TIER APIs and Registry Working Group Agenda and Notes

Wednesday 14 March 2018, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

- Video: https://bluejeans.com/678543210/browser

To join via Phone:

1) Dial one of these numbers or see all numbers - http://bluejeans.com/numbers
   +1.408.740.7256
   +1.888.240.2560(US Toll Free)
   +1.408.317.9253 (Alternate number)

2) Enter Conference ID: **678543210#**

Back to API WG wiki: http://j.mp/tierApiWiki
Handy Links[1]

Current meeting notes NEW DOCUMENT beginning 14 March 2018	

Meeting notes (THIS DOCUMENT) beginning 22 Sept. 2017 and ending March 9 2018

Archive of older meeting notes

- April 19 2017 to Sept. 20 2017 http://j.mp/apiRegWG-5
- 18 January 2017 to April 19 2017 http://bit.ly/tierApiReg
- 16 June 2016 to 18 January 2017: http://j.mp/1PWMCp5
- 4 November 2015 to 16 June 2016: https://tinyurl.com

Friday 9 March 2018 at 10:00 am Eastern, 7:00 am Pacific, 3 pm London

Participants

Keith Hazelton - UW-Madison (has to leave at the one hour mark)
Christopher Hoskin - University of Oxford
Jim Fox - UDub
Benn Oshrin - SCG (first hour only)

---

[1] TIER-API Agile Board (Backlog and Sprints)
Primary API and Registry WG Projects 2018

TIER APIs and Registry Working Group Agenda and Notes

Jon Miner (UW-Madison)
Tom Jordan - UW-Madison
Matthew Brookover, Colorado School of Mines

Agenda

1. Abstract for showcases

> @channel Wednesday we discussed some variation to the TIER Demos around integration and collaboration between COmanage and midPoint and what their possible roles can be within the TIER Reference Architecture.
>
> While different, this is not mutually exclusive to our thoughts on data flows from SOR to Registry and Provisioning / De-provisioning but more a matter of what can get done by Global Summit and what we want to focus on.
>
> We also hope to demonstrate some progress/results from the collaboration between the TIER WGs and the TIER Campus Success Program schools, perhaps around Banner integration etc.
>
> To this end we need to consider an Abstract for the Trust & Identity Showcase in the Global Summit Program.
>
> Some food for thought and open to comments and suggestions:
>
> *The Trust & Identity Showcase, distributed over 3 working sessions, will demonstrate how the TIER Campus Success project teams are collaborating with the TIER Working Groups in the areas of Integration with Banner, potential roles of COmanage and midPoint within the TIER Reference Architecture, how these components and applications cooperate in the context of data flows to the Registry, from the registry to provisioned systems and more.*
>
> We would like to get something into the program very soon so please add your thoughts, word-smith, and/or correct.
>
> Thanks much all! (-- BillK)

2. Scrummy stand-up reports
    a. Schema task force (Keith, Warren on point)
    b. API task force (BennO, JimF, Gabor on point?)

- Jim, BennO will work together next week and report out on Wednesday's

c. Messaging task force (EthanK, MichaelH? JimF? on point)
U Hawaii Message Documentation:
https://www.hawaii.edu/bwiki/display/UHIAM/Data+Available
   - Keep messaging simple for this round. Signed, not necessarily encrypted

3. Credential management Controller – Drill Down (MattB, WarrenC, arriving last half-hour)

   a. Documenting what this process is and providing clarifying information and advice

   b. WarrenC start by drawing a sketch of campus with an existing solution

   c. Banner subgroup:
      i. Wednesday call
      ii. JDBC, BEIS
      iii. John from Oregon State on their Ethos project; Feeding Chrome River tr. expenses, Ethos will be an abstraction above the deep internal schema in Banner; maybe John could do a demo
      iv. Group is collecting the sets of attributes that are derived from Banner
      v. Looking at pathways from Banner via Ethos into midPoint;
      vi. Lafayette puts Banner and COmanage side by side (at least as of TechEx) with a sneaker net between the two. No technical connection, but adding a non-trad person to COmanage: Step one is to create a skeleton person record in Banner so COmanage has a reliable user identifier.

4. Chris Hoskins working on a Kubernetes/Terraforming/…. Project. Has offered to share with TIER Packaging WG.

Next Meeting

Wednesday 14 March 2018, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

TIER APIs and Registry Working Group Agenda and Notes

Wednesday 7 March 2018, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

Participants

Jim Fox - UDub
Michael Brogan - U Wash
Bill Kaufman - Internet2
Jon Miner - UW-Madison
Michael Hodges - U of Hawaii
Keith Hazelton - UW-Madison
John Kamminga - UC Merced
Ethan Kromhout - UNC Chapel Hill
Benn Oshrin - SCG
James Babb - Uw Madison (late)

Agenda

5. Scrummy stand-up reports

    d. Schema task force (Keith, Warren on point)

```
COmsnsge: Data that gets provisioned to external systems, all associated to a person
```

```
'CoPerson' => (

'Co', (tenant)
   • Provision or not to midPoint?

'CoGroupMember' => ('CoGroup' => ('EmailListAdmin', 'EmailListMember', 'EmailListModerator')),
   • Auto mapping of some reference group like groups

'CoOrgIdentityLink' => ('OrgIdentity' => ('Identifier')),
   • Externally sourced info
```

```
    • Are interested in the identifier (account linking, authN, etc. purposes

'CoPersonRole' => ('Address', 'Cou', 'TelephoneNumber'),
    • Role == Bundle of attributes: Title, Affiliation, From/To dates. Sponsor, Dept.
    • Associated with COUs

'CoTAndCAgreement' => ('CoTermsAndConditions'),
    • Terms and Conditions (not likely to be provisioned out to, e.g., midPoint)

'EmailAddress', 0..n, typed

'Identifier',0..n, typed

'Name', 0..n, typed

'PrimaryName' => ('conditions' => ('PrimaryName.primary_name' => true)),

'SshKey',
    • And other authenticator types
    • Password svc tokens
    • X509 certs
    • ...

'Url' 0..n, typed

)
```

Schema mapping spreadsheet as a template

Gabor's minimal person schema

e. API task force (BennO, JimF, Gabor on point?)
   - Schema mapping spreadsheet as a template
   - SCIM support for messaging outbound from COmanage Registry to midPoint all the way to running code
   - How do we do extensions to schema (Use SCIM extension spec?)
     - Can this be deferred a bit?
   - ID Match API design is fairly stable, refactoring of attribute names, etc. Move into a spec (it's not SCIM, so what is it)
   - Scheduling: ID Match API spec ready for review at Global Summit?

f. Messaging task force (EthanK, MichaelH? JimF? on point)
   - What does the new institutional person message look like?
   - Michael Hodges: Lots of their messaging documentation is publicly available

        - https://www.hawaii.edu/bwiki/display/UHIAM/Data+Available
    - Target for
    - mP 'name' is globally unique but mutable;
    - But it might be better to establish a layer of indirection (JonM, MichaelHodges)
        - use AS PART OF A RESTful URL in the message
        - JimF: Use a unique ID; but if mP generates a message that resolves to the object representation, it can put what it wants in there

6. Credential management Controller – Drill Down (MattB, WarrenC, arriving last half-hour)

    a. Documenting what this process is and providing clarifying information and advice

> Hi Keith, this is probably 10 times longer then what most people want and about 1/3 of what is really going on.😀
>
> https://docs.google.com/document/d/1NOMlJwViqpl9Ww4NWHBbkngHGLlBTpIFx2AyVtj2mzo/edit?usp=sharing
>
> The real question I have is *how would I turn employee start dates, term codes and APDC codes into a useable set of reference groups* that would replace a 1000+ lines of Java and Groovy that enforce the various rules.
>
> See you at this afternoon's meeting!
>
> Matt Brookover

    b. WarrenC start by drawing a sketch of campus with an existing solution

    c. Getting the generic pattern into some level of detail.

3. So the schedule for demos at Global Summit will be:

T&I Showcase	Campus Success Program	Monday	2:45 - 4:00
T&I Showcase	TIER part 1 - SOR to Registry / Identity On-Boarding	Tuesday	1:15 - 2:30

/ COmanage as Registry, midPoint for provisioning aka Model 2

T&I Showcase TIER part 2 - Provisioning / De-provisioning Wednesday 8:45 - 10:00 /COmanage as 'just another SoR', midPoint as registry and provisioning aka Model 3

- We don't need to discuss now but we are working on an Abstract so if you have any thoughts please send them to wkaufman@internet2.edu or post in the tier-user-demos Slack channel.

- Notes from demo planning meeting last Monday https://docs.google.com/document/d/1k7Cr9igY9Kth8LSkVM776fGdScZ7W0JnnNHsF2C5py0/edit?usp=sharing

Next Meeting

Friday 9 March 2018 at 10:00 am Eastern, 7:00 am Pacific, 3 pm London

TIER APIs and Registry Working Group Agenda and Notes

Friday 2 March 2018 at 10:00 am Eastern, 7:00 am Pacific, 3 pm London

Participants

Warren Curry UFlorida
Ethan Kromhout - UNC Chapel Hill
Jon Miner - UW-Madison
James Babb - UW Madison
Benn Oshrin - SCG (first hour only)
Keith Hazelton - UW-Madison, late arrival
Bill Kaufman - Internet2, late arrival

Agenda

1. Person Registry Next Steps (Warren) -
    a) Finalize the schema to update (Keith, Warren on point)
        i) SCIM minimal person (from last summer work exists Keith
        ii) TIER Person standard extensions (base on COmanage attribute) *
            1) Cover on Wednesday (Keith)
        iii) Institution extension (define in more detail with example) (CSP - from a deod for the building of this, Keith/whc to find CSP help)
    b) API specification (congruent with msging) (BennO, GaborE on point)
        i) (AI) Get workers to move forward
        ii) Outbound to consumers (stds, SCIM, OneRoster)
        iii) Voluntolds? BennO?, GaborE?
    c) Messaging specification (congruent with API) (Ethan on point, wiith MichaelH, JimF)
        i) (AI) get workers to move forward
        ii) Ethan: Design: How to get mP to put something on message queue on creation/modification of person
        iii) Align API resource representation with message body, or at least identifiers in the message that can be used to GET the resource representation
    d) Matching API call(s) for Tier matching (BennO)

    e) Event triggering following registry entry (WHC concept, Ethan on point for midPoint, Tom)

    f) Tier Registry Deployment GUIDE how the parts relate and why…
        i) Multiple technical products

ii) How they interact for an onboarding process, how the APIs are used

h) DO we push groups in lieu of attributes. Does the reduction of attribute loose function. If not perhaps direct route to group tool vs a trip to registry make sense. Can coexist finding the harmony will be a learned / evolution to deploy. How do we describe this so it's easy for people to grasp the essentials? Do we need to evangelize

2. (When BillK joins) Time slots for the T&I Showcase Working Meetings at Global Summit.
   a. Review information in the tier-user-demos Slack channel
   b. Needs to be finalized today
   c. Campus success program will be Monday, so CIOs will
   d. Phase I and II of our showcases will be on Tuesday and Wednesday (2 on Tuesday)
   e. Global Summit schedule is now on the Internet2 site; don't worry about scheduling

3. NOTE: Availability of a Dockerized midPoint + Postgres + OpenLDAP (when/if Keith joins, otherwise Wednesday)
   a. Once you have the 280Mb file, it takes two commands to start full functioning midPoint on a machine running Docker
      i. docker-compose build
      ii. docker-compose up
      iii. Browse to http://localhost:18080
      iv. Log into midPoint with default admin credentials

