UH Applications Developers 9/16/2011

Michael Hodges, ITS, IAM

Julio Polo, ITS, IAM

Agenda

- UH Applications Developers Meeting
- Update on the Grouper project
- Update on the UHIMS Event Messaging Service
- Planned LDAP Pruning
- Acknowledgements Application Specifications
- Authentication to 3rd party service providers and the sharing of attributes
- The IAM public website and information for developers

UH Applications Developers Meeting

- Shoot for quarterly meetings.
- Increase alignment of IAM development with developers' needs.
- Ensure developers remain informed.
- Provide venue for early developer input.
- Provide opportunities for participation: design, use-cases, involvement, pilots.
- Increase collaboration in all directions.

Grouper Update - Pilot

- Production
  - https://grouper.hawaii.edu:8443/
- Termination report for ID Managers of:
  - Banner
  - ODS
  - PeopleSoft
  - RACF

Grouper Update – grp

- Homegrown shell tool that talks to Grouper:
- > help
- ls -- ls [group-substring...]
- find -- find group-substring uid-or-uUuuid...
- add -- add group-substring
- del -- del group-substring [uid-or-uUuuid]...
- mod -- mod group-substring [uid-or-uUuuid]…

Grouper Update – grp

- > ls term-rpt
- GROUP
- uh:custom:uhsystem:its:uhims:term-rpt:banner
- uh:custom:uhsystem:its:uhims:term-rpt:ods
- uh:custom:uhsystem:its:uhims:term-rpt:peoplesoft
- uh:custom:uhsystem:its:uhims:term-rpt:racf
- uh:custom:uhsystem:its:uhims:term-rpt:uh-data-center-access

Grouper Update – grp

- > find
- Usage: find group-substring uid-or-uUuuid...

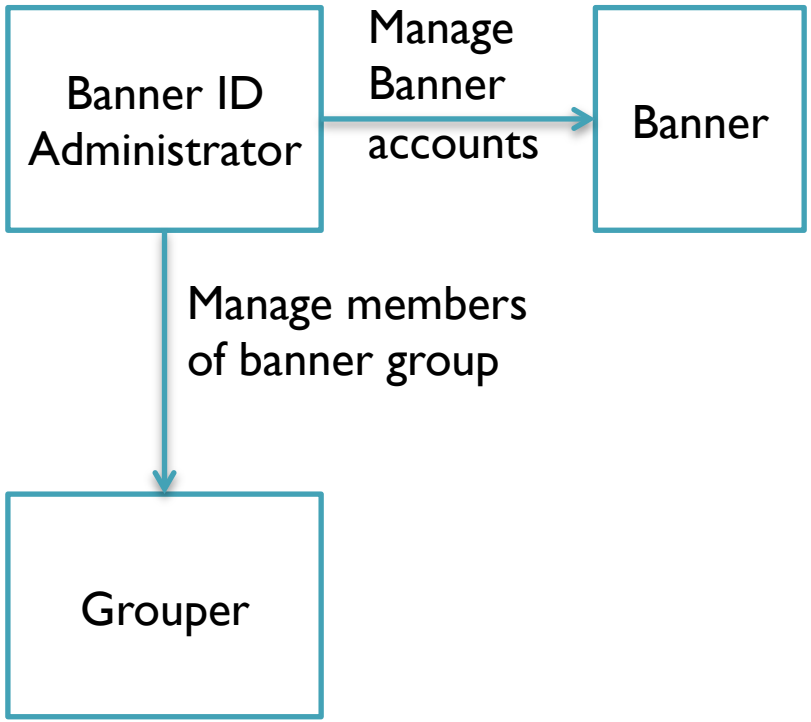
- > find term-rpt:banner jsmith
- GROUP: uh:custom:uhsystem:its:uhims:term-rpt:banner
- uid: | uhUuid: | cn: | Banner ID | Campus | Comments |
- johns | 99999999 | John Smith | JSMITH | HON |

