



Agenda

Intro to Grouper

Project status & recent news

- v2.1
- v2.2
- demo of new UI

Brief campus case studies: what we're doing with Grouper and why

- Michael Hodges, University of Hawaii
- Chris Bongaarts, University of Minnesota

Longer term roadmap

Wrap-up, opportunities to follow up



Introduction to Grouper

Tom Barton

University of Chicago and Internet2

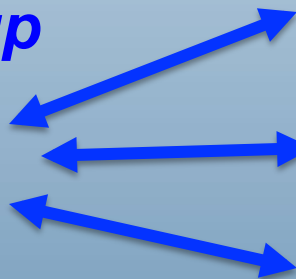
Manager – Grouper Project



Why have an access management strategy?

- Lower cost and time to deliver a new service
- Simplify and make consistent by using the same group or role in many places

***Physics 101
Course Group***



Email Group

Wiki Access

Lab Reservations

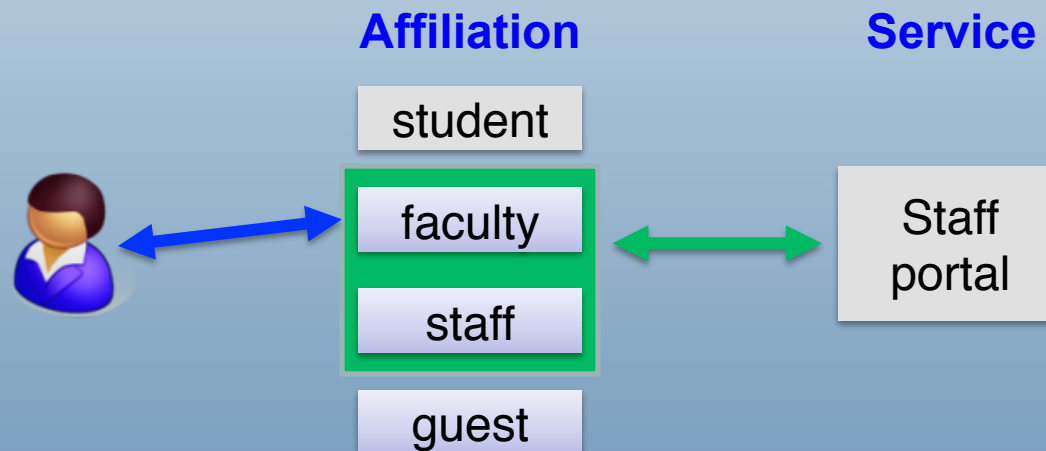
Additional benefits of access management

- Delegation to empower the right people to manage access. Take central IT out of the loop.
- Operational transparency. See who can access what, with a report rather than a fire drill.



Access management stages: authorization > authentication

1. Start out using a single user attribute, affiliation, in LDAP or Active Directory. This lets services implement simple access policies.



Access management stages: authorization > authentication

2. Enrich & centralize access management with groups determined from systems of record
 - Courses, financial accounts, departments
 - Define service-specific access policies in the centralized access management system

Math Faculty Group



can access

Math
Faculty
Resources

Access management stages: authorization > authentication

3. Get central IT out of the loop

- Distributed management
- Exceptions
- Departmental applications

*Math Faculty
Group*



+

*Math Support
Group*



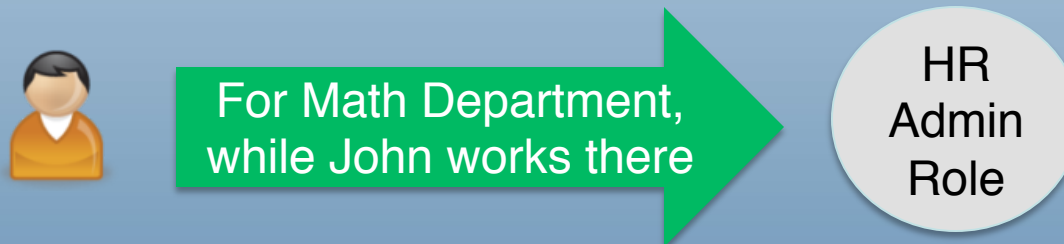
can access

Math
Faculty
Resources

Access management stages: authorization > authentication

4. Deeper integration of access management

- Direct integration with applications using web services
 - SOAP/REST/ESB
- Roles & privileges to support applications more deeply



