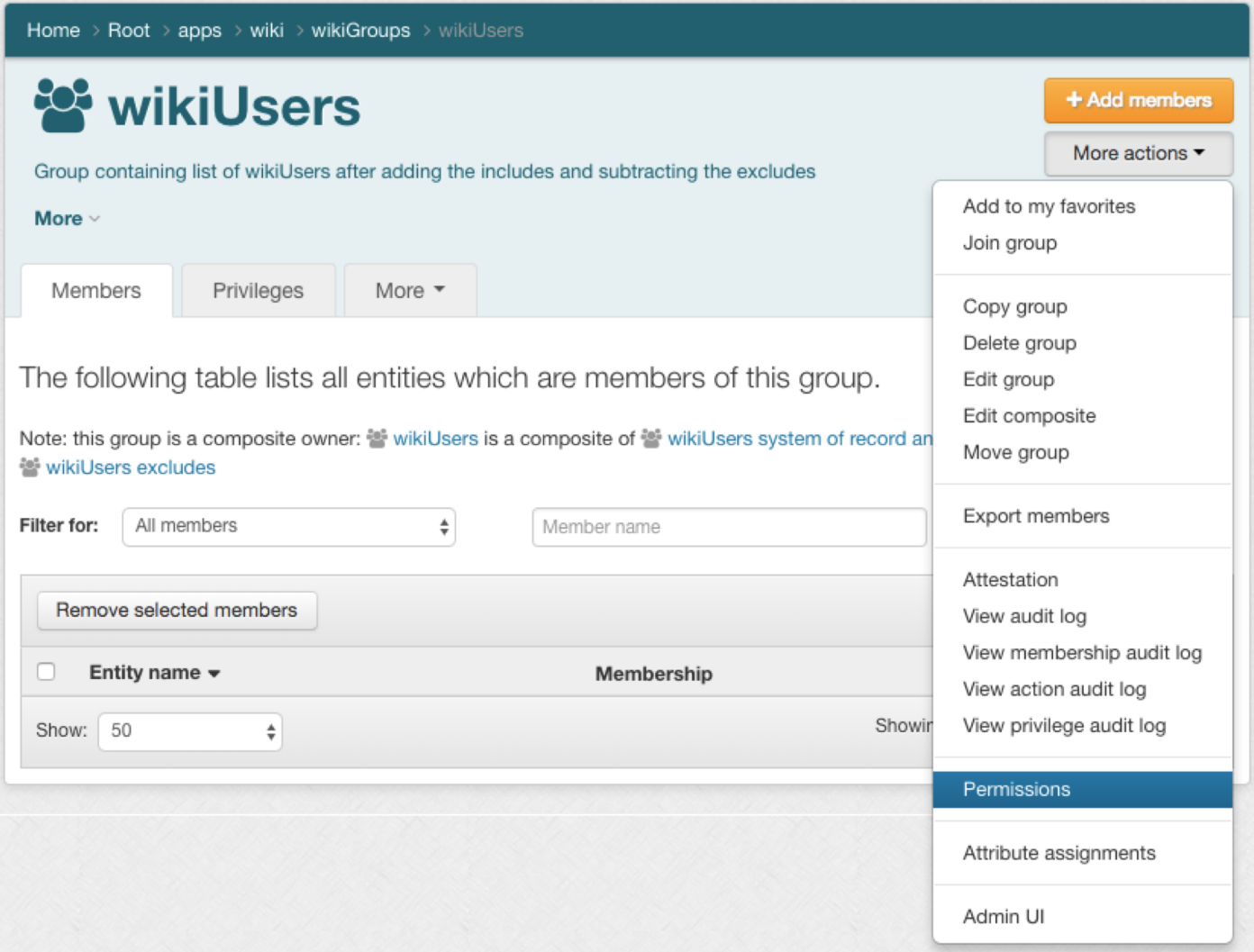
Convert wikiUsers to a role

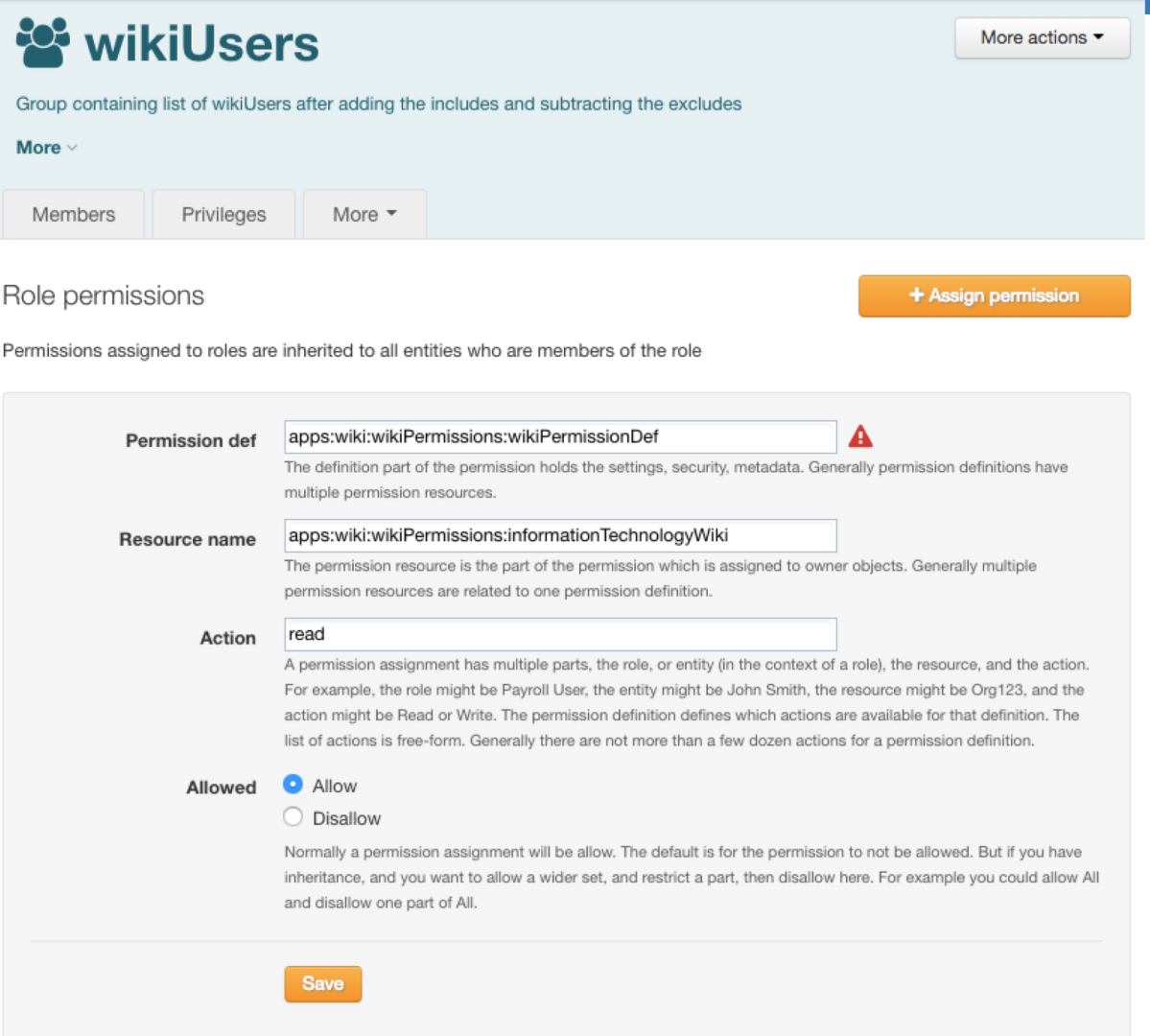
- Go to wikiUsers group
- Edit
- Show advanced properties
- Change to “role” instead of “group”