Grouper Update – grp

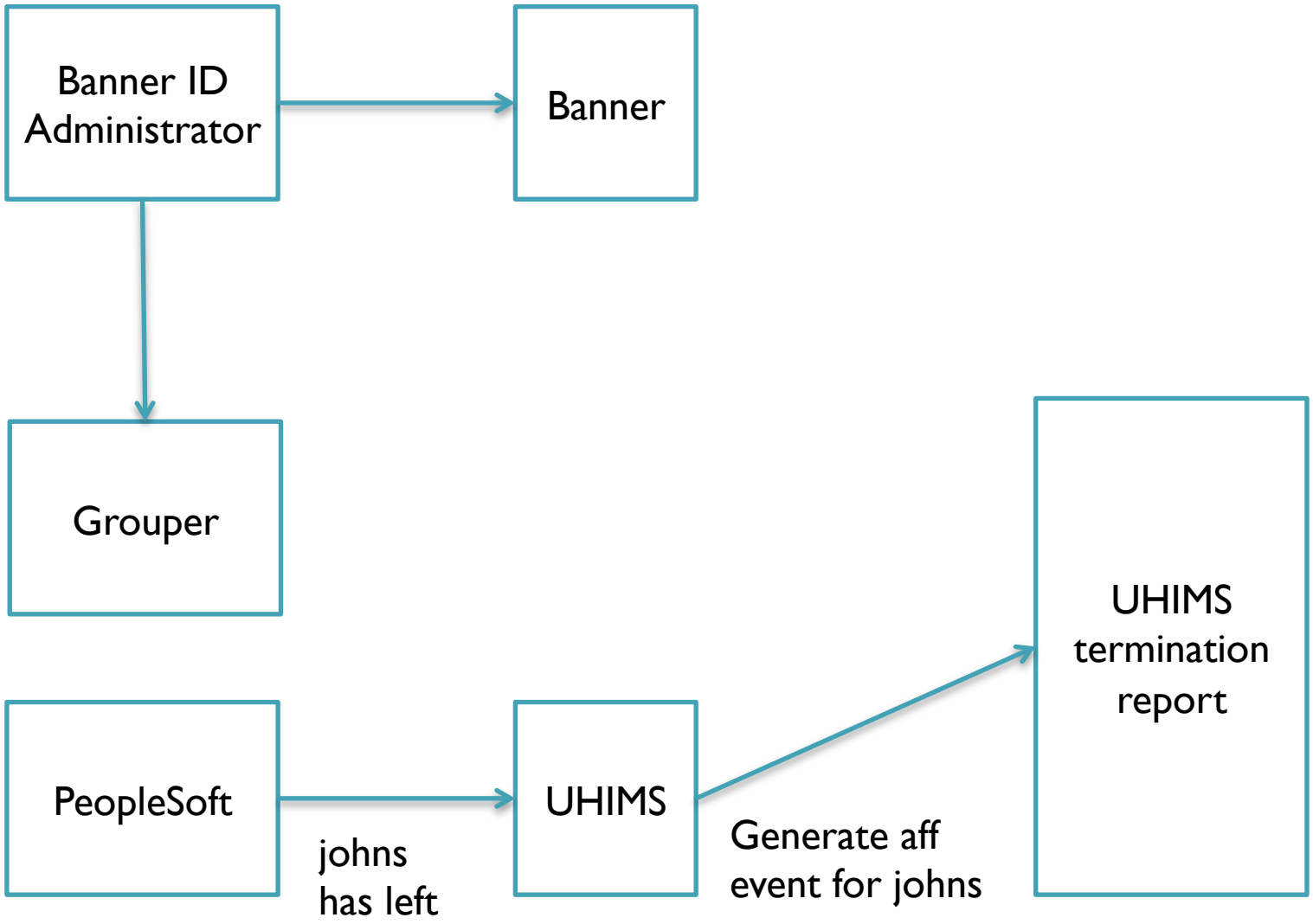
- > add
- Usage: add group-substring

- Enter uid or uhUuid (or control-D if done): janedoe
- uhUuid: 99999999
- uid: janedoe
- cn: Jane Doe
- Is this the right person? (yes)
- Banner ID? JANED
- Campus? WIN
- Comments?