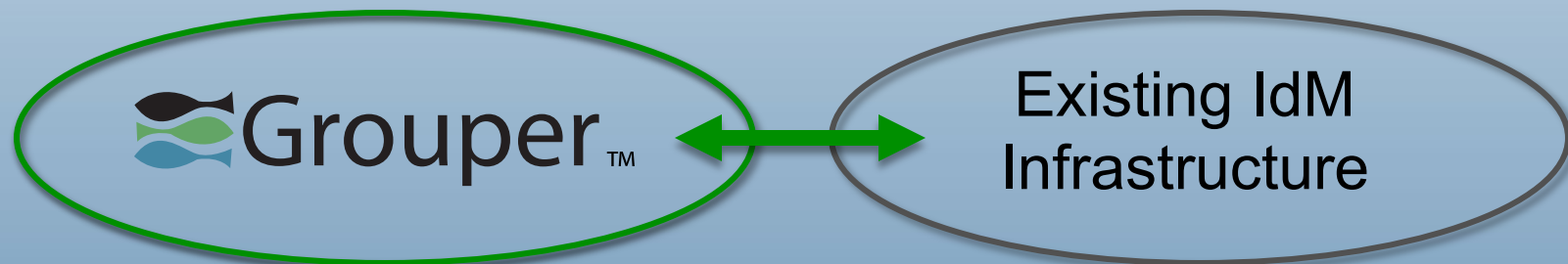
The Grouper Story

- Open source, community-driven project of the Internet2 Middleware Initiative
 - Initial release v0.5 in December 2004



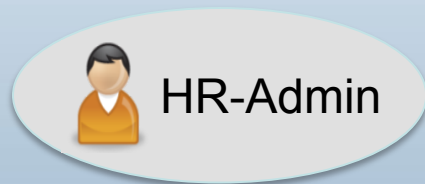
The Grouper Story

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



The Grouper Story

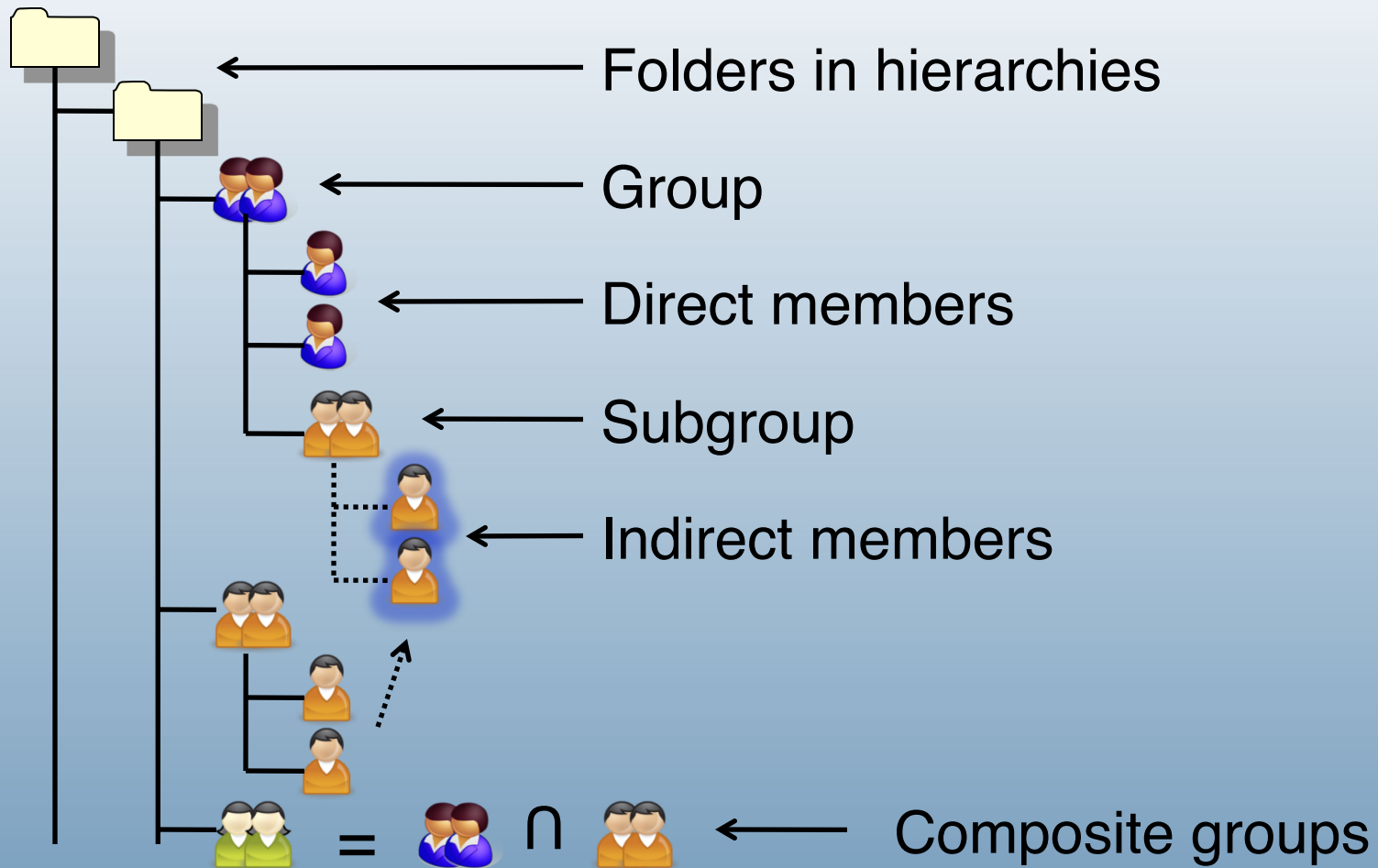
- Grouper v2.X expanded beyond groups
 - Roles & permissions