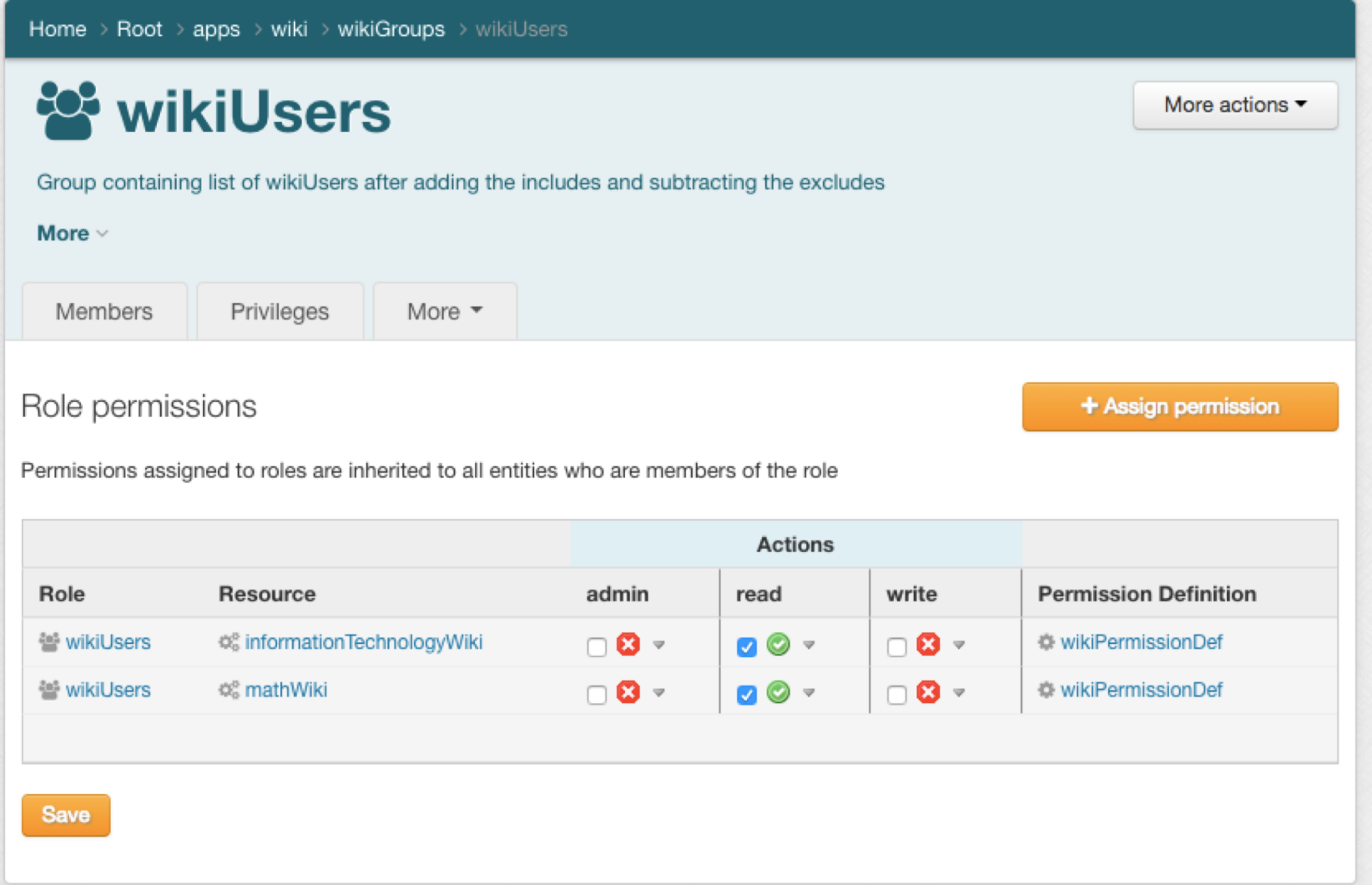

Home › Root › apps › wiki › wikiGroups › wikiUsers
wikiUsers
Edit group
Group name:
wikiUsers
Name is the label that identifies this group, and might change.
Group ID:
wikiUsers
ID is the unique identifier for this group. It should be short and simple, and might have character restrictions. The ID should rarely change, if ever.
Description:
Group containing list of wikiUsers after adding the includes and subtracting the excludes
Description contains notes about the group, which could include: what the group represents, why it was created, etc.
Hide advanced properties
Assign privileges to everyone:
READ VIEW OPTIN OPTOUT ATTRIBUTE READ
Select which privileges should be public for everyone. This is the same as assigning a privilege to EveryEntity.
Type:
Group
Role
This could be a Group or a Role. A Group is a collection of entities. A Role is a Group which can also hold permission information centrally for the application.
Save
Cancel