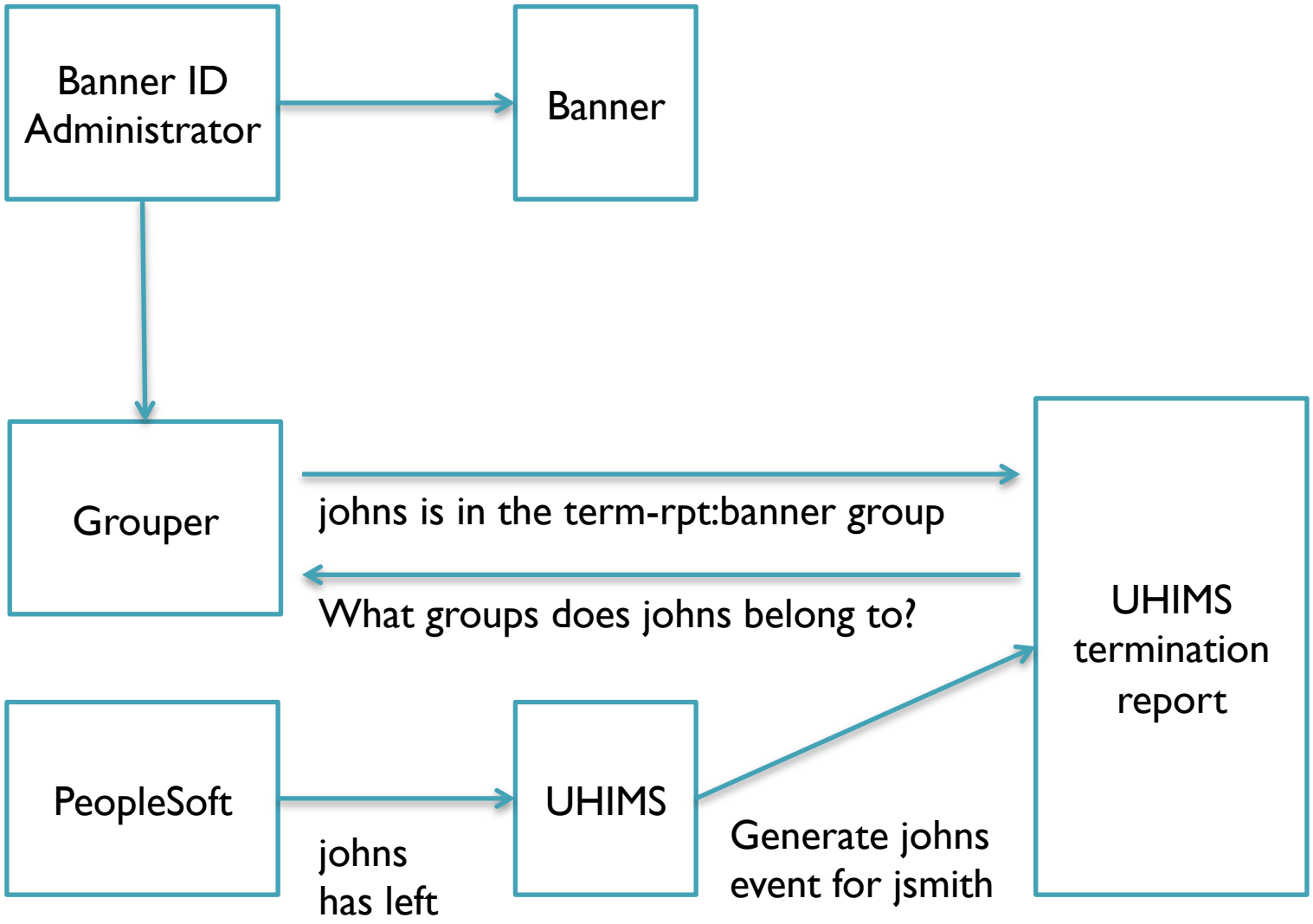
Grouper Update – Termination



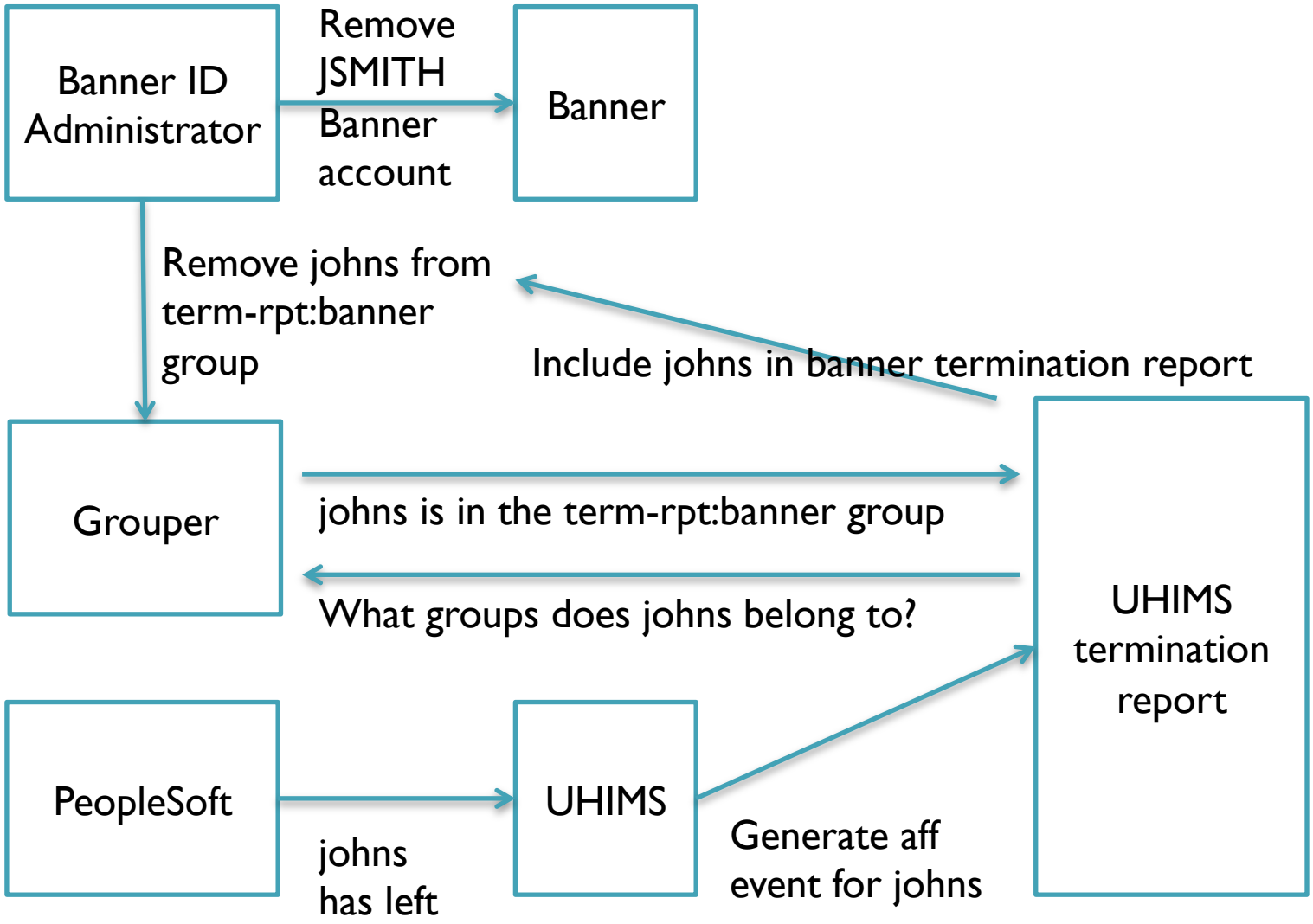
Grouper Update – Termination



Grouper Update – Termination



Grouper Update – Termination



Grouper Update – Pilot Benefits

- No spreadsheets for Banner, PeopleSoft, RACF, and ODS
- No wading through ALL terminations
- Receives targeted reports (or no report) for each