- Rules

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

Group: core concepts



Security & delegation

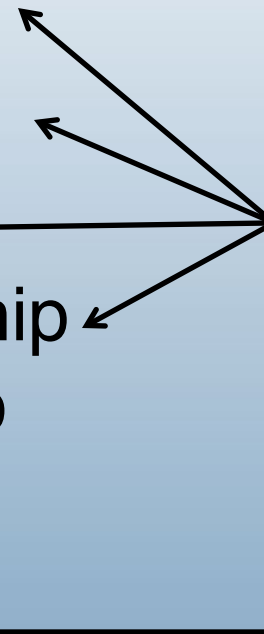


- Create groups
- Create subfolders

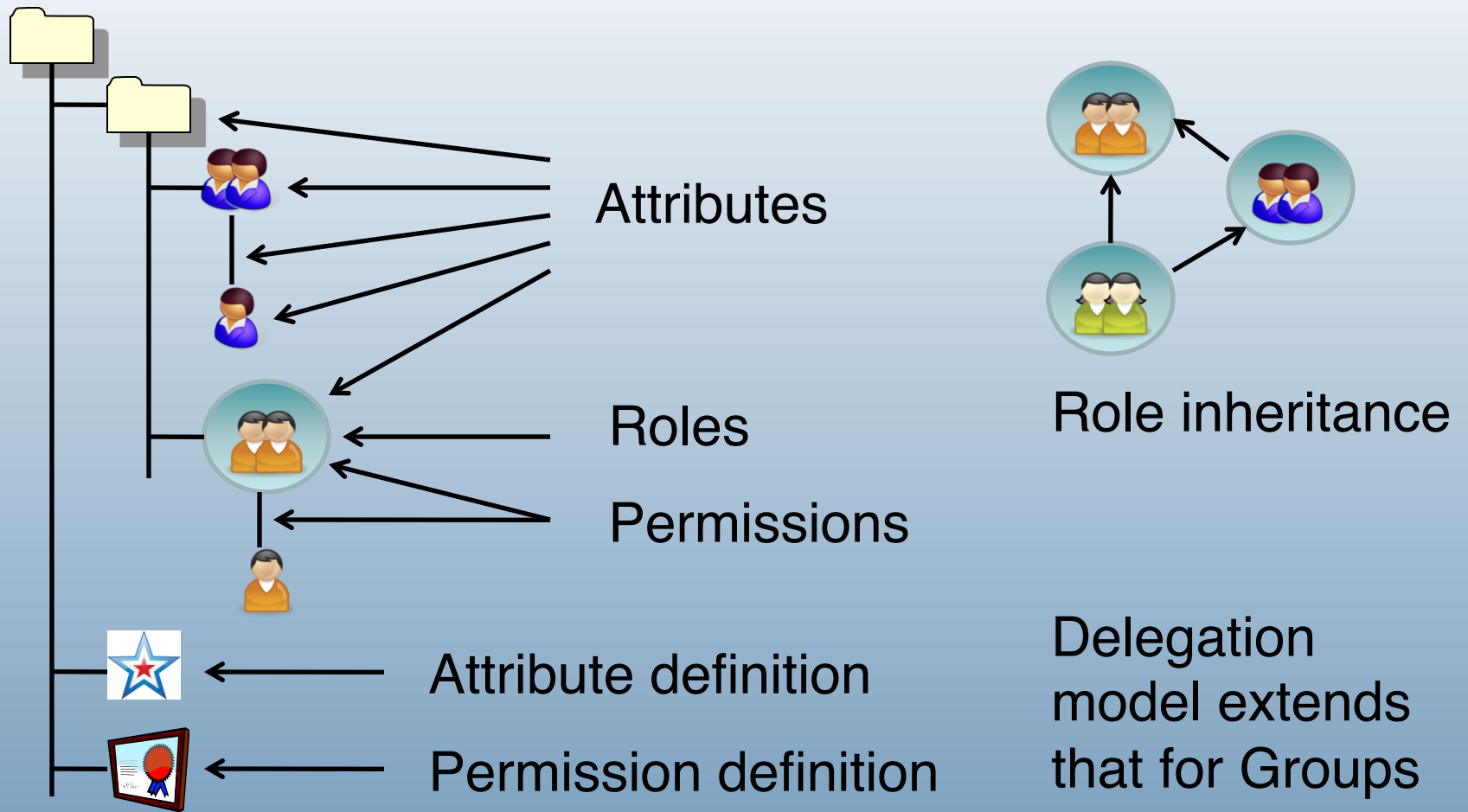


- Admin
- Update membership
- Read membership
- View group
- Opt-in
- Opt-out

Delegation



Beyond groups

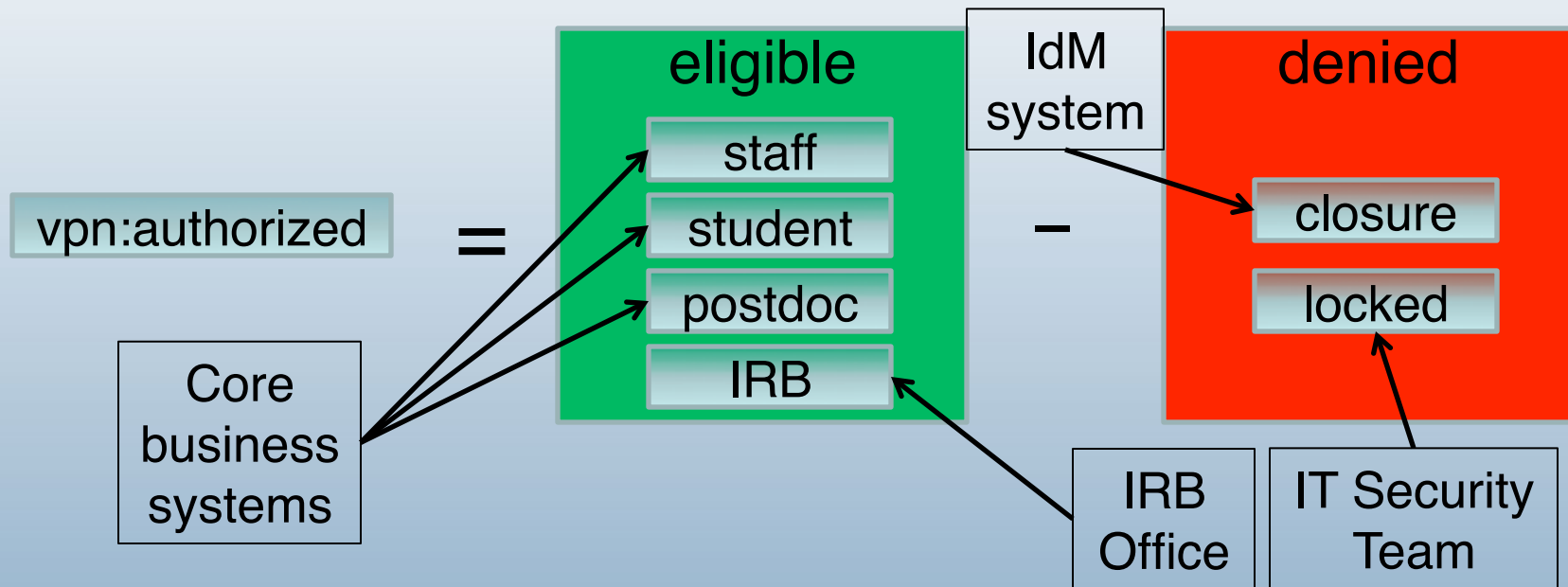


Access management lifecycle support

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



Access management for UChicago VPN



Different groups, different authorities
VPN only uses “vpn:authorized”



V2.1, V2.2, New UI

Chris Hyzer
University of Pennsylvania
Internet2

2.1.4

- Will be released momentarily (if not already)
- 4 months since 2.1.3
- 19 Jiras

2.1.4 (Important Jiras)

- Deleting attribute def with group which has privs, deletes members of group
- Rule to adjust privs based on group
- “Support” for Java 7
- Subject API search by status
- Lifelong group membership rule
- LDAP authentication for WS
- Various bugs and tweaks

2.2 Progress

- Config file overlays
- Grouper privileges are group lists
- Services in Grouper
- Unix GID management

2.2 Plan

- PSP improvements
- Conversion of legacy group types/attributes to new attribute framework
- Grouper user data
- SCIM interface
- UI

New Grouper UI

- Focus on most used parts of the UI
- Extensive user experience study and design
- Dojo for accessibility and improved usability and device support
- Make it easier for people to find things and perform tasks
- Responsive web design for mobile support
- See design:
<http://grouper-ui.uchicago.edu/hifi>

New Grouper UI – main screen

Home

Grouper




Institute of Higher Education

