Grouper Working Group

INTERNET®

Agenda

- Internet2 IPR, agenda bash
- Grouper v2.0 in brief
- Who's using Grouper? Survey take aways
- Focus on v2.x: current plans & discussion
- Grouper & OSIdM4HE
- Your items …

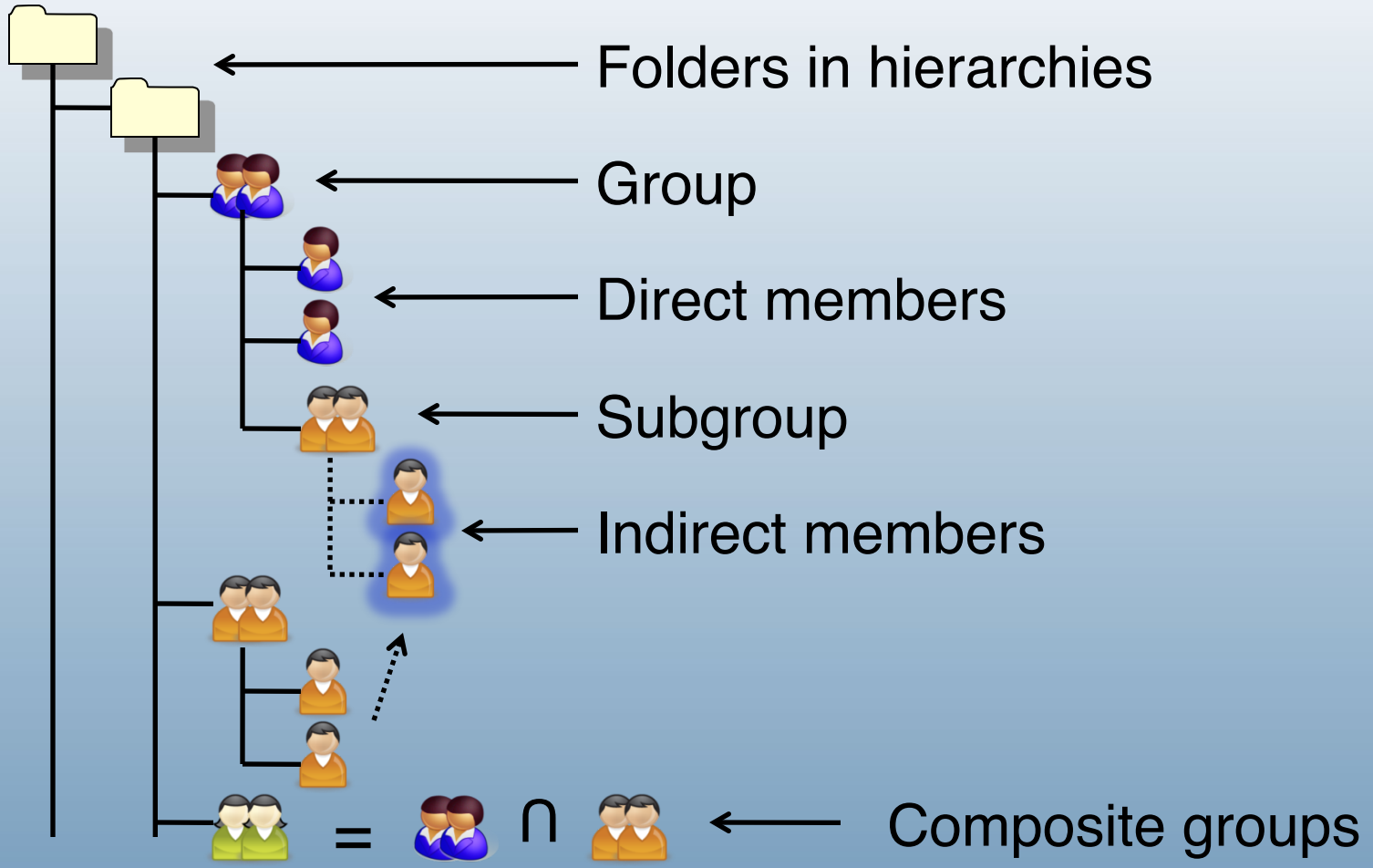
Grouper Story

- Open source, community-driven project of the Internet2 Middleware Initiative
  - Initial release v0.5 in December 2004
- Grouper originally focused on robust management of groups, emphasizing:
  - Delegation and distributed management
  - Integration with most any existing IdM infrastructure. See case studies and campus contributions at:
  - https://spaces.internet2.edu/display/Grouper/Community+Contributions
- Grouper v2.0 provides broader set of access management capabilities, including roles & permissions
  - Released 6 September 2011