Grouper Update – Future

- Speed listing of membership attributes
- Grouper 2.0 testing
- Populate automatic groups
- CAS or Shib AuthN
- LISTSERV sync
- Triggers for custom groups?
  - Auto-delete or auto-insert member if event matches criteria
- Pilot not necessarily typical. How do you envision using it?

Grouper Update – gsh

- adminUid = "jdoeboss";
- groupExt = "banner";
- groupName = "Banner";
- groupDesc = "Who has database or forms access to Banner";
- parentStemPath = "uh:custom:uhsystem:its:uhims:term-rpt"
- groupPath = parentStemPath+":"+groupExt;

// ITS IAM model for defining attributes

- attrStemPath = groupPath;
- defStemPath = attrStemPath+":attributeDefs";
- nameStemPath = attrStemPath+":attributeDefNames";

- ArrayList attrList = new ArrayList();
- attrList.add("Banner ID");
- attrList.add("Campus");
- attrList.add("Comments");

Grouper Update – gsh

- session = GrouperSession.startRootSession();

- // insert or update group
- // groupPath is "uh:custom:uhsystem:its:uhims:term-rpt:banner"

- GroupSave groupSave = new GroupSave (session);
- groupSave.assignGroupNameToEdit (groupPath);
- groupSave.assignName (groupPath);
- groupSave.assignDisplayExtension (groupName);
- groupSave.assignDescription (groupDesc);
- groupSave.save();

Grouper Update – gsh

- // assign group administrator
- Subject subject = SubjectFinder.findByIdentifier(adminUid)

- group = GroupFinder.findByName(session, groupPath, true)
- group.grantPriv(subject, AccessPrivilege.ADMIN, true);

Grouper Update – gsh

- // set attribute framework
- addStem(parentStemPath, groupExt, groupName);
- addStem(attrStemPath, "attributeDefs", "attributeDefs");
- addStem(attrStemPath, "attributeDefNames", "attributeDefNames");

Grouper Update – gsh

- stem = StemFinder.findByName (session, attrStemPath);

- item = "textInput";
- textInput = stem.addChildAttributeDef (item, AttributeDefType.attr);
- textInput.setAssignToImmMembership(true);
- textInput.setValueType(AttributeDefValueType.string);
- textInput.store();
- addStem(defStemPath, item, item);

- // allow group administrator to update attributes
- textInput.getPrivilegeDelegate().grantPriv(subject, AttributeDefPrivilege.ATTR_ADMIN, true);

Grouper Update – gsh

```
// define each attr
for (int i=1; i<=attrList.size(); i++) {
    item   = attrList.get( i-1 );
    addStem( nameStemPath, item, i+" "+item );
}
for (int i=1; i<=attrList.size(); i++) {
    item   = attrList.get( i-1 );
    stem.addChildAttributeDefName( textInput, item, item );
}
```

UHIMS Events - Person

- person.add
- person.modify.name
  person.modify.displayName
  person.modify.ssn
- person.modify.dob
- person.del
- person.modify.uhUuid

UHIMS Events - Affiliations

- aff.add.<uhDataOrigin>.<role>.<org>
- aff.delete.<uhDataOrigin>.<role>.<org>

Include remaining active affiliations in event?