This website allows you to manage groups associated with your organization and the members of those groups. For a list of answers to frequently asked questions, refer to the [support documentation](#).


Recent Activity

- Added [John Smith](#) as a member of the [Editors](#) group. 2/1/2013 8:03 AM
- Revoked [Bob Weston's](#) membership in the [Editors](#) group. 1/21/2013 9:00 AM
- ...
- Assigned the ADMIN privilege to [Jane Clivemore](#) in the [Senior Editors](#) group. 12/20/2012 9:00 AM

My Favorites

-  [Admins](#)
Root : Applications : Wiki
-  [Editors](#)
Root : Applications : Wiki
-  [Senior Editors](#)
Root : Applications : Wiki

Groups I Manage

-  [Admins](#)
Root : Applications : Directories
-  [Managers](#)
Root : Applications : Directories
-  [Approvers](#)
Root : Applications : Wiki

My Services

- [Virtual Private Network](#)
- [Wiki](#)
- [Blogs](#)
- [View all services](#)

NET®

New Grouper UI – main screen

The screenshot displays the main interface of the Grouper application. On the left, a sidebar contains a 'Create new group' button and a 'Quick Links' menu. The 'Quick Links' menu is circled in red and includes 'My Groups', 'My Folders', 'My Favorites', and 'My Services'. Below this is a 'Browse Folders' section with a tree view showing 'Root', 'Applications', 'Departments', and 'Reference Groups'. The main content area has a 'Home' header and a 'Grouper Institute of Higher Education' title. A descriptive paragraph follows, and then a 'Recent Activity' section with a table of events. At the bottom, there are three panels: 'My Favorites', 'Groups I Manage', and 'My Services', each listing various groups and their paths.