Access management is a process: making authZ more than authN

1. Start out using a single user attribute, *affiliation*, in LDAP or AD to let applications implement access policies
2. Enrich centralized access management using groups determined from systems of record
   - Courses, financial accounts, departments
   - Define service specific access policies in central IAM system
3. Get central IT out of the loop
   - Distributed management
   - Exceptions
   - Departmental apps
4. Increase integration of access management
   - Direct application integration with web services
   - ESB/SOA, REST/SOAP
   - Roles & privileges to support applications more deeply

Grouper: core concepts



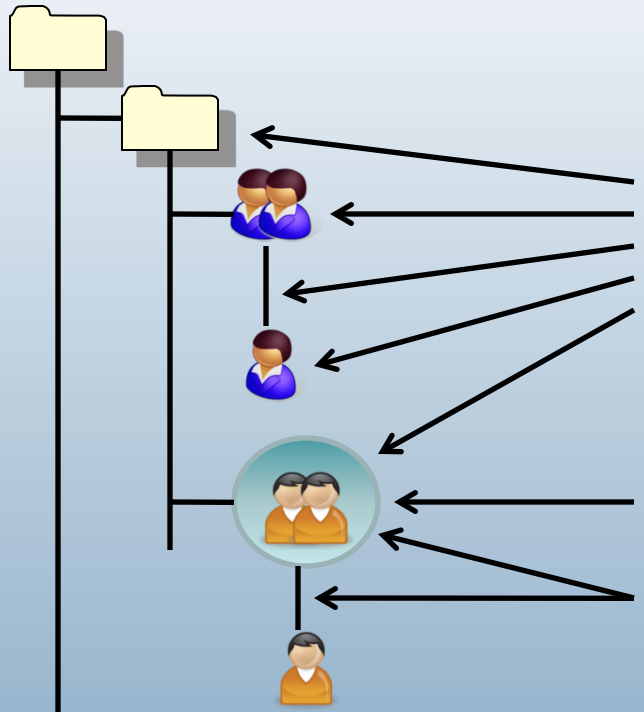
Security & delegation in Grouper

- Create groups
- Create subfolders

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

Delegation

Beyond groups



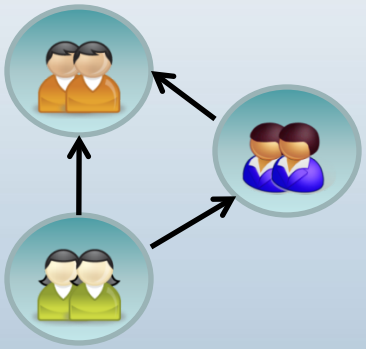
Attributes

Roles

Permissions

Attribute definition

Permission definition



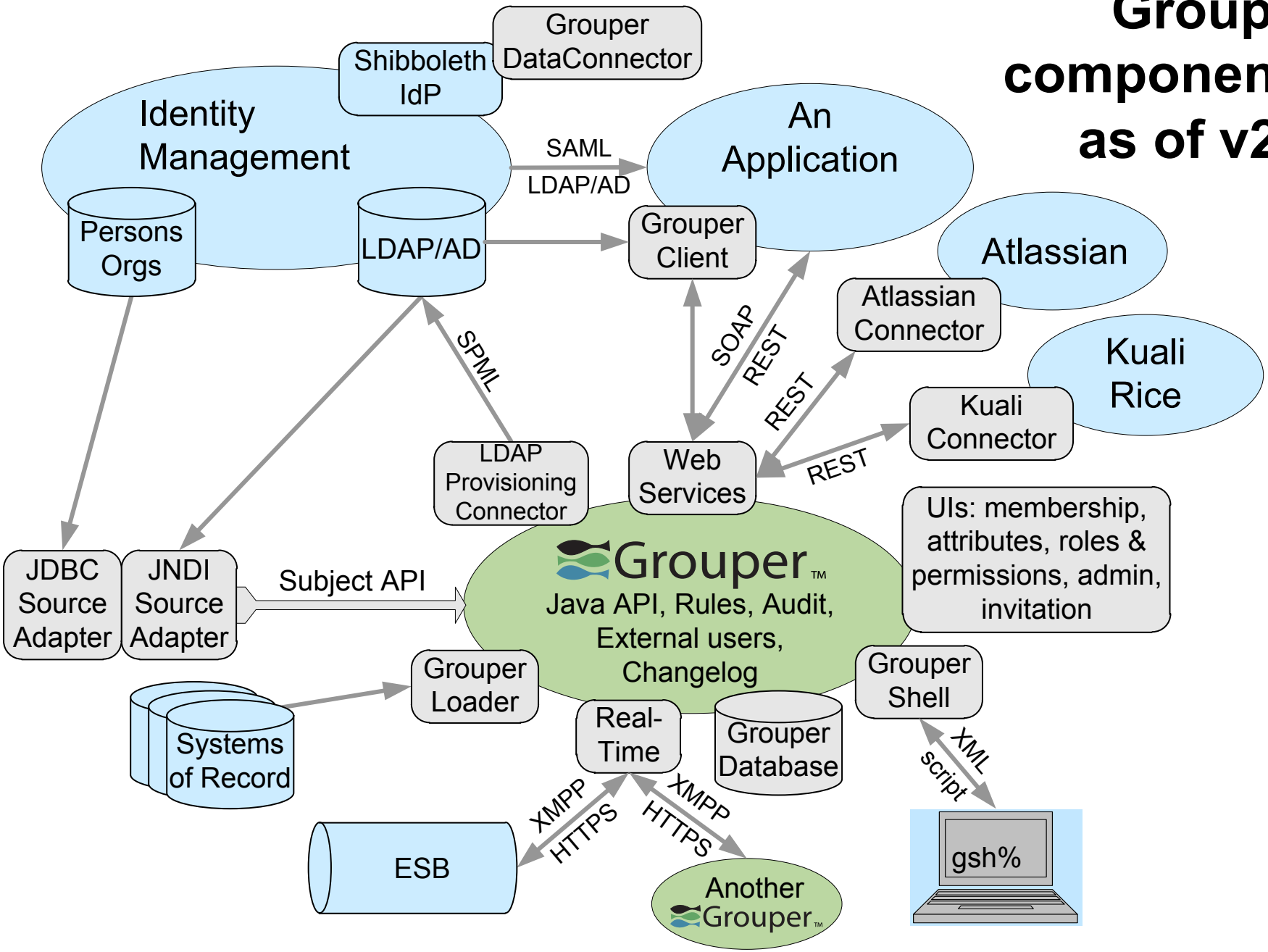
Role inheritance

Delegation model extends that for Groups

Access management lifecycle support

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

Grouper components as of v2.0



New and Improved in Grouper v2.0

Feature	Description
Rules	Execute built-in actions and expression language to add business logic to Grouper actions
Attribute and Permissions UIs	Ajax-y UIs to define, view, and assign attributes and permissions
Permission Disallow	To manage inheritance of permissions via Role, Resource, or Action hierarchies
Permission Limits	Built-in Policy Decision Point that combines run-time context with permissions to produce Allow/Deny
Point in Time Audit	Query Grouper's state at a previous time
External Subjects	Invitation processes leverage federation to let external Subjects be given group memberships and permissions
Syncing Groupers	Federate groups between two Groupers
Member Search & Sort	Selective Subject attribute caching for improved sorting and searching capability and speed
LdappcNG enhancement	Improved performance through caching

Grouper Survey