* See COmanage data tables at https://spaces.internet2.edu/display/COmanage/All+Tables

COmanage passes the following to its provisioning connectors:

```
'Co',
'CoGroupMember' => array('CoGroup' =>
array('EmailListAdmin', 'EmailListMember',
'EmailListModerator')),
'CoOrgIdentityLink' => array('OrgIdentity' =>
array('Identifier')),
'CoPersonRole' => array('Address', 'Cou',
'TelephoneNumber'),
'CoTAndCAgreement' =>
array('CoTermsAndConditions'),
'EmailAddress',
'Identifier',
'Name',
```

```
'PrimaryName' => array('conditions' =>
array('PrimaryName.primary_name' => true)),
'SshKey',
'Url'
```

Schema mapping spreadsheet as a template

TIER APIs and Registry Working Group Agenda and Notes

Wednesday 28 February 2018, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

Participants

Keith Hazelton - UW-Madison
Dean Lane - Rice
Matt Brookover - CO School of Mines
Ethan Kromhout - UNC Chapel Hill
Tom Jordan - UW-Madison
Jon Miner - UW-Madison (until 3)
Michael Brogan - U Wash
Christopher Hoskin - University of Oxford
Benn Oshrin - SCG
Bill Kaufman - Internet2
Gabor Eszes - Old Dominion
Warren Curry - UFlorida

Excused

Jim Fox
Michael Hodges

Agenda

7. COmanage -- midPoint Integration
    a. Exercise/Practicum with a set of VMs implementing conceptual models 2 and 3, Illustrating a set of user stories;
    b. Model 4: See if it emerges from the campuses...
        i. We have done COmanage / midPoint integrations using LDAP
            1. Would COmanage and midPoint happily share a single LDAP server?
                a. Depends on what we're trying to accomplish
                    i. "Will they clobber records the other one wrote?"
                b. COmanage expects an OU to be there for its persons
                c. That is Laf. model: Guests as an ou of their own
                d. COmanage assumes control of 'its' schema
            2. LDAP is a great lowest common denominator for integration across systems

    a. MidPoint can both write to LDAP and consume from LDAP, so LDAP can be used as an integration point between another LDAP writer and MidPoint.
3. If they each need their own, does this create concerns?
4. COnsensus: Id Match must happen upstream of the Person Registry
5. Could the midPoint team have read-only access to a live dev-instance COmanage LDAP instance? LDAP would then be treated as the COmanage SoR. See one of the TIER testbed vms; Paul to work with BennO.
6. NO.
7. Mooted: midPoint team to start work on a SCIM connector
    a. Is this server still running? ldap://midpoint.testbed.tier.internet2.edu:9389
8. See COmanage data tables at https://spaces.internet2.edu/display/COmanage/All+Tables
   COmanage passes the following to its provisioning connectors:

```
'Co',
'CoGroupMember' => array('CoGroup' =>
array('EmailListAdmin', 'EmailListMember',
'EmailListModerator')),
'CoOrgIdentityLink' => array('OrgIdentity' =>
array('Identifier')),
'CoPersonRole' => array('Address', 'Cou',
'TelephoneNumber'),
'CoTAndCAgreement' =>
array('CoTermsAndConditions'),
'EmailAddress',
'Identifier',
'Name',
'PrimaryName' => array('conditions' =>
array('PrimaryName.primary_name' => true)),
'SshKey',
'Url'
```

   Schema mapping spreadsheet as a template

9. I2 ‘general app integration model is either SAML based JiT for the Atlassian apps, anchored in LDAP for Sympa and Grouper; plan is to implement a RabbitMQ messaging bus but we don’t have the exact connector to midPoint model yet.

10. If we did, COmanage and midPoint could share connectors (since midPoint could function as the provisioning engine
    a. COmanage was never intended to be an industrial strength/scale provisioner, So if we solve the COmanage-midPoint integration problem, it would make sense for COmanage to use midPoint as provisioning engine and focus connector development on that model
    b. COmanage would need to look at the integration challenges with using ConnID connectors.

ii. If a site is running COmanage and midPoint, is it advisable for them to share a single identity per person?
    1. Yes in model 2; in model 3, makes sense for there to be a separate OU for COpeople; In model 3, a single ID Match repo could serve both COmanage and midPoint.

c. Technical Fit/Gap Exercise (TIER Provisioning Fit/Gap Worksheet developed by TomJ)
    i. Done back when we were trying to sort out roles (Venn Diagram)
    ii. [Keith] Share with BTAA Provisioning Best Practices WG
    iii. Has it outlived its usefulness?
    iv. The taxonomy of provisioning (Col A & B) is still valuable

8. midPoint -- Grouper integration
    a. Obvious configuration: Registry-managed LDAP as subject source for Grouper
        i. API call to have mP spit out lists of any filtered set of objects
        ii. mP provisions 3rd party identifier to Banner, Grouper uses Banner as subject
        iii. Have Grouper subscribe to 'new institutional identity created' and trigger Grouper processing
        iv. mP resource that publishes to AMQP and then any number of subscribers could tune in.
        v. SCIM connector: Keith
        vi. AMQP connector: Ethan
    b. Should Grouper and midPoint provision independently?

    c. Grouper could be the group and access management admin point
        i. it could drive midPoint organizations, roles, entitlements and groups.
        ii. It would do so by being configured as a midPoint Resource with configurable bi-directional data flows

9. (Wednesday, March 7) Credential management Controller – Drill Down (Warren)
    a. Documenting what this process is and providing clarifying information and advice
    b. WarrenC start by drawing a sketch of campus with an existing solution

c. MattB: Student admitted, SPML from Banner, push to campus ID system, student enters initial info; lets them into a Banner portal trailhead (Luminus); Intent to enroll causes Banner to fire off provisioning events to all the systems that the student will need to have access to.
d. Getting this into some generic level of detail. That cover examples / flow in general for campuses. Warren I will discuss with Matt and maybe with some others and get a strawman by next Wednesday.

10. (Wednesday, March 7) Organizations as entities (Keith)
    a. Uses for organizational structures in typical higher ed scenarios?
    b. midPoint model for organizations
    c. Grouper model for organizations
    d. COmanage model for organizations
        i. CO vs COU
        ii. Organizational hierarchies (COUs vs Departments)
    e. Can we come up with a shared conceptual model of data structures and operations that can be implemented with Grouper, COmanage and midPoint as desired? Warren & Matt
    f. Time to have solutions with real products...Working with the 10 Campus Success Program participants.

Next Meeting

Friday 1 March 2018 at 10:00 am Eastern, 7:00 am Pacific, 3 pm London

TIER APIs and Registry Working Group Agenda and Notes

Friday 23 February 2018 at **10:00 am Eastern**, 7:00 am Pacific, 3 pm London

Participants

Keith Hazelton - UW-Madison
Christopher Hoskin - University of Oxford
Jon Miner - UW-Madison
Ethan Kromhout - UNC Chapel Hill
Chris Hubing - Internet2
Warren Curry - U Fl
Nils Jacobson, Kavitha Kumar - Internet2
Jay Jordan - Internet2
James Babb - UW Madison (45 minutes late)

Agenda

1. Doodle for volunteers to work on I2GS demos: https://doodle.com/poll/6gyahf6ysng5u9zr (please reply today if interested)

2. Using Schema mapping spreadsheet to develop a representation of the TIER minimal person schema (Keith)
    a. https://gist.github.com/geszes/b63b5c3dedff2a2f702c6fd54555b9cc
    b. Schema comparison Spreadsheet
    c. RFC 7643: SCIM Core Schema
    d. Minimal registry https://spaces.internet2.edu/pages/viewpage.action?pageId=110331943
    e. in the midPoint user object
    f. In Sentrifugo

3. Setting up a new WG topic: Organizations as entities (Keith)
    a. Homework: Do we see uses for them in typical higher ed scenarios
    b. midPoint model for organizations
    c. Grouper model for organizations
    d. COmanage model for organizations

    i. CO vs COU
    ii. Organizational hierarchies
e. Time to have solutions with real products...Working with the 10 Campus Success Program participants.

4. Can we declare the Registry Update Controller – Drill Down ready for V1? https://spaces.internet2.edu/x/GYZQBw (Warren)
    a. Any quibbles, questions, suggestions?
    b. Included some material from last Friday's discussion and Chris Hoskins
    c. Eventually part of a TIER Deployment Guide or TIER Architect's Notebook
    d. For now, bring to top level on TIER Wiki
    e. JonM: In general it's exactly what we need to do, incorporate into a TIER Best Practices Guide.
    f. WarrenC: Create versions that are specific for particular software packages on how to implement these best practices

5. (Wednesday) COmanage midPoint Integration: User Story ->
    a. Exercises with a set of VMs implementing models 2 & 3, some basic user story; Practicum
        i. We have done COmanage / midPoint integrations using LDAP
        ii. What else?
    b. Technical Fit/Gap Exercise (TIER Provisioning Fit/Gap Worksheet developed by TomJ)

6. Kubernetes for COmanage orchestration (ChrisHoskins)
    a. Still learning curve; fair amount of effort expended so far, conceived of as 'version 0.1'
    b. HELM 'apt-get' for Kubernetes
    c. Handling of secrets is challenging; Bitnami package for secrets
    d. ChrisHu: had growing interest in Kubernetes, lack the cycles to make a serious move. Invite ChrisHo to contribute ideas to the COmanage packaging project. Orchestration tool of choice for distributed containerized environments

Next Meeting

- **Wednesday 28 February 2018, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC**

TIER APIs and Registry Working Group Agenda and Notes

Wednesday 21 February 2018, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

- Recording

Participants

Jim Fox - UDub
Bill Kaufman - Internet2
Michael Hodges - U of Hawaii
Warren Curry - UFlorida
Gabor Eszes - Old Dominion
Benn Oshrin - SCG
Michael Brogan (U Wash)
Brian Woods - Rice U
Jared Kosanovic - Oregon State U
Keith Hazelton - UW-Madison
Mike LaHaye - Internet2
Nils Jacobson - Internet2
Tom Jordan - UW-Madison
Jon Miner - UW-Madison (post fire alarm)
Robin Karlin - Carnegie Mellon
Ethan Kromhout - UNC Chapel Hill (as of 3:30 Eastern)
Kavitha Kumar - Internet2
Marc Miles (U Wash)

Agenda

Remember to record the meeting and send the link (please include link to last Wed (Feb 14th) meeting recording)! Another reminder is to update the link for this document in the meeting invitation email ;-)

1. Points of integration between COmanage and midPoint (Keith, BennO)
    a. Model I: COmanage as SOR and midPoint as registry and provisioning engine

b. Another model: "Map, Match, and Merge",JeremyR, BennO: Classic higher ed situation: multiple sources, need to merge info to single person record per real person;
    i. *Identity governance-like situation*

c. Another: "master data management": Like Internet2 situation: midPoint can play the role of MDM (person hub), synchronizing, reconciling information between various systems
    i. *Provisioning-like situation*
    ii. At Internet2, Salesforce used as CRM but in some other regards as a source of authoritative information (golden record)
    iii. Bi-directionality
    iv. Distinguish data that is important to provisioning decision vs just “data of interest to systems outside the one that creates and manages it. (Is this a sharp distinction)
    v. Gabor will share a summary of our current consensus

d. User Story -> Technical Fit/Gap Exercise (TIER Provisioning Fit/Gap Worksheet developed by TomJ)
    i. Exercises with a set of VMs implementing models 2 & 3, some basic user story; Practicum
        1. We have done COmanage / midPoint integrations using LDAP
        2. What else?