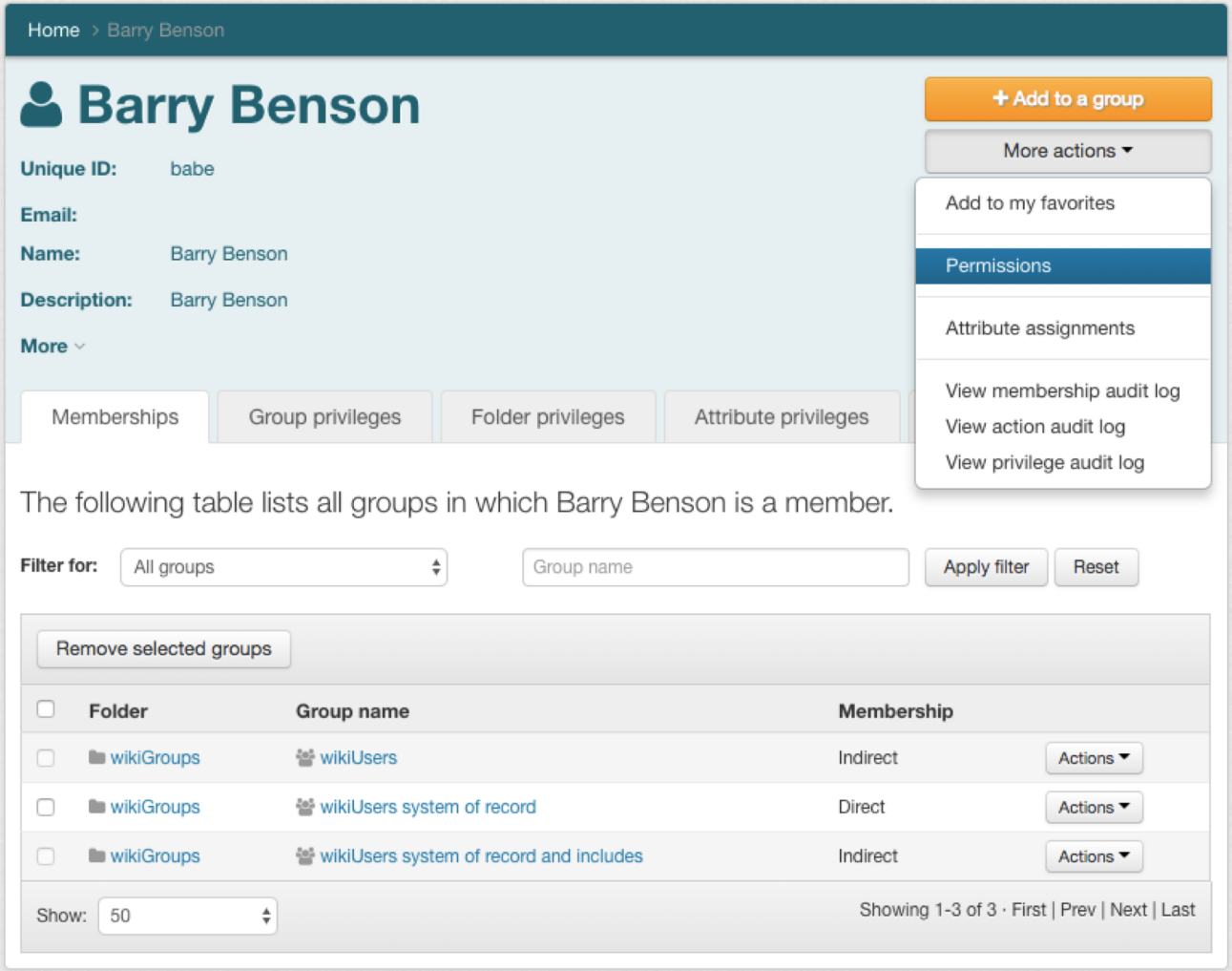
Assign permissions

- Add permissions
  - wikiUsers role can READ all wikis
  - One user in wikiUsers role can ADMIN the informationTechnology wiki
    - Note, the individual permission assignment might currently has an issue when selecting role


Home › Root › apps › wiki › wikiGroups › wikiUsers
wikiUsers
Group containing list of wikiUsers after adding the includes and subtracting the excludes
More
+ Add members
More actions
Add to my favorites
Join group
Copy group
Delete group
Edit group
Edit composite
Move group
Export members
Attestation
View audit log
View membership audit log
View action audit log
View privilege audit log
Permissions
Attribute assignments
Admin UI
Members
Privileges
More
The following table lists all entities which are members of this group.
Note: this group is a composite owner: wikiUsers is a composite of wikiUsers system of record an
wikiUsers excludes
Filter for:
All members
Member name
Remove selected members
Entity name
Membership
Show:
50