Quick Links

- My Groups
- My Folders
- My Favorites
- My Services

Browse Folders

- Root
 - Applications
 - Departments
 - Reference Groups

Home

Grouper

Institute of Higher Education

This website allows you to manage groups associated with your organization and the members of those groups. For a list of answers to frequently asked questions, refer to the [support documentation](#).

Recent Activity

Added John Smith as a member of the Editors group.	2/1/2013 8:03 AM
Revoked Bob Weston's membership in the Editors group.	1/21/2013 9:00 AM
...	
Assigned the ADMIN privilege to Jane Clivemore in the Senior Editors group.	12/20/2012 9:00 AM

My Favorites

- [Admins](#)
Root : Applications : Wiki
- [Editors](#)
Root : Applications : Wiki
- [Senior Editors](#)
Root : Applications : Wiki
- [Wiki](#)

Groups I Manage

- [Admins](#)
Root : Applications : Directories
- [Managers](#)
Root : Applications : Directories
- [Approvers](#)
Root : Applications : Wiki
- [Editors](#)

My Services

- [Virtual Private Network](#)
- [Wiki](#)
- [Blogs](#)
- [View all services](#)

New Grouper UI – main screen

The screenshot displays the Grouper main interface. On the left is a sidebar with a '+ Create new group' button, 'Quick Links' (My Groups, My Folders, My Favorites, My Services), and 'Browse Folders' (Root, Applications, Departments, Reference Groups). The main content area has a 'Home' header, the title 'Grouper', and the organization name 'Institute of Higher Education'. Below this is a descriptive paragraph and a link to support documentation. The 'Recent Activity' section, circled in red, lists three events: adding John Smith to the Editors group (2/1/2013 8:03 AM), revoking Bob Weston's membership (1/21/2013 9:00 AM), and assigning ADMIN privileges to Jane Clivemore in the Senior Editors group (12/20/2012 9:00 AM). At the bottom are three panels: 'My Favorites' (Admins, Editors, Senior Editors, Wiki), 'Groups I Manage' (Admins, Managers, Approvers, Editors), and 'My Services' (Virtual Private Network, Wiki, Blogs, View all services).

New Grouper UI – main screen

The screenshot displays the main interface of the Grouper system. On the left is a navigation sidebar with a 'Create new group' button and a 'Quick Links' section containing 'My Groups', 'My Folders', 'My Favorites', and 'My Services'. Below this is a 'Browse Folders' section with a tree view showing 'Root', 'Applications', 'Departments', and 'Reference Groups'. The main content area has a 'Home' header and a title 'Grouper' for the 'Institute of Higher Education'. A descriptive paragraph follows, mentioning support documentation. The 'Recent Activity' section lists actions such as adding John Smith to the Editors group and revoking Bob Weston's membership. At the bottom, three panels are visible: 'My Favorites' (circled in red), 'Groups I Manage', and 'My Services'. Each panel lists groups with their root paths, such as 'Admins' at 'Root : Applications : Wiki'.

New Grouper UI – main screen

The screenshot displays the main interface of the Grouper application. On the left, a sidebar contains a 'Create new group' button and a 'Quick Links' menu with items like 'My Groups', 'My Folders', 'My Favorites', and 'My Services'. Below this is a 'Browse Folders' section with a tree view showing 'Root', 'Applications', 'Departments', and 'Reference Groups'. The main content area has a 'Home' header and a 'Grouper Institute of Higher Education' title. A descriptive paragraph follows, and then a 'Recent Activity' section lists actions such as adding John Smith to the Editors group and revoking Bob Weston's membership. At the bottom, three panels are visible: 'My Favorites' (listing Admins, Editors, Senior Editors, and Wiki), 'Groups I Manage' (listing Admins, Managers, and Approvers), and 'My Services' (listing Virtual Private Network, Wiki, and Blogs). A red circle highlights the 'Groups I Manage' panel.

New Grouper UI – main screen

The screenshot displays the Grouper main interface. On the left is a sidebar with a '+ Create new group' button and a 'Quick Links' section containing 'My Groups', 'My Folders', 'My Favorites', and 'My Services'. Below this is a 'Browse Folders' section with a tree view: 'Root', 'Applications', 'Departments', and 'Reference Groups'. The main content area has a 'Home' header and a 'Grouper Institute of Higher Education' title. A descriptive paragraph follows. The 'Recent Activity' section lists three events: adding John Smith to the Editors group (2/1/2013 8:03 AM), revoking Bob Weston's membership (1/21/2013 9:00 AM), and assigning ADMIN privileges to Jane Clivemore in the Senior Editors group (12/20/2012 9:00 AM). At the bottom are three panels: 'My Favorites' (Admins, Editors, Senior Editors, Wiki), 'Groups I Manage' (Admins, Managers, Approvers, Editors), and 'My Services' (Virtual Private Network, Wiki, Blogs, View all services). A red circle highlights the 'My Services' panel.