UHIMS Events – Aff Transitions

- aff.transition.none.participatory
- aff.transition.participatory.ohana
- aff.transition.ohana.participatory
- aff.transition.none.ohana
- aff.transition.ohana.none
- aff.transition.participatory.none
- aff.transition.none.retiree
- aff.transition.ohana.retiree
- aff.transition.participatory.retiree
- aff.transition.retiree.participatory
- aff.transition.retiree.none

UHIMS Events – Username

- username.add
- username.modify.password
- username.modify.accountName
- username.modify.googleBasis
- username.modify.type
- username.modify.status
- username.delete.uid
- username.modify.uid

UHIMS Events – Username

- username.access.suspend
- username.access.restore
- username.deprovision.lifecycle

UHIMS Events – Email

Based on UH username, first.last, or otherwise

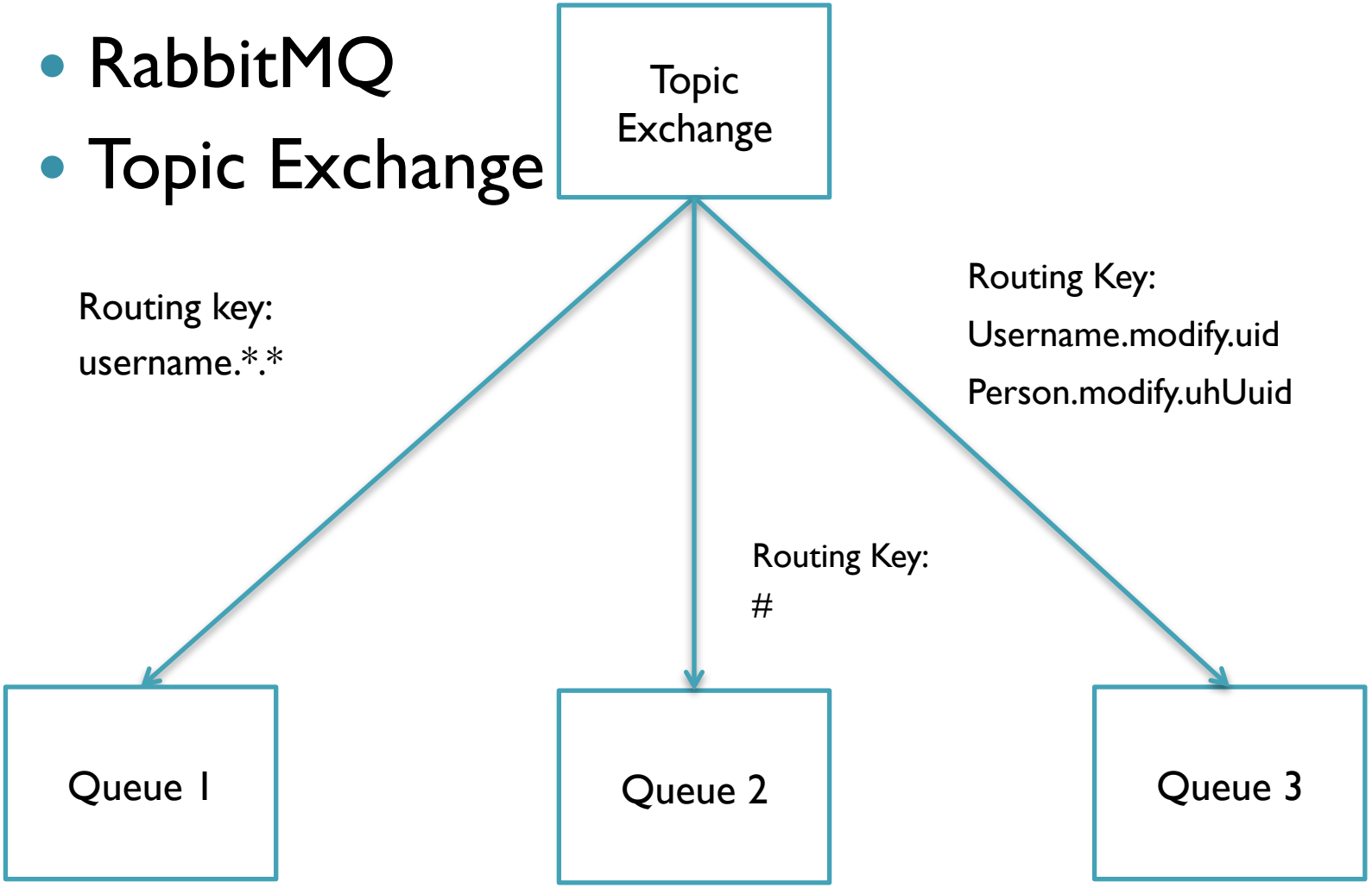
- email.add
- email.modify.uid
- email.modify.uhUuid
- email.del