- Late June – early July 2011

Stage	Respondents (121)	Self-Identified Respondents (69)
Production	37	24
Deploying	20	13
Evaluating	40	21

- International adoption: 4 continents
- Healthy pipeline of new adopters

Some takeaways

Strengths	Strong community
	Integration architecture works: more than 30 applications mentioned by respondents
	Comprehensive, multi-featured
Weaknesses	Admin UI isn't suited to non-technical users
	Documentation wiki needs improvement
	LDAP provisioning connector lacks real-time incremental capability
Adoption Obstacles	Insufficient resources or priority
	Commitment to legacy environment or commercial suite

- v2.0: wiki improvements begun
- v2.1: real time & incremental LDAP provisioning
- v2.2: new Ajax-y UI

GROUPER GOING FORWARD

Roadmap v2.1 (winter 2011)

Planned	• Real-time incremental LDAPPCNG • LDAP Grouper loader • Grouper entities in namespace • Hibernate upgrade • Grouper WS/client group/stem finder sorting/paging
Discuss	• Subject attribute WS security • Always available readonly client • Grouper WS attr/permission expansion • uPortal integration update • Unix GID management

Roadmap v2.2 (winter 2012?)

Planned	• New UI • Collecting objects in Grouper into a "service" • Other stuff not done from 2.1 roadmap
Discuss	• Externalizing Shib release policy into Grouper (e.g. entitlements, memberships, etc) • FIFER server • Your item here

Discussion – it's all about you!

- Wondering if Grouper can help with one of your use cases?
- Already using Grouper and have some questions or needs?
- Are you doing, or know of, related work bearing on the above?
- Want to partner with us to have your use case drive design of a v2.X feature?
- Any other questions while we're all together?

Notes from discussion

- OAuth - voot on github
- Workflow integration in Grouper?
- Enhancements to Rules? XMPP messages
- Interest from CMU and COManage for earlier 2.2 release for UI capability.
- Federated Groupers for permissions
- Outreach to science community, training, commercial support.
- Easier installation process? Packaging changes for v2.2?

www.internet2.edu