New Grouper UI – group screen

The screenshot shows the Grouper web interface. At the top left is the Grouper logo. At the top right, there is a search bar and the text 'Logged in as awilliams · Log out · Help'. Below the logo is a '+ Create new group' button. On the left side, there is a 'Quick Links' section with links for 'My Groups', 'My Folders', 'My Favorites', and 'My Services'. Below that is a 'Browse Folders' section with a tree view showing a hierarchy: Root > Applications > Wiki (selected) > Editors. The main content area has a breadcrumb trail: Home > Root > Applications > Wiki > Editors. The title 'Editors' is displayed with a group icon. To the right of the title are two buttons: '+ Add members' and 'More actions'. Below the title is a descriptive paragraph: 'The members of this group have basic editor permissions in the Wiki. Editors have permissions to create and edit content but require approval in order to publish.' Below this is a 'More' dropdown menu. Underneath are three tabs: 'Members' (selected), 'Privileges', and 'More'. The main content area contains the text: 'The following table lists all entities which are members of this group.' Below this text is a 'Filter for:' section with a dropdown menu set to 'All members', a text input field containing 'Member name', and 'Apply filter' and 'Reset' buttons. Below the filter is a 'Remove selected members' button. The table below has two columns: 'Entity Name' and 'Membership'. It lists three members: 'Senior Administrators' (Direct), 'Staff' (Direct), and 'Abbott, Jane' (Direct). Each row has an 'Actions' dropdown menu.

Home > Root > Applications > Wiki > Editors

Editors

The members of this group have basic editor permissions in the Wiki. Editors have permissions to create and edit content but require approval in order to publish.

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	Actions ▾
Senior Administrators	Direct	Actions ▾
Staff	Direct	Actions ▾
Abbott, Jane	Direct	Actions ▾

New Grouper UI – privileges screen

The screenshot shows the Grouper UI interface. At the top left is the Grouper logo. A search bar is at the top right, and the user is logged in as 'awilliams'. The main navigation bar shows the path: Home > Root > Applications > Wiki > Editors. On the left sidebar, there are 'Quick Links' (My Groups, My Folders, My Favorites, My Services) and 'Browse Folders' (Root, Applications, Directories, Service Q, Virtual Private Network, Wiki, Wordpress, Departments, Reference Groups). The main content area is titled 'Editors' and includes an 'Add members' button and a 'More actions' dropdown. Below this is a description of the group's permissions. A 'More' dropdown menu is open, showing 'Members', 'Privileges', and 'More'. The 'Privileges' tab is selected, displaying a table of entities with their privileges. The table has columns for Entity Name, Admin, Read, Update, OptIn, OptOut, and View. The entities listed are 'Every Entity', 'Senior Administrators', 'Staff', and 'Carlin, Hank'. A red arrow points to the 'Actions' dropdown for the 'Carlin, Hank' entity.

Home > Root > Applications > Wiki > Editors

Editors

The members of this group have basic editor permissions in the Wiki. Editors have permissions to create and edit content but require approval in order to publish.

More ▾

Members Privileges More ▾

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

Filter for: Everyone ▾ Entity name Apply filter Reset

Update: Assign the ADMIN privilege ▾ Update selected

<input type="checkbox"/>	Entity Name ▾	Admin	Read	Update	OptIn	OptOut	View	
<input type="checkbox"/>	👤 Every Entity		✓				✓	Actions ▾
<input type="checkbox"/>	👤 Senior Administrators	✓	✓	✓	✓	✓	✓	Actions ▾
<input type="checkbox"/>	👤 Staff	✓	✓	✓	✓	✓	✓	Actions ▾
<input type="checkbox"/>	👤 Carlin, Hank		✓		✓		✓	Actions ▾

Real World Cases Studies

- Brief campus case studies
 - Michael Hodges, University of Hawaii
 - Chris Bongaarts, University of Minnesota



Groupier beginnings at the University of Hawaii



- Michael Hodges, Manager,
Enterprise Middleware,
Identity and Access Management





Getting Started with Grouper

- Designing the Stem, we kept it very simple:
 - auto (automatically generated institutional groups)
 - everyone
 - everyone@honolulu
 - faculty
 - students@manoa
 - custom (applications and individuals manage these)
 - uhsystem
 - banner
 - ohr
 - test (applications and individuals test here)
 - mhodges (developer's UH Username)



Getting Started with Grouper

- First Pilot Project, make an auditor happy
 - Utilize Grouper groups to enhance our daily termination reports.
 - Reports are sent daily to each of the ERP account administrators (and others).
 - **Problem:** They each try and sift through the haystack for Usernames, and sometimes miss.
 - **Solution:** each account admin maintains a Grouper group. The termination reports include only those of interest. Everyone is happier.
 - The pilot is a success.