UHIMS Events – Dir Listing

- dirListing.public
- dirListing.internal

UHIMS Event Messaging

- RabbitMQ
- Topic Exchange



UHIMS Event Messaging - Producer

- broker-connection -> new (credentials)
- broker-connection -> obtain a channel
- channel -> declare exchange
- "xname"
- type=direct
- passive=false
- durable=true
- auto_delete=false
- channel -> publish
- msg
- "xname"
- properties
- "routing_key"

UHIMS Event Messaging - Consumer

- broker-connection -> new (credentials)
- broker-connection -> obtain a channel
- channel -> declare exchange
- "xname"
- type=topic
- passive=false
- durable=true
- auto_delete=false
- channel -> queue declare
- "qname"
- channel -> bind
- "qname"
- "xname"
- "routing_key"

UHIMS Event Messaging - Consumer

- channel -> subscribe [actually called basic_consume()]
- msg_consumer(channel, ***method***, message_header, message_body),
- channel -> basic_ack (delivery_tag = method.delivery_tag)
- if quitting
- channel -> basic_cancel("consumer_tag")
- channel -> stop_consuming()
- else
- print message_body
- "qname"
- "consumer_tag"

- channel -> start_consuming()

LDAP Pruning

- Keep
  - Active aff
  - Directory listing, WPMS
- No longer a person registry
  - Anyone?
  - Alternatives

Acknowledgements Application Specifications

- A UH Security Program initiative.
- Automates the existing Confidentiality Agreement process.
- Enables applications to check for Acknowledgements prior to granting access.
- Specifications, draft review
  - Comments?
  - Suggested use-cases?

Acknowledgements App Specs

- Phase I
  - Acknowledgements only
  - LDAP assertions only
  - Target delivery for pilots, 11/2011
- Phase II
  - Certifications
  - CAS assertions
  - Shibboleth assertions
- Phase III (maybe or maybe not)

Acknowledgements App Specs

- Desirable Objects
  - Acknowledgements

    as in, I hereby acknowledge that I have read and understand the Confidentiality Agreement.
  - Certifications

    as in, successfully demonstrating via test questions that I have read and understand E2.214 (not a Phase I deliverable).

Acknowledgements App Specs

- Audiences
  - Users
    have UH Credentials and can assert acknowledgements and pass certifications.
  - Policy Reps
    can create and manage their own acknowledgements and certifications.
  - Admins
    can provision and de-provision Policy Reps.

Acknowledgements App Specs

- Acknowledgements and Certifications (ACs)
  - ACs must be owned by someone(s); group/ dept accounts are eligible.
  - Multiple applications can reference a single AC; a single app can reference multiple ACs.
  - A User's AC includes the date of the last successful encounter, but application logic determines if the AC is stale or not.

Acknowledgements App Specs

- User Interface specs
  - Web-enabled self-service tool for end-users.
  - Requires UH credentials to access.
  - Users can access all ACs.
- User is informed of which ACs have been acknowledged/passed and when.
- User can easily distinguish which ACs should be acknowledged/passed in the near future so as not to have to come back very soon.

more . . .