e. [BennO]: setup calls on the side to move this forward

2. Next steps in documenting Identity OnBoarding. (Warren)

a. Can we declare the Registry Update Controller – Drill Down ready for V1? (are we ready to remove the Draft label from https://spaces.internet2.edu/x/GYZQBw ?)
    i. Let’s see if there are open issues by Friday that keep us from declaring “Version 1”

b. Credential management Controller – Drill Down (Warren)
    i. Documenting what this process is and providing clarifying information and advice

c. Groups Update Controller – Drill down (who?)

i. Very dependent on group structure, so look for Bill Thompson's help
   1. Base thought on Grouper deployment models Basis, Reference, Application, etc… ,
   2. HTTP APIs need to be fleshed out
   3. JimF: UDub has a groups API; We've been looking for a REST API for Grouper for a loooong time; It's too hard to do from scratch
   4. "It's just sets", well, yes, but….
   5. We have APIs for managing groups and memberships
   6. What other group-related services need APIs before we can declare success on a vendor-agnostic guideline
   7. List of group that bear on provisioning and access rights
   8. New people need to be made subjects eligible to be put into groups,drive group memberships
   9. If SCIM works, it'll work with any group service implementation
   10. SCIM couples you to a particular set of required attributes
   11. [Keith] Group API review to see what the required features and operations is.
   12. We need to get specific about what we need in the realm of groups services
   13. Documenting what this process is and providing clarifying information and advice

3. A dockerized HR System of Record (Sentrifugo) for integration testing (Ethan)
   a. Open source HR system, Sentrifugo
   b. Ethan creating a fully dockerized version with containers for Sentrifugo, and MariaDB https://github.com/ekromhout/docker-sentrifugo
   c. Add AMQP tracer into the container for RabbitMQ that is coming

4. Using Schema mapping spreadsheet to develop a representation of the TIER minimal person schema (Keith)

   a. in the midPoint user object
   b. In Sentrifugo

➢ Brief discussion around Global Summit time slots for the T&I Showcase.
   a. First offer is for 12 noon - 1:15pm each day
      i. Benn: direct conflict with COmanage BOF Tuesday - will send note to Kelly
      ii. Warren: could be somewhat positive for folks that don't want to miss other sessions but likely more negative since many like to meet for lunch to have chats and also there are CIOish activities planned around lunch

iii. Bill: will review full T&I Track in detail, talk to Ann, and see what other options we can find to fit in w/o direct conflict, perhaps using some of lunch time or not.

Next Meeting

Friday 23 February 2018 at 10:00 am Eastern, 7:00 am Pacific, 3 pm London

TIER APIs and Registry Working Group Agenda and Notes

Friday 16 February 2018 at **10:00 am Eastern**, 7:00 am Pacific, 3 pm London

Participants

Keith Hazelton - UW-Madison (Last ½ hour only)
Warren Curry - U Florida
Benn Oshrin - SCG
James Babb - UW Madison
Jon Miner - UW Laguna Beach
Chris Hyzer - Penn

Christopher Hoskin - University of Oxford
Ethan Kromhout - UNC Chapel Hill

Robin Karlin - Carnegie Mellon University

Agenda

1. Registry Update Controller - ID match: Detailed process description (Warren)
    a. https://spaces.internet2.edu/pages/viewpage.action?pageId=122717721
    b. Small word change to possible matches to potential matches - done
    c. Discussed the Identity Match UI (out of box) version being developed by SCT. It will provide basic abilities to set configuration and to resolve identity potential matches.
        i. It will work with direct data access and make use of internal tools.
        ii. Discussed that institutions should review this before considering what they need beyond the delivered tolling.
        iii. Institutional tools will be able to use api calls to build custom resolution UI
    d. Notion of the owner of the identity being able to contribute to the resolution came from Christopher Hoskin and Jon Miner . Discussed issues involved with this approach.
        i. Jon - Wisconsin Linking Key was discussed that is provided to the identity owner. They can use it to assist if they can log in to service.
        ii. Discussed care needed so that abuse does not occur.
        iii. Oxford may provide additional detail on there concept.
        iv. Warren - added the notion of the identity owner assisting in resolution to the document.
2. (When Keith joins the call) Non-person entities in the Registry: “Services” in midPoint

Thank you Pavol,

I'm sorry I haven't responded sooner. I've been working on other projects, and other parts of midPoint.

I've setup some "Services" and those are working great for what we need. I'm hoping to start work on the delegated admin aspects soon. Thanks for sending the URIs.
Have a great day!
Brad

On 2/5/18, 11:03 AM, Pavol Mederly wrote:

Hello Brad,
looking at the source code I would say that correct URIs for services are

- ...#servicesAll
- ...#services
- ...#service

(analogous to #rolesAll, #roles, #role). But please try if it works as expected.

As for the conceptual question about using services instead of roles: I think it might be a good idea, even if I haven't heard of anyone doing that before. :) Please have a look at this page: https://wiki.evolveum.com/display/midPoint/Roles%2C+Services+and+Orgs (I think you maybe already did that.)

Technically, the main difference between RoleType, ServiceType, and OrgType is that midPoint maintains a closure table for OrgType objects in order to quickly answer queries like "is X a child of Y (potentially via more intermediaries)?" Besides that, all of them can carry inducements, authorizations, mappings, etc - as these are defined in parent type called AbstractRoleType.

So, yes, maybe using services instead of roles might be a good idea. Perhaps Radovan could comment on this as well after returning from TIIME meeting.

Pavol Mederly
Software developer
evolveum.com

On 02.02.2018 1:14, Brad Firestone wrote:
Hello,

I am planning to make use of Services in place of Roles to grant users access to a "service" that we provide. An example might be "Email". If I understand correctly, it seems like this is a

good use of Services since I'm giving access to a service. If I used Roles, I would probably assign the Role: Email User. Services just seems more natural. If I'm not understanding Services correctly, please let me know.

My other question is how to assign the correct authorizations for a "delegated administrator" to be able to work with Services. On the wiki page:

https://wiki.evolveum.com/display/midPoint/GUI+Authorizations

I find the list of all the actions including Org, Roles, and many others. But I don't see "Services" anywhere in the list. So I'm not sure how to grant authorization for the delegated administrator to work with Services. If it's not possible without giving "all" access, that's okay. I just want to know before I go too far into setting up Services.

Thank you!
Brad

Next Meeting

- **Wednesday 21 February 2018, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC**

TIER APIs and Registry Working Group Agenda and Notes

Wednesday 14 February 2018, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

- Recording

Participants

Warren Curry - UFlorida
Jared Kosanovic - kosanovj@oregonstate.edu - Oregon State U
Jim Fox - UDub
Keith Hazelton - UW-Madison
Michael Hodges - U of Hawaii
Matt Brookover - CO School of Mines
Gabor Eszes - Old Dominion
Michael Brogan - U Wash
Nils Jacobson, Kavitha Kumar, IJ, Sudip Guha, Jay Jordan- Internet2
Benn Oshrin - SCG
Ethan Kromhout - UNC Chapel Hill
Shilen Patel - Duke
Dean Lane - Rice
Robin

Agenda

1. List steps, assign tasks: Create an instance of the Alpha version of the TIER multi-purpose Grouper container for WG dev work.
    a. Get an instance for the working Group up
    b. Do we know steps for doing it.
    c. Is there someone able/ willing to do it?
        i. Keith to contact Packaging WG to see if useful..
        ii. Bill K to research where to put the install.
        iii. Someone to load it to the testbed instance,
            1. Ethan K (UNC) volunteer to install.. He is a Grouper novice so it should serve as a good test.
        iv. Similar step for Midpoint after midPoint training

2. Schema work: Request and response bodies for TIER APIs

    a. OpenAPI Initiative 3.0-based specification;

i. Gabor E, Ethan K, Jim F and Keith H (AI)

b. Open source SCIM implementations
   i. Ping open source SCIM 2 implementation (based on UnboundID work)
   ii. Charon: open source SCIM 2 SDK, server and client code from WSO2
      1. Build your own SCIM implementation with WSO2 Charon
   iii. Open Source IAM (OSIAM) on github including documentation
   iv. Grouper's SCIM library is Penn State's SCIM 2.0 package
   v. Create specification for Registry Update Controller per Tom's diagram

c. The controllers are independent components
d. They should be implemented by the Registry providers, not by TIER WG staff
e. GaborE: Would something like this level of granularity be a valid deliverable under the TIER; As a group we are unintentionally non-committal about whether code gets delivered; What's our decision?
f. Warren working on a drill-down version of this diagram, and yes, it's a good TIER deliverable; We have to facilitate the production of running code to implement the diagrams, WG members are not intended to take on the software development role. Campus Success
g. COmanage team and midPoint team would be good candidates to provide the implementations
h. GaborE: The task "Create specification" is ours; But the diagrams are valuable deliverables in themselves.
i. GaborE, Warren, TomJ take the lead on the specifications and the diagrams

3. New Environment Goal: Containerized COmanage as SoR feeding containerized midPoint Registry and Provisioning Engine;

4. Jared Kosanovic: API developments at Oregon State University (recruited by
   a. Message-driven API and campus-locations API
   b. Some of the ways we design and present our APIs.
   c. JSON:API is their chosen specification language
   d. Dropwizard Java framework for implementing APIs
   e. Swagger for documentation
   f. /locations endpoint
      i. https://github.com/osu-mist/locations-frontend-api/blob/develop/swagger.yaml
   g. Elasticsearch as repo
   h. Multiple data sources normalized under a single endpoint, locations; hides complex data environment from users
   i. A locally developed API (inspired by BYU) as the integration point for their RabbitMQ messaging service

    i. Our message API is being used in production but we are in the process of implementing all of the authorization endpoints. I will be sure to share some documentation/code when I am able. -Jared
  j. BYU events hub;
  k. Identify API to get a UserID from ID on an RFID chip in the ID card
  l. The api gateway is Apigee
    i. Vendor/system accounts are done differently; this is mostly used for user-owned access
  m. The event endpoint is dumb pipes with smart endpoints; schema definitions a work-in-progress and up to the endpoints
  n. Use API Gateway to manage access; different endpoints for different subsets of a resource based on access rights.
  o. Encryption of messages? All API traffic is over TLS 1.2, but not with client keys; message would link to an API call for finer grained
  p. Gabor: Say you have a mobile app, you need to authN a call to backend. How do you solve it? TBD, most stuff is public so not sensitive yet.
  q. All API calls are authenticated using Oauth2 client credentials. An exception is some event producing applications within the message API. Some third-party vendors can only send events to a web service using basic auth. - Jared

5. NOTE: New Campus Success Program SIG on Banner to midPoint integration--implementing our WG's' proposed architecture for Multiple SoRs to Registry, and the associated graphic, TIER Entity Registry -- Identity Onboarding
  a. Matt Brookover: The work is just getting started
  b. Banner: Old Dominion has it too; Is Banner special in some way? Only in that a number of schools have Banner and they ideally want to share a midPoint connector, so alignment on schema is a good thing

6. NOTE on AMQP support in RabbitMQ: The latest release of RabbitMQ, 3.7, includes a Shovel plugin. The new plugin supports AMQP 1.0 endpoints in both directions (as a source and destinations) to complement its native AMQP 0.9.1 support. This means that Shovel now can move messages from an AMQP 1.0 only broker to RabbitMQ or vice versa. See https://www.rabbitmq.com/blog/2018/02/05/whats-new-in-rabbitmq-3-7/

7. Question from Rice: Sentrifugo was used in one of the WG demos. Does anyone know if this component is available for download as used in the demo? Or some pointers to it's configuration for the demo? Someone who we might be able to talk to? Ethan will reach out to Dean Lane.