Getting Started with Grouper

- Second Pilot Project, augment LISTSERV lists
 - Automate membership of the UH Hilo Fac/Staff campus-wide discussion LISTSERV list.
 - **Problem:** Some people consider the list to be ham, others spam.
 - **Solution:** Allow the campus list administrator to augment an “auto” list using Grouper “inclusion” and “exclusion” groups.
 - We (IAM) populate the “auto” group for the campus and perform the Grouper math (auto + inclusion – exclusion) to rebuild the list, nightly.



Going Places with Grouper

- Expand the Augmented LISTSERV lists pilot
 - Provide Group Administration tools
 - Friendly interface for managing inclusion/exclusion group membership.
 - Support group functionality for enabling/disabling:
 - Reflection to LISTSERV lists (in the near future)
 - Reflection to Sakai groups, Google groups, etc.
 - End-user options (none vs. opt-in/out)
 - Provide End-User tools
 - Provide users with a personal list of auto groups/reflections so that they can opt in/out of each.



Going Places with Grouper

- Support more institutional groups
 - Expand the “auto” groups to include additional institutional groups: students by major, program; departments for each campus; etc.
- Evangelize (**middleware rocks!!!**)
 - Leverage our UH Applications Developers forum to share, educate, and inspire others in IT to leverage this and other tools being developed to support authentication, authorization, and utilization of middleware in general.

Grouper at the University of Minnesota

**Christopher A. Bongaarts
Grouper Virtual Working Group
May 20, 2013**



UNIVERSITY OF MINNESOTA

Driven to DiscoverSM

In the beginning...

- Grouper 1.2.1 in production August 2008
- Driver: BPEL access management for Enterprise Financial System project
 - Using LDAP groups to represent roles
 - Wanted UI with delegated administration
- Similar desires for helpdesk access to user management interface



Timeline, continued

- Upgraded to 1.5.2 in March 2010
- Switched to UW LDAP source adaptor April 2010
- Upgrade to 2.1.3 planned for summer 2013



Applications using Grouper for access management

- BPEL workflows
- Helpdesk account management
- WorkFlowGen
- VPN groups
- Oracle Business Intelligence (OBIEE)
- Various departmental sites



Other uses

- Google Apps provisioning
 - Overrides for health care component
- Netfiles (Xythos WFS) central groups
- Identifying test directory users



Example group

The screenshot displays the Grouper web interface. At the top left is the University of Minnesota logo, and at the top right is the Grouper logo. A navigation bar includes the text "Welcome cab", a "Log out" link, a "Act as self" dropdown menu, and a "Change" button. A left sidebar contains navigation links for "My enrollment", "My memberships" (highlighted), "Join groups", "My responsibilities", "Manage groups", "Create groups", "My tools", "Explore", "Search", "Folder workspace", "Group workspace", "Entity workspace", and "Help". At the bottom of the sidebar, it says "Grouper is sponsored by" with the Internet2 logo.

The main content area is titled "MY MEMBERSHIPS" and "Browse groups hierarchy". It provides instructions on how to find groups and lists three options: "Browse the groups hierarchy", "List your groups", and "Search for groups by name".

Below this, there is a section for "Browse or list groups" with a "List my groups" link. The "Current location is:" section shows a breadcrumb path: "Root: University of Minnesota: Office of Information Technology: Access Control" and a "Lists: Managers" link. It indicates "Showing 1-4 of 4 items" and lists four groups: "Readonly Groups", "Active Directory", "Can Spoof while testing", and "Duluth".

At the bottom, there is a "Search groups" section with an "Advanced groups search" link. It features a search input field, a "Search groups" button, a "Search from" dropdown menu set to "Root", and radio buttons for "Display results by" with options for "Path", "Name", and "ID Path".