wikiUsers
More actions
Group containing list of wikiUsers after adding the includes and subtracting the excludes
More
Members
Privileges
More
Role permissions
+ Assign permission
Permissions assigned to roles are inherited to all entities who are members of the role
Permission def
apps:wiki:wikiPermissions:wikiPermissionDef
The definition part of the permission holds the settings, security, metadata. Generally permission definitions have multiple permission resources.
Resource name
apps:wiki:wikiPermissions:informationTechnologyWiki
The permission resource is the part of the permission which is assigned to owner objects. Generally multiple permission resources are related to one permission definition.
Action
read
A permission assignment has multiple parts, the role, or entity (in the context of a role), the resource, and the action. For example, the role might be Payroll User, the entity might be John Smith, the resource might be Org123, and the action might be Read or Write. The permission definition defines which actions are available for that definition. The list of actions is free-form. Generally there are not more than a few dozen actions for a permission definition.
Allowed
Allow
Disallow
Normally a permission assignment will be allow. The default is for the permission to not be allowed. But if you have inheritance, and you want to allow a wider set, and restrict a part, then disallow here. For example you could allow All and disallow one part of All.
Save


Home > Root > apps > wiki > wikiGroups > wikiUsers
wikiUsers
More actions
Group containing list of wikiUsers after adding the includes and subtracting the excludes
More
Members
Privileges
More
Role permissions
+ Assign permission
Permissions assigned to roles are inherited to all entities who are members of the role
Actions
Role
Resource
admin
read
write
Permission Definition
wikiUsers
informationTechnologyWiki
wikiPermissionDef
wikiUsers
mathWiki
wikiPermissionDef
Save


Home › Barry Benson
Barry Benson
+ Add to a group
More actions
Unique ID: babe
Email:
Name: Barry Benson
Description: Barry Benson
More
Add to my favorites
Permissions
Attribute assignments
View membership audit log
View action audit log
View privilege audit log
Memberships
Group privileges
Folder privileges
Attribute privileges
The following table lists all groups in which Barry Benson is a member.
Filter for: All groups
Group name
Apply filter
Reset
Remove selected groups
Folder
Group name
Membership
wikiGroups
wikiUsers
Indirect
Actions
wikiGroups
wikiUsers system of record
Direct
Actions
wikiGroups
wikiUsers system of record and includes
Indirect
Actions
Show: 50
Showing 1-3 of 3 · First | Prev | Next | Last

Subject permissions

+ Assign permission

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

Permission def

apps:wiki:wikiPermissions:wikiPermissionDef

The definition part of the permission holds the settings, security, metadata. Generally permission definitions have multiple permission resources.

Resource name

apps:wiki:wikiPermissions:informationTechnologyWiki

The permission resource is the part of the permission which is assigned to owner objects. Generally multiple permission resources are related to one permission definition.

Action

admin

A permission assignment has multiple parts, the role, or entity (in the context of a role), the resource, and the action. For example, the role might be Payroll User, the entity might be John Smith, the resource might be Org123, and the action might be Read or Write. The permission definition defines which actions are available for that definition. The list of actions is free-form. Generally there are not more than a few dozen actions for a permission definition.

Role

apps:wiki:wikiGroups:wikiUsers

The role is a special type of Group which can associate members with permissions or allow members to have individual permissions assigned in the context of the role.