TIER APIs and Registry Working Group Agenda and Notes

Next Meeting

Friday 16 February 2018 at 11:00 am Eastern, 8:00 am Pacific, 4 pm London

- **NOTE: Start time delayed one hour this time only;**

TIER APIs and Registry Working Group Agenda and Notes

Friday 9 February 2018 at **10:00 am Eastern**, **7:00 am Pacific, 3 pm London**

Participants

Keith Hazelton - UW-Madison
Dean Lane - Rice
Alexander Dutton - Oxford
Christopher Hoskin - Oxford
Bill Thompson - Lafayette
Jon Miner - UW-Madison
James Babb - UW-Madison
Bill Kaufman - Internet2
Matt Brookover - Colorado School of Mines
Chris Hubing - Internet2
Keith Wessel - University of Illinois at Urbana-Champaign

Agenda

1. Did the Campus Success Program Face-to-Face earlier this week suggest changes to any of our WG priorities or planned deliverables?
    a. Links to scribing docs for the breakout sessions at the CSP F2F

2. midPoint - COmanage

    a. Choose one? Use both?
        i. Participating campuses plans include COmanage only, midPoint only and COmanage as a System of Record with midPoint as Registry,

        ii. Several sites will start with one package with plans to add the other into the mix later

    b. midPoint project plans;
        i. Early steps toward forming a midPoint Special Interest Group to share experience and advice, choose common approaches where possible

        ii. A multi-campus technical evaluation plan; Janemarie Duh and Carl Waldbieser will take lead (Bill Thompson reporting)

    c. midPoint - Banner integration; kernel of wiki page

- Identity Onboarding Requirements:
  Action Item: After discussions around Identity Matching, Rest APIs, and Integrations with multiple SORs, the group identified an action to define requirements and methods around Identity Onboarding.

  Lead: Matthew Brookover, Colorado School of Mines

  Discussion: Among the topics explored were:
  Determine patterns for the integration of Banner with midPoint (midPoint is a component recently adopted by TIER that can serve as a Registry and Provisioning engine).
  Evaluate the ID Match service effort under way in TIER.
  Collaborate on the emerging TIER architecture for SoR ID Matching and Registry.
  Determine the potential use of RESTful connectors with midPoint and determine the priorities for different connectors following the midPoint training that many schools are undergoing at the end of February 2018.

d. Identity Matching strategies with midPoint as Registry

e. Working group on Grouper (Bert Bee-Lindgren is intrigued with Grouper Training Environment Start)
   i. Grouper → Liam Hoekenga (UofM)
      - Implementation Checklist
      - Enhanced deployment guide
      - Prioritization process
      - Subject adapter for midPoint (?)
      - Loader jobs sourced from Banner (anyone could template out the queries, not just Grouper team)

3. Alex's IdM/onboarding demo http://github.com/alexsdutton/idm
   a. Current vision: COmanage as Registry (minimize the distinction between traditional affiliations and new populations (guests, collaborative researchers), midPoint as Provisioning Engine

4. Provisioning and De-Provisioning

   a. CSP F2F session
      i. Establish and maintain a T&I community collection of connectors

b. BTAA provisioning WG offer to launch investigative work on bulk operations over APIs to help with the bursty streams of changes in higher ed (semester transition, etc) (Keith Wessel)
    i. Bulk provisioning and de-provisioning; Goes hand-in-hand with SCIM work; also a natural place to define best practices
    ii. BTAA will concentrate on requirements for bulk operations (initial data migrations, old-fashioned daily reloads from System of Record; Reconciliation to fix unsynced repositories; Semester churn, Graduation turnover is another classic example
c. Widely seen as a recurring problem with lots of one-off solutions; UW-Madison, CO School of Mines, U Ill. 1,000s of new students who are looking for their NetIDs the morning after the semester load. It's a race they haven't always won.Hoping to move to an on-demand where students get their NetID when they accept an admission offer.
d. James, Jon: ran out of 3-digit numbers to append to names to form NetID
e. Oxford: 8 character username: org bit at front, limits coming up
f. Namespace pollution

5. BTAA project to collect and catalog SCIM schemas (Keith Wessel)

    a. Working on evaluation strategy for Provisioning and De-Provisioning in general
    b. About to start, the effort is part detective work, part research
    c. Goal is to get SCIM schema all into one place; Mostly in form of SCIM-compliant extensions
    d. BTAA and TIER will collaborate on the work and on disseminating the results; These will be pushed to Internet2 GitHub

Chat window
https://docs.google.com/document/d/1zDK5oJjMmPda0M57KBcdnyXu3uXrafWf2HlzNAxc7k0/edit Alexander Dutton https://wiki.evolveum.com/display/midPoint/Provisioning+Standards "SCIM is an IETF effort that targets almost the same problem as SPML. Unfortunately SCIM is repeating almost all the mistakes of SPML." ☹ Christopher Hoskin https://www.imsglobal.org/activity/onerosterlis

https://www.businesswire.com/news/home/20160524005521/en (not heard of clever before)

Next Meeting

Wednesday 14 February 2018, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

8. Note: New Campus Success Program SIG on Banner to midPoint integration--implementing our WG's' proposed architecture for Multiple SoRs to Registry, and the associated graphic, TIER Entity Registry -- Identity Onboarding

TIER APIs and Registry Working Group Agenda and Notes

Friday 2 February 2018 at 10:00 am Eastern, 7:00 am Pacific, 3 pm London

Participants

Warren Curry - U Florida
James Babb - UW Madison
Bill Kaufman - Internet2
Keith Hazelton - UW-Madison
Chris Hyzer - Penn
Christopher Hoskin - University of Oxford
Alex Dutton - University of Oxford
Benn Oshrin - SCG (first hour only)
Jon Miner - UW-Madison
Paul Caskey - Internet2
Tom Jordan - UW-Madison
IJ Kim, Jay Jordan, Kavitha Kumar, Mike LaHaye, Nils Jacobson - Internet2

Agenda

1. Steps 1 - 6 on the Architecture diagram as a how-to DRAFT in Progress on ID Match processes (Warren)
    a. Discussion on how we would want to match, what do do with people of "questionable providence"
    b. How to communicate downstream that an identity might not be "complete" or might have a match?
        i. How does this dovetail with LOA?
        ii. Assurance vectors
        iii. OSU: Everything that makes it in has high assurance
    c. General agreement that this goes along with how we have looked at this in the past.

Next Meeting

Wednesday 7 February 2018, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

TIER APIs and Registry Working Group Agenda and Notes

Wednesday 31 January 2018, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

Participants

Christopher Hoskin - University of Oxford
Michael Hodges - U of Hawaii
Jim Fox - UDub
Keith Hazelton - UW-Madison
Ethan Kromhout - UNC Chapel Hill
Bill Kaufman - Internet2
Nils Jacobson - Internet2\
MIchael Brogan - U Wash
Gabor Eszes - Old Dominion
Benn Oshrin - SCG
Chris Hubing - Internet2

Kavitha Kumar - Internet2
Jon Miner - UW-Madison (first hour)
Warren Curry - UFlorida
Paul Caskey - Internet2 (must leave at top of hour)
Robin …..
Adrian C...

Agenda

1. COmanage / midPoint division of labor
    - I. COmanage only
        - Suitable for typical Virtual Organizations, order of 100 participants;
    - II. COmanage Primary, midPoint Downstream
    - III midPoint Primary, COmanage Upstream
    - IV midPoint Primary, COmanage Downstream
    - V midPoint only

b. Where does Salesforce fit in the Internet2 platform project?

c. Benn's starter page on the topic
    - Is the Grouper Deployment Guide a good model for addressing this issue? General sentiment is yes, potential TIER adopters would find a Deployment Guide on COmanage/midPoint

I'm putting together a summary of planned architectures at

> various institutions. A first question I'd like to hear about is COmanage / midPoint and the various ways they can be leveraged.
>
> There are 5 very high level alternatives mapped out here: https://spaces.internet2.edu/x/kIVQBw Please share with this group your direction with respect to these two packages. Have you settled on a model? What would help you choose one?
>
> --Keith on I2 Slack tier-peers channel.

- Compare and contrast with this diagram: (TIER ENTITY REGISTRY - IDENTITY ONBOARDING with Messaging Flow)
- https://drive.google.com/open?id=158tp5wx9vfCIsAo6mjHk-Tv41e8vjkL5

d. Fit-gap Grouper/COmanage/midPoint: (March, 2017)
e. COmanage Feature List (from recent presentation)
f. midPoint Feature List
g. Evolveum: Feature comparison of midPoint and other open source IAM suites

2. Primary API and Registry WG Projects 2018 Task list review

a. Provisioning
   - Deliverable: A COmanage - midPoint Connector
     - Don't look in the COmanage blackbox
     - Write a COmanage to midPoint connector
     - Pull model from midPoint
     - Write a midPoint to COmanage connector
       - COmanage has a REST API, but we may want something more like SCIM
     - Event Message: midPoint, COmanage would need
       - Show me all the changes since this point-in-time
     - Other Connectors
       - Slack, LucidChart, SalesForce (SF-midPoint Connector), ...
b. API Guidelines
   - RESTful access to the Person Registry
   - Architecture diagram as a guide to design
c. Schema and extension mechanisms
   -
d. Event-driven messaging
   -

TIER APIs and Registry Working Group Agenda and Notes

Next Meeting

Friday 2 February 2018 at **10:00 am Eastern**, 7:00 am Pacific, 3 pm London

- Steps 1 - 6 on the Architecture diagram as a how-to DRAFT in Progress on ID Match processes (Warren)

TIER APIs and Registry Working Group Agenda and Notes

Friday 26 January 2018 at 10:00 am Eastern, 7:00 am Pacific, 3 pm London

Participants

Igor Farinic - Evolveum
Keith Hazelton - UW-Madison
Ethan Kromhout - UNC Chapel Hill
James Babb - UW Madison
Bill Kaufman - Internet2
Warren Curry - U-Florida
Jim Jokl - U-Virginia
Jon Miner - UW-Madison (audio only, first 30-ish)
Christopher Hoskin — Oxford
Alexander Dutton — Oxford
Benn Oshrin - SCG
Chris Hyzer - Penn