Another example group

Browse or list groups ⓘ

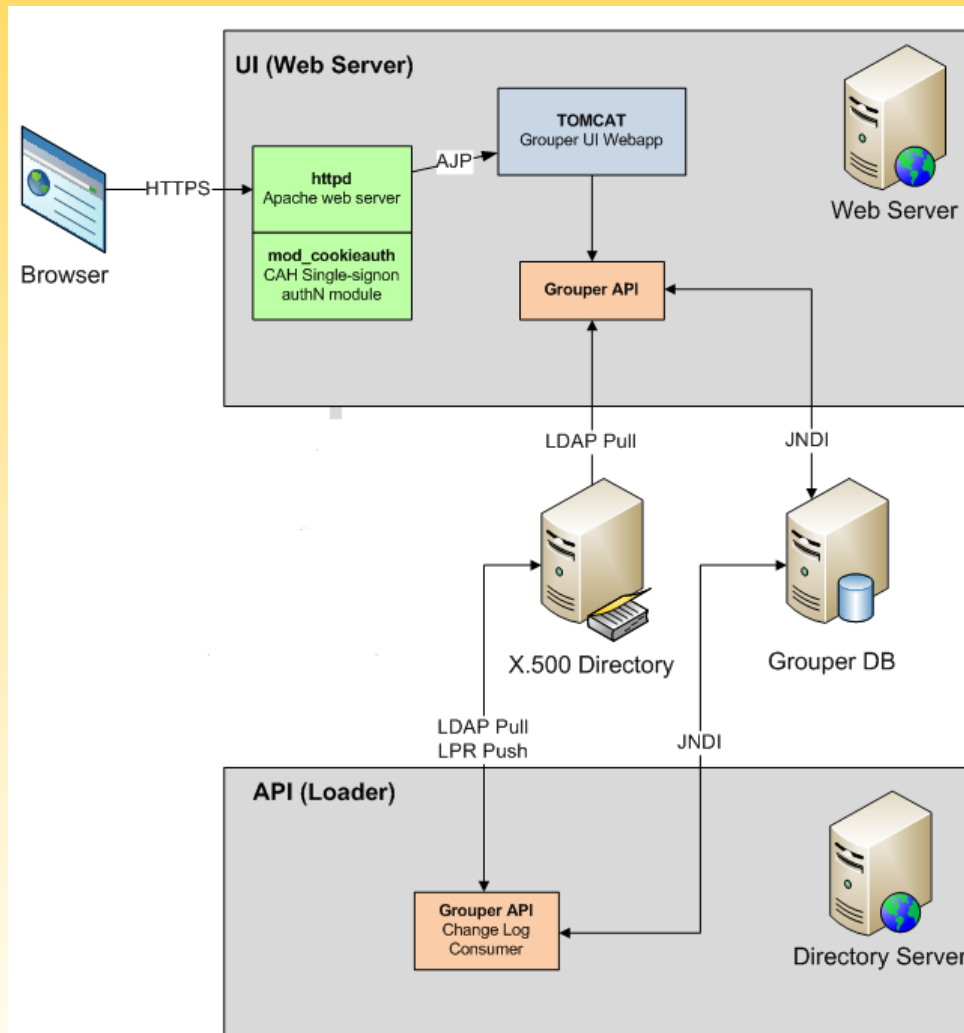
Current location is:
📁 Root: 📁 University of Minnesota: 📁 WorkFlowGen: 📁 PRD: 📁 **ASR**

Showing 1-10 of 10 items

- 📁 AstraAccess
- 📁 FeeWaiverAppeal
- 📁 Grad
- 📁 PDR
- 📁 StudentServiceFeeAppeal
- 👤 **All_Staff**
- 👤 **ASR Process Managers**
- 👤 **One_Stop_Counselors**
- 👤 **ProcessSupervisors**
- 👤 **SF_Collectors**



Deployment Architecture



Access methods

- Group management via web UI only
 - Requires two-factor authN (OTP fob)
- Client access
 - LDAP (expressed as group objects, isMemberOf)
 - Shibboleth (SAML isMemberOf attribute)
 - Gets data from LDAP
 - Attribute filters with stem regexes work slick



Directory provisioning

- Using Grouper Loader changelog API
- Locally written Java class sends updates to person registry database
- Person registry pushes updated group data to LDAP directory



Future directions

- Investigate using the PSP for LDAP provisioning
- Create local documentation
- Encourage more applications to use Grouper for access control



Contact

Chris Bongaarts

Identity Management

University of Minnesota

cab@umn.edu



UNIVERSITY OF MINNESOTA
Driven to DiscoverSM

Grouper Roadmap

V 2.2

New UI

Services

Improved configuration

SCIM interface

Treat privileges as
Group lists

Unix GID management

Legacy attribute
migration

COmanage integration

Not Yet Assigned

Security plugins

Access Management
Standard WS API

Further KIM-Grouper
integration

More WS operations

Register for notifications

More provisioning
connectors

Ongoing

Grouper Core
enhancement

Community
contributions

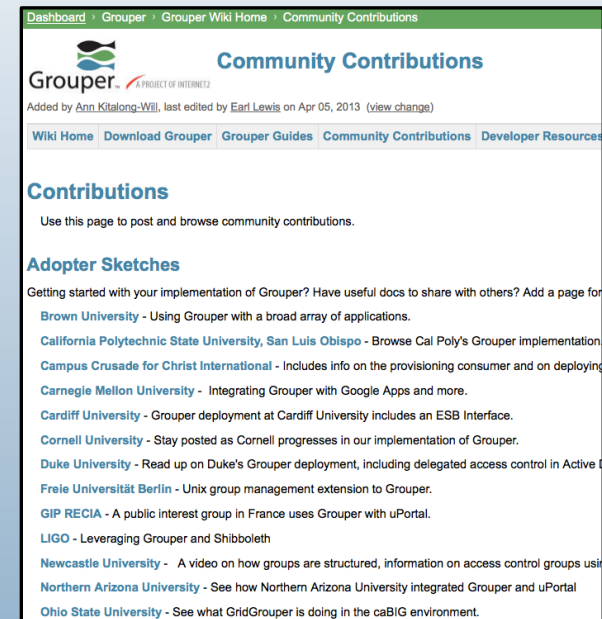
Getting Started and Learning More

- Grouper Training Videos
 - 51 videos, with an average 120 views
 - Tracks for:
 - Managers
 - System. Admins
 - Developers/Architects
 - End Users



Contributing to the Community

- Share information about your deployment with the community
- Participate on the Grouper-Users list





Thanks!

Further information:

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

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