Acknowledgements App Specs

- Email notifications for pending expirations
  - Allow Policy Rep to select a notification schedule.
- Policy Reps can create, update, enable/ disable, delete, reassign or extend AC ownership
  - deleting and disabling an AC has potential ramifications.
  - default to pass if the application references an AC that is missing or disabled

more . . .

Acknowledgements App Specs

- Admins can provision/deprov and enable/disable Policy Reps
  - Q: must a person be fac/staff to be authorized? A: no, Admins determine
  - Q: are Grouper groups appropriate for tracking Policy Reps? A: tbd
  - Q: should UHIMS Life Cycle also trigger deprovisioning ownership? A: yes
  - Q: What happes to ACs that become orphaned (ownerless)? A: tbd

Acknowledgements App Specs

- Data Storage
  - Data tracks each user AC and the date last updated successfully.
  - Expiration dates are NOT by definition in scope. It is up to the application to apply business rules.
  - Life Cycle: all User data is removed when the user no longer has an active affiliation with UH. Returning to UH imposes a fresh start.

Acknowledgements App Specs

- Data Retrieval
  during authentication to determine authorization
  - LDAP
  - CAS - upgrading to CAS 3.x may be a prerequisite (not a Phase I deliverable)
  - Shibboleth via attribute release policy

Acknowledgements App Specs

- Ideas in the Parking Lot
  - Track who took which online quizzes, etc and reporting back to a dept, unit, etc.
  - POs may want to track who amongst their staff have done the confidentiality agreement.
  - Departments may want to impose their own acknowledgements for their own staff or for their own guests.

Acknowledgements App Specs

- AC Specific Questions?

Authentication to 3rd-Party Service Providers

- Background
  - UH is a member of the InCommon Federation, which includes 230 Higher Ed institutions and 80 3rd-party Service Providers.
  - Membership provides the first level of vetting. 3rd-party SPs must be sponsored by a Higher Ed institution and must adhere to documented set of Operational Practices.
- Operational Practices

Authentication to 3rd-Party Service Providers

- Operational Practices
  - SSO requires that UH define a policy (in XML) to control exactly what attributes are released to a 3rd-party Service Provider.

Authentication to 3rd-Party Service Providers

- UH Operational Practices (a work in progress)
  - Release the bare minimum attributes.
  - When identifying attributes to be released, the on-line application must inform the user that they are accessing a 3rd-party application.
  - Vet requests for release of information with IRAO (a new set of data governance practices are currently emerging).
  - Impose vendor confidentiality agreements where contractually appropriate.
  - Protect user privacy by providing 3rd-party service providers with targeted Ids rather than UH numbers, even if releasing no other attributes.

The IAM Public Website

- Contents
  - News and Events
  - For Individuals –
    UH Username Services, Managing Your Identity Information
  - For Campus Identity Reps –
    UH Identity Management Services
  - For Campus Technology Administrators –
    ID Management and Authentication Solutions
  - For UH Developers - Developer Resources
  - For the InCommon Federation - Operational Practices
  - General Info –
    UH Identity and Access Management Overview
  - Terminology –
    Terminology, Standard Codes and Definitions

The IAM Public Website

- Hosted as a public facing wiki space.
- Future plans for a secured wiki space for developers only.
- Requests for additional content encouraged.
- Requesting that you provide us your authentication solutions for posting as use-cases.
- *The website is a work in progress…*

Wrap-up & Preview Agenda

- Questions?

- Preview (tentative next agenda)
  - Introduce planned LDAP test environment and planned configuration changes to enforce rate limiting
  - Using LDAP (Authz) and SASL (Authn) for pass-through authn to control lab computers access
  - Update on Grouper 2.0 for Role Based Access Control
  - Update on the UHIMS Event Messaging Service
  - Update on the Acknowledgements Self Service application

UH Applications Developers 9/16/2011

Michael Hodges, ITS, IAM

Julio Polo, ITS, IAM

Thank you!!!

IAM: https://www.hawaii.edu/bwiki/x/DwBYDQ