Agenda

1. midPoint training discussion (Igor Farinic, Evolveum CEO)
    a. Use of Docker image for workstation install of midPoint
        i. Evolveum devs to join tier-packaging channel?
        ii. BillK will add Igor, Radovan to tier-packaging mailing list
    b. Deployment Fundamentals training
    c. Normalizing of person schema across systems of record; How would you approach that with midPoint resources and shadow accounts as part of the identity reconciliation process; See diagram of SoRs to midPoint
    d. Igor: we can add material on that to upcoming training; we do want to cover bootstrapping
    e. Three-day training specifically on Connectors; Think of connectors as protocol transformations; JimJ: Could remote connectors be used as an integration point for messaging? IgorF: Yes.
    f. Install Eclipse plugin as a prerequisite;
    g. Want to get the training group to be up to speed having the Docker images up and running prior to starting the training; Two hour setup on the Friday before training to get everything set up on trainee's machines
    h. Will be using Zoom and can keep chats, do screen sharing and so on
    i. Specifics on docker and vms will be decided by Monday, Jan. 29.
    j. 10 people per group, groups A & B

k. Dates for training being finalized
    i. 2 groups A & B
        1. The training would be weeks 2/19-23 and 2/26-3/2 (there may be a little flexibility here)
        2. Training would be split to be
            a. Group A (2) days week 1 and (3) days week 2
            b. Group B (3) days week 1 and (2) days week 2

l. What about SME/Lab assistants in addition to formal trainees? Bill & Igor will discuss. A way to keep the numbers to 10 per group, but allow I2 types to assist

2. Oxford IAM Adventures (Chris and Alex)
    a. Architecture diagrams, person registry design
        i. Use of Essential Project; Looking for suitable tools. Oxford uses data and processing modeling (CaseWise); New Enterprise IT Architecture position (officially, we can't do EA in an IT Service department, hence "IT" in the job title); He had a different tool; Graphviz, PlantUML, Archi for Archimate; Modellio; Casewise bought by ErwinBP, plain HTML5 used for the diagrams they shared. Service Design Model;
        ii. Target IAM architecture
        (We got this from https://techvisionresearch.com/iam-reference-architecture/)
        iii. midPoint, COmanage capability map
        iv. Identity Management Done Right: A User-Centric Approach
        v. Chris, General Data Protection Regulation (GDPR) training last week in London
        vi. Using Kubernetes to manage Docker containers and Terraform to set it up; VLE being selected; their current option is Sakai. Are there any institutions using Grouper with their LMS; U Penn uses Grouper with Canvas; UW-Madison demoed Grouper with Canvas; UNC finishing a project using O365 groups managed by Grouper and used by Sakai; Ask Grouper users list or EDUCAUSE IdM list; Warren: U Fl doing same as UNC
        vii. Approach to roles;
            1. Recommended reading: Grouper Deployment Guide V1.
    b. Upcoming Proof of Concept at Oxford
        i. AWS (Terraform, Kubernetes) http://comanage.ops.cshoskin.net/registry/
        ii. Still in planning stages; get anonymized data from colleges, from HR, Microsoft BizTalk as ESB; Now in transition to other products;
        iii. Event-driven messaging is gaining in popularity over ESB
    c. Chris Hoskin dockerized version of Essential Project: How-to tips

3. Trust and Identity Showcases for 2018 Global Summit, May, San Diego

a. BillT mentioned, SteveZ, AnnW, KevinM very supportive
b. Should we propose 1, 2 or 3 Showcase sessions? TechEx did the one big demo version; 3-4 20-25 minute showcases; (Working meetings, not track sessions):
c. Warren: Maybe two sessions, Showcase Part 1, Showcase Part 2, 60-90 minutes in length
    i. Intake processes--SoR to Person Registry (see diagram);
    ii. Output side: Provisioning & SAML attribute delivery
d. Ann might propose a Showcase part 3 (Campus success program presentation)

As many/most of you know we determined that “demos” no longer suffices for all of the quality work that many of you have put into the development of TIER middleware software to present to the Community are Global Summit and the Technical Exchange.

The WG members determined that “Showcase” was a better description going forward and as the TIER Initiative will move to a sustainable portion of the Trust & Identity Program, the thought was to demonstrate the most current developments as a T&I Showcase during the primary program days of Global Summit intermixed with T&I Track Sessions as a Working Meeting.

This will allow discussion and good Q&A as the desire is to put these artifacts into the hands of others who may develop their own internal MVPs etc.

While we will likely retain some flexibility in the final venue, we must submit our best guess as to how we would like to organize and present the Showcase, either as 1 major session with multiple demonstrations, or spread over 2 or even 3 sessions.

This submission is due Friday, January 26th. We have discussed this several times during WG calls and likely will discuss briefly during Friday’s call, but I wanted to give everyone a chance to chime in.

To that end I have created a Doodle Poll to get your feedback.

The poll is at https://doodle.com/poll/5xg67zqv2wtmepbc

Thanks for your feedback!

Best regards
--
Bill Kaufman

4. Task list review for additional 2018 deliverables
    a. Provisioning
    b. API Guidelines

   c. Schema and extension mechanisms
   d. Event-driven messaging

Next Meeting

Wednesday 31 January 2018, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

3. Task list review for additional 2018 deliverables
   a. Provisioning
   b. API Guidelines
   c. Schema and extension mechanisms
   d. Event-driven messaging

Friday 2 February 2018 at 10:00 am Eastern, 7:00 am Pacific, 3 pm London

- COmanage / midPoint division of labor, continued;

TIER APIs and Registry Working Group Agenda and Notes

Wednesday 24 January 2018, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

Participants

Warren Curry UFlorida
Benn Oshrin - SCG
Bill Kaufman - Internet2
Jon Miner - UW Madison
James Babb - UW Madison
Keith Hazelton - UW-Madison
Ethan Kromhout - UNC Chapel Hill
Jim Fox - UDub
Michael Hodges - U of Hawaii
MIchael Brogan - U Wash
Tom Jordan - UW Madison
Paul Caskey - Internet2
Gabor Eszes - Old Dominion

Agenda

1. ID Match Implementation Tasks including schema (Benn, Warren)
    a. ID Match Attributes (may not be a complete set so if you have opinions on additional or different attributes please use the email list to discuss)
        i. Enterprise or Campus “system” id? - Warren: arch diagram refers to the institutional ID (would like to keep terms consistent)
        ii. Note the Cifer Core Schema is what the POC was originally built on
        iii. Schema crosswalk table as reference
        iv. Gabor’s Gist as reference
        v. Parking lot issues
            1. SOR system identifier handling
            2. DoB not defined in SCIM core
            3. Name is single-value in SCIM core
            4. How to carry other identifiers…
            5. Is reg controller responsible for picking up on the results of human evaluation of potential matches?
            6. Weird local identifiers other than the institutional one.
        vi. Registry controller can be seen the orchestration agent for the ID Matching functionality; Is it registry controller’s job to tell other systems about any consequent registry changes? Yes, probably via event message publications
        vii. If I want info about the matching database, can I get it?

TIER APIs and Registry Working Group Agenda and Notes

1. https://spaces.internet2.edu/display/cifer/SOR-Registry+Strawman+ID+Match+API#SOR-RegistryStrawmanIDMatchAPI-RequestPendingMatches
2. https://spaces.internet2.edu/display/cifer/SOR-Registry+Strawman+ID+Match+API#SOR-RegistryStrawmanIDMatchAPI-Request:SearchOnly
3. https://spaces.internet2.edu/display/cifer/SOR-Registry+Strawman+ID+Match+API#SOR-RegistryStrawmanIDMatchAPI-ForcedReconciliationRequest

2. Additional midPoint topics we'd like to see covered as part of the Evolveum training sessions
    a. Discussed in TIER Packaging
        i. Use docker version of midPoint in their VM
        ii. Still provide their VM with demo files, etc., etc.
        iii. Longer-term container design using docker secrets - TIER philosophy
        iv. Connector Development vs Message variance by SOR and a common messaging format.
        v. Book
    b. Tee-up the topics for Friday morning WG call

3. Fit between local work and TIER deliverables Primary API and Registry WG Projects 2018
    a. Dave Schafer is lead for planning this
    b. BTAA provisioning

4. Chris Hoskins has a dockerized version of the open source Essential Project. Is there interest in such a architecture modeling tool?

Notes from BlueJeans chat window
Message from Benjamin Oshrin: https://spaces.internet2.edu/display/cifer/SOR-Registry+Strawman+ID+Match+API#SOR-RegistryStrawmanIDMatchAPI-RequestPendingMatcheshttps://spaces.internet2.edu/display/cifer/SOR-Registry+Strawman+ID+Match+API#SOR-RegistryStrawmanIDMatchAPI-RequestPendingMatches Message from Benjamin Oshrin: https://spaces.internet2.edu/display/cifer/SOR-Registry+Strawman+ID+Match+API#SOR-RegistryStrawmanIDMatchAPI-Request:SearchOnlyhttps://spaces.internet2.edu/display/cifer/

SOR-Registry+Strawman+ID+Match+API#SOR-RegistryStrawmanIDMatchAPI-Request:SearchOnly

Message from Benjamin Oshrin:
https://spaces.internet2.edu/display/cifer/SOR-Registry+Strawman+ID+Match+API#SOR-RegistryStrawmanIDMatchAPI-ForcedReconciliationRequesthttps://spaces.internet2.edu/display/cifer/SOR-Registry+Strawman+ID+Match+API#SOR-RegistryStrawmanIDMatchAPI-ForcedReconciliationRequest

Message from Ethan Kromhout: The notion of midPoint doing the standardizing of the input makes sense to me, but does probably break the idea of a simple multi purpose messaging connector. Seems like you would need on customized to the message format of each SOR.

TIER APIs and Registry Working Group Agenda and Notes

Friday 19 January 2018 at **10:00 am Eastern**, 7:00 am Pacific, 3 pm London

Participants

Keith Hazelton - UW-Madison
Dean Lane - Rice
Ethan Kromhout - UNC Chapel Hill
Jon Miner - UW-Madison
Bill Kaufman - Internet2
Bill Thompson - Lafayette College
Tom Jordan - UW-Madison
Alexander Dutton - Oxford
Christopher Hoskin - Oxford
James Babb - UW Madison
Paul Caskey - Internet2
Warren Curry - U Fl

Agenda

1. Finalizing initial set of schema specifications (Gabor, Keith)
    a. Schema crosswalk table as reference
    b. Latest schema model from OpenAPI 3.0
    c. Proposal: Use these models to formalize SCIM resource representations and for any additional resources and extensions TIER defines
    d. Latest JSON schema proposal on which OpenAPI 3.0 schema is modeled
        i. draft-handrews-json-schema-00 (core)
        ii. draft-handrews-json-schema-validation-00
        iii. draft-handrews-json-schema-hyperschema-00
        iv. draft-handrews-relative-json-pointer-00
    e. Gabor's Gist
    f. Grouper API schema; The TIER-style APIs for Grouper User, Group and Membership are stable, and there is an OpenAPI (Swagger) specification for them.

> **From:** Brian Savage <brian.savage@bc.edu>
> **Reply-To:** "brian.savage@bc.edu" <brian.savage@bc.edu>
> **Date:** Wednesday, May 4, 2016 at 10:59
> **To:** TIER-API <tier-api@internet2.edu>

TIER APIs and Registry Working Group Agenda and Notes

Subject: [tier-api] Swagger and TIER basic group operations

Hi,

Here's another swagger 2.0 example but closer to home...
I used the basic group operations Chris had documented here:
https://spaces.internet2.edu/display/DSAWG/TIER+API+SCIM+user+groups
and here:
spaces.internet2.edu/display/DSAWG/TIER+API+SCIM+group+members
as fodder for creating a basic swagger spec (it certainly doesn't accurately include nuances of ongoing TIER API discussions but may be close to the two basic operations previously described).