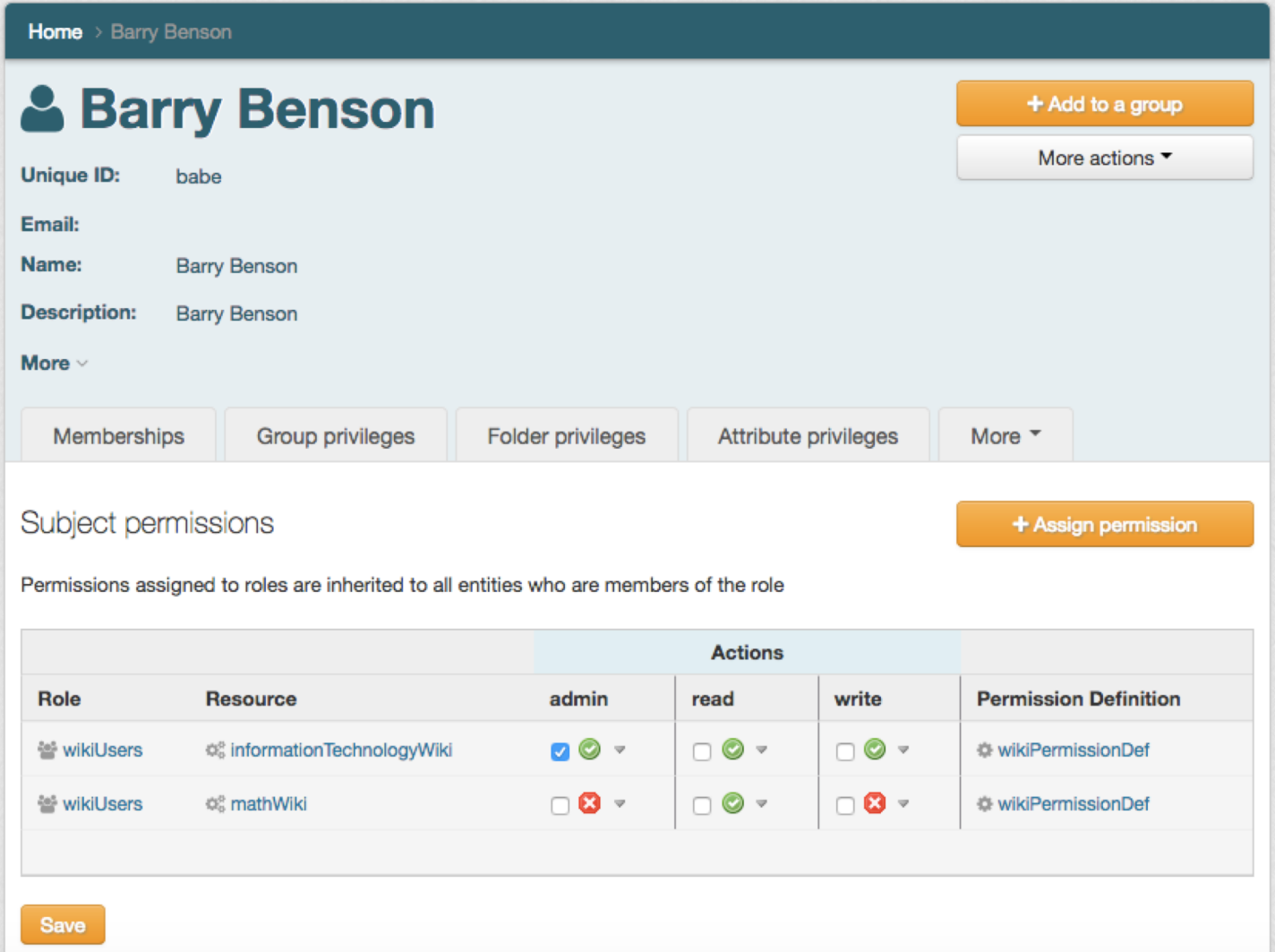
Allowed

- (•) Allow
- ( ) Disallow

Normally a permission assignment will be allow. The default is for the permission to not be allowed. But if you have inheritance, and you want to allow a wider set, and restrict a part, then disallow here. For example you could allow All and disallow one part of All.

Save

CC BY NC


Home › Barry Benson
Barry Benson
+ Add to a group
More actions
Unique ID: babe
Email:
Name: Barry Benson
Description: Barry Benson
More
Memberships
Group privileges
Folder privileges
Attribute privileges
More
Subject permissions
+ Assign permission
Permissions assigned to roles are inherited to all entities who are members of the role
Actions
Role
Resource
admin
read
write
Permission Definition
wikiUsers
informationTechnologyWiki
wikiPermissionDef
wikiUsers
mathWiki
wikiPermissionDef
Save

CC BY NC

Memberships | Group privileges | Folder privileges | Attribute privileges | More

Analyze permission result

The overall result of whether a role or a subject in a role can perform an action on a resource could depend on many permission assignments which imply other permissions. This screen shows the relevant assignments and which assignment is responsible for the result.

Permission type	Entity
Role	wikiUsers
Action	read
Permission resource	informationTechnologyWiki
Permission definition	wikiPermissionDef
UUID	1a91b8fdf0d84c3988593cd0fad8cb83
Start permission on date	
End permission on date	
Permission result	✓

Result reason

This explains why the relevant assignments cause the result

Permission type	Permission role	Entity	Action	Resource	Allowed	Assignment rank	Rank reason	Permission definition	UUID
Entity	wikiUsers	Barry Brooks	admin	informationTechnologyWiki	✓	1		wikiPermissionDef	
Role	wikiUsers		read	informationTechnologyWiki	✓	2		wikiPermissionDef	

INTERNE

Thanks!

Further information:

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

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

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

GROUPER IN ACTION

PRESENTED BY: CHRIS HYZER, UNIVERSITY OF PENNSYLVANIA
BILL THOMPSON, LAFAYETTE COLLEGE
KEITH WESSEL, UNIVERSITY OF ILLINOIS
CHRIS HUBING, INTERNET2

© 2018 Internet2