You should be able to go to editor.swagger.io
and File-Import URL from here:
https://gist.githubusercontent.com/bsavage/31a2e90ef377fde70e00814babf3da89/raw/48f8a597a43c7e63cd000cf413688b0f8b3ce5dd/tierBasicGroupsSwagger.yaml

Cheers,
Brian Savage

g. Get a single wiki page with pointers to the completed work items

2. Review, comment on Grouper Deployment Guide V.2 revised draft on the Grouper Training Environment (Bill Thompson)
    a. see notes/comments in the draft

3. What TIER topics would be of most interest to our new Oxford representatives? (Chris, Alex)
    a. Chris and Alex have both been added to the email lists
    b. Project Board meeting; EA advocating leveraging TIER; Over next 10 weeks put together a PoC, prototype. COmanage up & running; make it available to try out. Colleges to produce some test data to do more realistic trials;
    c. Chris has to put together arch diagrams, designs of person registry;
    d. Looking for a better sense of COmanage/Grouper/MidPoint; How to use them together to best advantage; BennO has been working on this
    e. Lafayette: Non-traditional students, guests, managed with COmanage which also manages LDAP registry;

f. Campus Success Program folks: many interested in midPoint, some interested in COmanage
g. As you come across an integration use case, post it to Slack, mailing lists; Some sites might come back with experiences or tools https://hub.docker.com/r/mans0954/
h. TIER GitHub demo work https://github.internet2.edu/TIER

Oxford Links

http://www.tei-c.org/release/doc/tei-p5-doc/en/html/ref-persName.html

http://users.ox.ac.uk/~iamsm/target-architecture/data/name/ (ask the list for demo credentials)

https://hub.docker.com/r/mans0954/

https://github.com/mans0954

TIER APIs and Registry Working Group Agenda and Notes

Wednesday 17 January 2018, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

Participants

Warren Curry - UFlorida
Keith Hazelton - UW-Madison
Ethan Kromhout - UNC Chapel Hill (Will have to leave just before 4:00)
Bill Kaufman - Internet2
Michael Hodges - U of Hawaii
Jim Fox - UDub
Carey Black - tOSU
Michael Brogan - UWash
Benn Oshrin - SCG
Tom Jordan - UW-Madison
Gabor Eszes - Old Dominion
Paul Caskey - Internet2

Agenda

1. Review documents for Id Match, define tasks toward production mode
    a. SOR-Registry Strawman ID Match API https://spaces.internet2.edu/display/cifer/SOR-Registry+Strawman+ID+Match+API
    b. ID Match PoC - This is from tech ex -
        i. The term ‘canonical rule:’ rules that define a definitive yes/no match event
        ii. The term ‘potential rule’: rules that define possible fuzzy matches https://spaces.internet2.edu/display/TIERENTREG/ID+Match+PoC
        iii. Two categories of rules: canonical rule: generates a match or no match; potential rule: Rules that can only generate fuzzy matches; Canonical rules are applied first, if no definitive answer, then invoke the potential rules. The API draft included a confidence field, but it was not implemented in the ID Match PoC.
    c. ID Match Strawman - Flow https://wiki.jasig.org/download/attachments/50858970/id-match-flow.png?api=v2
    d. ID Match Scoping - matrix of https://docs.google.com/spreadsheets/d/1hENmQWbykyiKCdwu-Pz4qCYLeTfSki2PYfCl8tJRmx0/edit#gid=0
    e. What attributes can/will be used:in the matching process; Needs to be reviewed in light of our focus on SCIM; align attributes with SCIM (Links from Gabor below)
        i. https://spaces.internet2.edu/display/DSAWG/Entity+Registry+Record+Merge (inspired by

https://spaces.internet2.edu/display/DSAWG/New+person+from+institutional+source)
   ii. https://gist.github.com/geszes/b63b5c3dedff2a2f702c6fd54555b9cc
f. The component that invokes the Match engine is the decision maker. The ID Match API provides the data on the basis of which the decision is made.
g. Functional integration points: think of name-change scenario; get re-added to another SoR later; Match engine will only know about the older name; Resolution of potential match, once it's resolved it has to get back to the Match Engine. Alternatively the Match engine could have a UI that admins use
h. COmanage has lightweight matching now; eventually it will use the Match Engine with UI. Do attribute synchronization via provisioning acts.
i. How much data does the Match Engine carry natively? All of it. No callouts to Registry. General intent, the Registry will be the proxy for the SoR role; Phase 1 we're treating IdMatch repo as carrying an accurate representation of current SoR data.
j. Is data that match engine works on, is it a window on results of other matches or a window on the SoRs; under the hood, 1 giant table, when a record comes in, attach an SoR label and insert a row. If there's a reference id, a successful match operation.
k. Action Items / Tasks: Review the materials linked from item e. Above (thanks, Gabor); Goal for Wednesday: determination of how the Match Engine will do its work; Warren will produce a strawman. Match Engine V1 will include a minimal administrative UI;

2. Brainstorming content for Global summit (May 6-9, San Diego)
   a. Think TIER Showcase(s), something beyond TIER Demos
      i. Kevin/Ann/Steve propose Trust & Identity Showcase
      ii. Have the option for large room 1 or more days in parallel with the main program
         1. How many folks would be optimal? 40/60/80/100/more ?
         2. (1) long session for 2 or 3 demonstrations or multiple sessions with each focused on a single demonstration
         3. Probably want to look at T&I Track and avoid collisions
   b. Let's see what the T&I track sessions [AI] - Bill to get, end up being; Shape our showcase(s) in the light of that.
   c. If we have a predominantly decision-maker audience, we don't want a long, tech
      i. Steve Zoppi note to TIER Component Architects
         1. *Our usual targets of Global Summit and Technology Exchange will continue to be our delivery checkpoints with a couple of possible changes:*
            We will probably not continue to use the ends of those meetings as we have in the past for developer me etings. Mostly – due

to everyone's fatigue by the end of the events, but because we may be able to create more convenient vehicles between those events to achieve the same goals.
Instead, we will consider a more "harmonized" series of sessions which currently exist as separate sessions by component. In other words, it may be more useful to consider consolidation of separate, component-oriented BOFs and dev meeting times into sessions that span more than one component and focus on "activities and outcomes" rather than just the components. Your inputs will be crucial in determining how we best allocate time for these two member meetings.
Global Summit and Technology Exchange will be used to Showcase your collective work – ***How do we best do this?***

1)

3. Epics, Stories and Story Points as Agile Project Management tools for our 2018 work
    a. TIER-API Agile Board

4. Upcoming midPoint training opportunity
    a. Prioritize for Campus Success program
    b. End of feb first week of March, two groupings. A - B
    c. Info is at https://docs.google.com/document/d/1XCIMvK01cxxRGZW3SmTSVvZEaHwvrgwkftbNVNLr8QM/edit?usp=sharing
    d. Campus Success Folks have the priority

5. Feasibility of using COmanage as an invitation/guest SoR integrated with other SoRs feeding midPoint as person registry and provisioning engine
    a. Lafayette is taking this path; COmanage as a guest registry; Banner is SoR for the standards fac/staff/student populations;
    b. COmanage writes to LDAP at Lafayette
    c. Alternative modes: LDAP first, then mP; build midPoint messaging or ConnID connectors for COmanage.
    d. Architect per the diagram we have been developing
    e. Carey: What are the reasons for using COmanage + midPoint vs just midPoint or just COmanage
        i. Organizational sources (SoR)
        ii. Enrollment flows for bringing in guests of many sorts
            1. Invitation subsystem in COmanage
            2. Self-sign-up
            3. Conscription

iii. Need elevator pitch at some point once we settle on the advisory. Would be ideal to have this by Global Summit

6. Any WG members interested in working with a subset of the Campus Success Program participants on Banner as System of Record (midPoint and possibly COmanage as Person Registry)
    a. Warren: Why is Banner special? Shouldn't we encourage the group to adopt our architecture rather than doing a point-to-point

TIER APIs and Registry Working Group Agenda and Notes

Friday 12 January 2018 at 10:00 am Eastern, 7:00 am Pacific, 3 pm London

Participants

Keith Hazelton - UW-Madison
Ethan Kromhout - UNC Chapel Hill
Chris Hubing - Internet2
Tom Jordan - UW-Madison
Bill Kaufman - Internet2
Steve Zoppi - Internet2
Paul Caskey - Internet2
Benn Oshrin - SCG
Jim Fox - UDub
James Babb - Uw Madison
Jon Miner - UW Madison
Gabor Eszes - Old Dominion
Ann West - Internet2
Christopher Hoskin - Oxford
Alexander Dutton - Oxford

Agenda

1. Oxford University's emerging IdM architecture (Christopher Hoskin, Alexander Dutton)
    a. Doing IdM Right--A User-Centric Approach
    b. New Enterprise IT Architect
    c. Christopher and Alexander are advocates for leveraging TIER deliverables. They are interested in better understanding the state of play with TIER and TIER adoption in US

2. (HOMEWORK for Wednesday, Jan. 17) Review documents - for Id Match. References provided by Benn Oshrin review these if possible.
        i. Below (ii - v) are a collection of docs prepared over a period of time related to Id Match. BennO and I discussed these on January 4th. There are terminology and naming cleanup issues that should be addressed in the documents to align with TIER. Review to develop a better understanding of the current Id Match version one for TIER … this should help prepare for a fuller conversation on Wednesday , January 17th.

ii. SOR-Registry Strawman ID Match API https://spaces.internet2.edu/display/cifer/SOR-Registry+Strawman+ID+Match+API
iii. ID Match PoC - This is from tech ex -
    1. The term 'canonical rule' define a match event
    2. The term 'potential rule' defines a possible match event https://spaces.internet2.edu/display/TIERENTREG/ID+Match+PoC
iv. ID Match Strawman - Flow https://wiki.jasig.org/download/attachments/50858970/id-match-flow.png?api=v2
v. ID Match Scoping - matrix of https://docs.google.com/spreadsheets/d/1hENmQWbykyiKCdwu-Pz4qCYLeTfSki2PYfCl8tJRmx0/edit#gid=0

3. Tom Jordan's Event matrix. Drill down and noodling session. Goal is to break this down.
    a. Latest version - https://www.lucidchart.com/invitations/accept/42044780-5c2a-4d3b-883c-e8fc544e9ba8
        i. PDF version if you cannot access Lucidchart is https://drive.google.com/file/d/158tp5wx9vfCIsAo6mjHk-Tv41e8vjkL5/view?usp=sharing
        ii.
    b. A full state machine conceptual model of a person registry entity (Jim Fox)
        i. Tom: Message types we proposed up to now seems too procedural. Vs model where controllers subscribe to higher-level event streams
        ii. What are the person states?
        iii. JimF: State is not a singleton. It's a set of attributes; One is has-account, another is has-email.
        iv. Defined progressions (student life-cycle); Then there's other side which is the state as a collection of things that have happened to a person. Controllers manage the state transitions in the latter case.
        v. Logic in the controllers: ent group controller notices changes and moves person to next lifecycle state
        vi. The diagram is a picture of a specific instance of a general architecture
        vii. Source system attribute update; how would we describe that event?
        viii. JimF: State is info about person that controller needs to decide if an action needs to be taken.
        ix. How do we help controllers sort what they care about from the stream of all events.
        x.

4. Report from the TIER Architecture for Internet2 operations F2F in Ann Arbor
    a. Internet2 applications + IAM infrastructure: Goal by March 31
        i. COmanage (Id Match?)
        ii. Grouper
        iii. Satosa (IdP Proxy that checks and can update LDAP and also check IDs and attributes and can redirect folks to enrollment flows etc.) All being moved into the Identity Python repo
            1. [AI] Keith/Bill set agenda item in near future to have Paul/BennO describe the Satosa functionality in depth
        iv. OpenLDAP
        v. RabbitMQ
        vi. Confluence
        vii. Jira
        viii. Sympa
    b. Followed later by integration of all the above with midPoint taking on the registry and provisioning functionality
    c.

Next Meeting

Wednesday 17 January 2018, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

- Brainstorming content for Global summit (May 6-9, San Diego): TIER Showcase(s) instead of TIER Demos
- Epics, Stories and Story Points as Agile Project Management tools for our 2018 work

TIER APIs and Registry Working Group Agenda and Notes

Friday 5 January 2018 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

- Video: https://bluejeans.com/678543210/browser

To join via Phone:

1) Dial one of these numbers or see all numbers - http://bluejeans.com/numbers
+1.408.740.7256

+1.888.240.2560(US Toll Free)
+1.408.317.9253 (Alternate number)

2) Enter Conference ID: **678543210#**

Back to API WG wiki: http://j.mp/tierApiWiki
Handy Links[2]

Current meeting notes beginning 22 Sept. 2017
Archive of older meeting notes

- April 19 2017 to Sept. 20 2017 http://j.mp/apiRegWG-5
- 18 January 2017 to April 19 2017 http://bit.ly/tierApiReg
- 16 June 2016 to 18 January 2017: http://j.mp/1PWMCp5
- 4 November 2015 to 16 June 2016: https://tinyurl.com

Participants

James Babb - UW Madison
Tom Jordan - UW Madison
Bill Thompson - Lafayette College
Ethan Kromhout - UNC
Jon Miner - UW Madison
Bill Kaufman - Internet2
Chris Hyzer - Penn
Warren Curry - UFlorida
Benn Oshrin - SCG (first hour only)
Carey Black -tOSU (late)
Brett Bieber - Nebraska

---

[2] TIER-API Agile Board (Backlog and Sprints)

TIER APIs and Registry Working Group Agenda and Notes

5. TIER-API Agile Board (Backlog and Sprints) Story points per task (BillK) - **push to the 12th**

   [AI] Bill to send out some type of primer and short task for estimating on the project Epics prior to next meeting. Maybe have a short discussion on that Wed.

6. Event-Driven Messaging: Provisioning to Slack from midPoint via SCIM,
   a. See the revisions to the sheet titled “Narrative Version” inside the following pdf (Tom, Warren)
   b. Latest version - https://www.lucidchart.com/invitations/accept/42044780-5c2a-4d3b-883c-e8fc544e9ba8
      i. Pdf version
      ii. Warren will send out some clarification (specifically on terminology) information on ID Matching after discussions with BennO. Will have BennO available for discussion on this on the Wed, Jan 19th meeting.
      iii. Comments from anyone who has not been in the loop on this diagram:
         1. Brett - color coding is not clear (Tom only made it visually distinct but will clarify)
         2. Brett interested in corner case ID Match situations that might be represented as errors in the diagram but real things that need to be handled
         3. What if Exact Match? No real need to be updated? But could have a match from the past (from Source repo) but needs to be updated in the Registry - These are separate databases (thin vs thick registry)
7. Grouper Security Model (Link to Doc)
   a. Grouper Privilege Matrix review and will be scheduled for
   b. Grouper - internal security model, on the Grouper call list. TIER recommended approach for this. Analogous to the Grouper deployment GUIDE from last year. Build the grouper TIER recommended practice.
   c. Hyzer - take time to review the model. Look for issues and capture in JIRA and then polish it and make sure all is working.
   d. Discussion on practice (noodling privileges.)
      i. Notion that there is a body of knowledge that the community can bring to the table.
      ii. Brett (Nebraska) - Apps and recommended structure for the service owners, distributed IT permission handling, getting standard permissions and template.
      iii. Template for new service, managers inherit privileges in stem
      iv. Managing transitioning privileges (Wisconsin)

v. Brett: ref and basis data having appropriate READer groups, who can read them all. Models for setting this up
vi. Granting privileges to a group of people (a college) vs individuals added to groups are performance considerations. Groups require more processing vs individual with privileges. This should be discussed in the practice document. Readers Group, etc… Cautions and how to avoid a pit. Folder inherited privileges would be good to READ but if you want UPDATErs to only have privileges on the includes/excludes, then a loader group query to assign the courseUpdaters that privileges would be best. If you need a more dynamic list of READers / UPDATErs, maybe make those a loader group...
vii. CARY - How to set up access for Reference groups: Hyzer - build what you need, Start with Admin, then READers, Managers (update/read) to manage memberships, Cary - Loader job - to build permissions - Access Control area - This clearly needs a practice and better defined / documented practice… Loader usage, vs UI usage, these structure recommendations and practice need to be documented with respect to deployment ease, maintenance ease , and performance implications.
viii. Hyzer - individuals privilege (lurking) around (object created in a folder due to member of a group, assign the group the admin privilege not the individual, this is a very very good idea to be documented.
ix. Group based privilege so when staff individuals change maintenance is minimized and being a member a group the admin. Ownership of something shifts how does that affect the group knowledge.
x. Inherited Privilege - will become effective in near real time. Implemented and is pending, Removal of privilege is also of concern. Hyzer - These could be accomplished with rules and vetos.
xi. Next version v2.4 around Jan/Feb, see Grouper Roadmap
xii. Attribute permissions could use better documentation about what is needed for a user to be able to use a UI feature. (Example: access to rulesAttrDef and rulesTypeDef appears to be needed for a user to be able to add inherited privileges to folders. Even if the user is an admin of the folder that they are setting the inherited privileges on.)

8. Next Wednesday: January 10, 2018
    a. Tom Jordan's Event matrix. Drill down and noodling session. See link in today's item 2. Goal is to break this down. Latest version - https://www.lucidchart.com/invitations/accept/42044780-5c2a-4d3b-883c-e8fc544e9ba8

[AI] Bill to send out some type of primer and short task for estimating on the project Epics prior to next meeting. Maybe have a short discussion on that Wed.

    b. Review documents - for Id Match

c. Here are some references… provided by Benn Oshrin review these if possible.
   i. Below (ii - v) are a collection of docs prepared over a period of time related to Id Match. BennO and I discussed these on January 4th. There are terminology and naming cleanup issues that should be addressed in the documents to align with TIER. Benn and I discussed possibly revising these into a TIER Id Match document. Review to develop a better understanding of the current Id Match version one for TIER … this should help prepare for a conversation on Wedensday , January 17th. Warren will high level review these a prep for the 17th on January 10th or 12th.
   ii. SOR-Registry Strawman ID Match API

https://urldefense.proofpoint.com/v2/url?u=https-3A__spaces.internet2.edu_display_cifer_SOR-2DRegistry-2BStrawman-2BID-2BMatch-2BAPI&d=DwIDaQ&c=pZJPUDQ3SB9JplYbifm4nt2lEVG5pWx2KikqINpWlZM&r=UBkKx63rTinSBj-2DQ-E7g&m=n6UzfSn2BiAzn2uO9t1XvsKc30yoPIZivA1wTb8xeEk&s=i0hKM2QEh_lJudcfa7G7acd3Ml7t1cqAnvxdU11c3bk&e=

   iii. ID Match PoC - This is from tech ex -
      1. The term canonical rule define a match event
      2. The term potential rule defines a maybe a match event

https://urldefense.proofpoint.com/v2/url?u=https-3A__spaces.internet2.edu_display_TIERENTREG_ID-2BMatch-2BPoC&d=DwIDaQ&c=pZJPUDQ3SB9JplYbifm4nt2lEVG5pWx2KikqINpWlZM&r=UBkKx63rTinSBj-2DQ-E7g&m=n6UzfSn2BiAzn2uO9t1XvsKc30yoPIZivA1wTb8xeEk&s=nWObpToMr6SYUaCnmTqYNLWy7wwPnkfqW5nst5Wjebk&e=

   iv. ID Match Strawman - Flow
https://urldefense.proofpoint.com/v2/url?u=https-3A__wiki.jasig.org_download_attachments_50858970_id-2Dmatch-2Dflow.png-3Fapi-3Dv2&d=DwIDaQ&c=pZJPUDQ3SB9JplYbifm4nt2lEVG5pWx2KikqINpWlZM&r=UBkKx63rTinSBj-2DQ-E7g&m=n6UzfSn2BiAzn2uO9t1XvsKc30yoPIZivA1wTb8xeEk&s=lEAdn69npMcOLZ3RahnOPwmTdXbADfFcLjhTCyJaCR0&e=

   v. ID Match Scoping - matrix of

https://urldefense.proofpoint.com/v2/url?u=https-3A__drive.google.com_open-3Fid-3D1hENmQWbykyiKCdwu-2DPz4qCYLeTfSki2PYfCl8tJRmx0&d=DwIDaQ&c=pZJPUDQ3SB9JplYbifm4nt2lEVG5pWx2KikqINpWlZM&r=UBkKx63rTinSBj-2DQ-E7g&m=n6UzfSn2BiAzn2uO9t1XvsKc30yoPIZivA1wTb8xeEk&s=N3ehZWrtXhWTY9NwPoQqD9pwvT6XahrsWI7ekbmRwrE&e=

9. Bill Kaufman, TIER-API Agile Board (Backlog and Sprints) Story points per task (BillK) - **push to the Friday 12th**

Wednesday 3 January 2018, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

- Video: https://bluejeans.com/678543210/browser

To join via Phone:

1) Dial one of these numbers or see all numbers - http://bluejeans.com/numbers
+1.408.740.7256

+1.888.240.2560(US Toll Free)
+1.408.317.9253 (Alternate number)

2) Enter Conference ID: **678543210#**

Back to API WG wiki: http://j.mp/tierApiWiki
Handy Links[3]

Current meeting notes beginning 22 Sept. 2017
Archive of older meeting notes

- April 19 2017 to Sept. 20 2017 http://j.mp/apiRegWG-5
- 18 January 2017 to April 19 2017 http://bit.ly/tierApiReg
- 16 June 2016 to 18 January 2017: http://j.mp/1PWMCp5
- 4 November 2015 to 16 June 2016: https://tinyurl.com

Participants

Keith Hazelton - UW-Madison
MIchael Brogan - University of Washington
Jim Fox - UDub
Michael Hodges - U Hawaii
Bill Kaufman - Internet2
Bill Thompson - Lafayette College
James Babb - UW Madison
Tom Jordan (UW-Madison) - first hour
Jon Miner - UW-Madison

Agenda

[3] TIER-API Agile Board (Backlog and Sprints)

TIER APIs and Registry Working Group Agenda and Notes

1. Grouper Deployment Guide V1.2 DRAFT
    a. Q5.1.4 Account Policy Groups
        i. https://docs.google.com/document/d/1tjurbk8aCAZwQ0dB_NzXqpwpZdY3xJ3Wed09_hOd4pI/edit?usp=sharing
        ii. JimF: This is really in the domain of the account server; Preferable to sending attributes and letting the service decide
        iii. Not one or the other, both have their place
        iv. UHawaii vision: enterprise reporting on authorization; get admins to manage that with Grouper so there's a single view of access management;
        v. How do we decide to proceed when a problem can be addressed by either Grouper or midPoint
        vi. Does this belong more naturally in a midPoint deployment guide or push to an appendix.
        vii. Lafayette won't really have a case study with midPoint by Global Summit
        viii. Bundles (employee-audience, "employee-like")
        ix. SaaS providers are persniketty about licensing terms about who is eligible for their service, so bundles don't work well in that environment
        x. Is the bundle notion a better fit for the more traditional on-campus services model
        xi. Hard to put access control policy in a UI for service admins; It really requires a conversation to determine the true intended service audience
        xii. Do a survey of service providers on what 'groups' they intend to serve?

    b. Grouper Security Model GDG V1.2 DRAFT
        i. https://docs.google.com/document/d/1Zgb708hFJjk49kw6SGCfP1ZrcHYEka5i5GRni0z7iyA/edit#heading=h.ym56foe4cx41
        ii. HOMEWORK for Friday: WG members with solutions in place, please review the proposed approaches here in the light of your practical experience.
        iii. What is the Grouper model for privileges/permissions on grouper-internal objects?

2. Messaging flows in the narrative version tab of the Multiple Source Systems to Registry diagram, v. 2.2 (pdf)

    a. Preliminaries: Does anyone want to take on the task of externalizing the business logic into an orchestration tool? That would be an alternate architecture to the one outlined below
    b. In this model, each component manages the messages they consume and the messages they publish. The process logic is in these message switches.

TIER APIs and Registry Working Group Agenda and Notes

i. Step 1: Person is entered into HR system

ii. An HR-specific connector normalizes data and sends a 'New Source Person' message to the Person Event Queue.
    1. Use the Pub-Sub pattern?
    2. Create a channel for each named event in the diagram?
        a. Normalized 'Source Person' message (keyed by source ID)
        b. 'Institutional Person - Complete' message (keyed by Institutional ID)
        c. 'Institutional Person - Credentialed' message (keyed by Institutional ID)
        d. Membership change for Group X.
    3. What is our normalized Source Added Person message data model? Resolvable link to the corresponding source record plus metadata?
    4. Smaller number of more generic messages vs larger number of more specific messages: Where's the balance?
    5. TomJ: Could use message types on a channel to convey specific sub-type; but don't send a firehose to a system that expects a shot glass.

iii. The Person Registry receives the 'Source Added Person' message and invokes the IdMatch service to see if this is a person already known to the Registry
    1.

iv. The IdMatch service returns match information (e.g. 'exact match', 'possible match', 'no match')
    1.

v. Based on the results of the IdMatch call, the Registry Update Controller will either add a new person, update an existing person, or invoke a manual review process.
    1. Should the Registry use messaging to connect with the Enterprise Person Repository for CRUD operations? Or a synchronous request/response model (e.g. Restful API)?

vi. Whenever a person is added / updated in the Person Registry, an 'Add / Update Institutional Person' message is generated and placed on the Person Queue.

vii. The Credential Management Controller receives the 'Institutional Person' message and prepares the credentialing system for the user to activate or register a credential.

viii. The user activates or registers a credential using the institution's activation process

ix. The Credential Management Controller generates a 'Credentialed Institutional Person' message to inform systems that the user has been assigned a credential.

x. The Groups Update Controller receives an 'Institutional Person - Credentialed' message and gathers information about the person via the Person API

xi. The Groups Update Controller uses data from the Person API to update data-driven group memberships within the grouping / authorization system.

10. Plans for Global Summit, TIER Architects/Developers meeting and Demos
    a. Plan for Thursday morning TIER Architects/Developers meeting
    b. Workshop (Sun or Thurs paid registration - likely NOT) vs working group sessions (slotted during GS Mon-Wed (possibly Sunday) kind of like a Session but not formal presentation); Where should we slot our demos?
    c. Panel is reviewing session proposals already closed; 'working meetings' could be used for TIER Showcases (formerly known as demos)

Next Meeting

Friday 5 January 2018 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

11. TIER-API Agile Board (Backlog and Sprints) Story points per task (BillK) - **push to the 12th**

    [AI] Bill to send out some type of primer and short task for estimating on the project Epics prior to next meeting. Maybe have a short discussion on that Wed.

12. Event-Driven Messaging: Provisioning to Slack from midPoint via SCIM,
    a. See the revisions to the sheet titled "Narrative Version" inside the following pdf (Tom, Warren)

TIER APIs and Registry Working Group Agenda and Notes

Wednesday 20 December 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

Participants

Bill Kaufman - Internet2 (running a few minutes late)
Ethan Kromhout - UNC
Warren Curry - UFlorida
Keith Hazelton - UW-Madison
Michael Brogan - U Washington
Benn Oshrin - SCG
Jon Miner - UW-
Tom Jordan - UW-Madison
Gabor Eszes - Old Dominion
Bill Thompson - Lafayette

Agenda

13. Event-Driven Messaging: Provisioning to Slack from midPoint via SCIM,
    a. See the sheet titled “Narrative Version” inside the following document: lucidchart, pdf (Tom, Warren)

    b. Follow the related email thread on our list: “Re: [tier-api] Re: some additional details related the narrative or documentation adding to the SOR diagram”
    c. What does it mean to actually get a person into the Registry from an SoR? To credential an enterprise person? For Grouper to add memberships for a new institutional person.
    d. WarrenC: If I’m offering services to an external user: User activation covers both local credential issuance and
    e. Each controller is responsible for its own state and its own publications and subscriptions
    f. Should we send a federated identity through search/match? Person Registry is a profile repository; UW-Madison: We never try to link based on unverified self-asserted information.
    g. Credential controller is where all the credential management functions (account linking, etc.) happen.
    h. 1 and 2 could be genericized and then a single diagram could cover multiple SoRs
    i. JimF: Should be a message back from Grouper saying change in an institutional group membership; BillT: Or maybe this should be conceived as a subject

attribute change leveraging the Group management.; Practical implications for the storyline whether you are managing groups or managing subject attributes.

j. BillT: identifier/username/security principal; username as subject id; As soon as there is a security principal, then they can be fed into subj. Attr. mgmt via Grouper; JonT: What we want to demo in this diagram is that there is a series of messages that flow back and forth between component;
k. TomJ: Companion document: The current diagram is a state diagram; Companion would expound on the diagram to describe what possible states a person can exist in, include coverage of message semantics in sense of what it signifies from a business sense.
l. TomJ: What should we call this thing? Identity lifecycle?

14. TIER Event-Driven Messaging study group

    a. Look over this Gartner doc in advance

    b. Add messaging solution annotations to the Steps from the diagram narrative

       Preliminaries: Does anyone want to take on the task of externalizing the business logic into an orchestration tool? Otherwise we will take a path of having each component manage the messages they consume and the messages they publish.

       i. Step 1: Person is entered into HR system

       ii. An HR-specific connector normalizes data and sends a 'Source Added Person' message to the Person Queue.
           1. Use the Pub-Sub pattern?
           2. Create a channel for each named event in the diagram?
           3. What is our normalized Source Added Person message data model? Resolvable link to the corresponding source record plus metadata?
           4. Smaller number of more generic messages vs Larger number of more specific messages: Where's the balance?
           5. TomJ: Message types to convey specific sub-type; but don't send a firehose to a system that expects a shot glass.

       iii. The Person Registry receives the 'Source Added Person' message and invokes the IdMatch service to see if this is a person already known to the Registry
           1.

iv. The IdMatch service returns match information (e.g. 'exact match', 'possible match', 'no match')
    1.

v. Based on the results of the IdMatch call, the Registry Update Controller will either add a new person, update an existing person, or invoke a manual review process.
    1. Should the Registry use messaging to connect with the Enterprise Person Repository for CRUD operations?

vi. Whenever a person is added / updated in the Person Registry, an 'Add / Update Institutional Person' message is generated and placed on the Person Queue.

vii. The Credential Management Controller receives the 'Institutional Person' message and prepares the credentialing system for the user to activate or register a credential.

viii. The user activates or registers a credential using the institution's activation process

ix. The Credential Management Controller generates a 'Credentialed Institutional Person' message to inform systems that the user has been assigned a credential.

x. The Groups Update Controller receives an 'Institutional Person - Credentialed' message and gathers information about the person via the Person API

xi. The Groups Update Controller uses data from the Person API to update data-driven group memberships within the grouping / authorization system.

15. Grouper Deployment Guide V1.2 DRAFT
    a. For next time: Q5.1.4 Account Policy Groups
        i. https://docs.google.com/document/d/1tjurbk8aCAZwQ0dB_NzXqpwpZdY3xJ3Wed09_hOd4pI/edit?usp=sharing

    b. Grouper Security Model GDG V1.2 DRAFT
        i. https://docs.google.com/document/d/1Zgb708hFJjk49kw6SGCfP1ZrcHYEka5i5GRni0z7iyA/edit#heading=h.ym56foe4cx41
        ii. Grouper privs, etc.

iii. Pre-population of security groups
iv.

Next Meeting

Wednesday 3 January 2018, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

16. TIER-API Agile Board (Backlog and Sprints) Story points per task (BillK)
    a. [AI] Bill to send out some type of primer and short task for estimating on the project Epics prior to next meeting. Maybe have a short discussion on that Wed.

TIER APIs and Registry Working Group Agenda and Notes

Friday 15 December 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

Participants

Jim Fox - UDub
Jon Miner - UW-Madison (in transit)
Ethan Kromhout - UNC Chapel Hill
Tom Jordan - UW Walworth
Warren Curry - U Florida
James Babb - UW Madison
Keith Hazelton - UW Madison
Bill Kaufman - Internet2

Agenda

- Keith to start the BlueJeans session, will rejoin the call for the last 30 minutes

- Narrative to supplement the Reference Architecture diagram of Registration flow (Warren, Tom)
    - https://www.lucidchart.com/invitations/accept/6aa1fd8d-9d58-45d6-976a-d3f43c61b4f9

    - See TIER-API email thread “RE: some additional details related the narrative or documentation adding to the SOR diagram”

- TIER-API Agile Board (Backlog and Sprints) Story points per task (BillK)
    - [AI] Bill to send out some type of primer and short task for estimating on the project Epics prior to next meeting. Maybe have a short discussion on that Wed.

- Event-Driven Messaging Architecture: TIER study group launch
    - HOMEWORK for Wednesday, Dec. 20: Look over this Gartner doc in advance (good for language/terminology but Tom’s diagram is more the correct architecture)
    - Common IAM use cases
    - Tell everyone that something happened, then they can respond as they will

Next Meeting (last meeting of 2017)

Wednesday 20 December 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

- Event-Driven Messaging Architecture: TIER study group launch

TIER APIs and Registry Working Group Agenda and Notes

- HOMEWORK: Look over this Gartner doc in advance

TIER APIs and Registry Working Group Agenda and Notes

Wednesday 13 December 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

Participants

Jim Fox - UDub
Ethan Kromhout - UNC Chapel Hill
Bill Kaufman - Internet2
Keith Hazelton - UW-Madison
Michael Hodges - U of Hawaii
Julio Polo - U of Hawaii
IJ Kim - Internet2
Michael LaHaye - Internet2 TSG
Chris Hubing - Internet2
Benn Oshrin - SCG
Tom Jordan - UW-Madison
Warren Curry - U Florida
Bill Thompson - Lafayette College
Jon Miner - UW-Madison
James Babb - Uw Madison
Gabor Eszes - Old Dominion

Agenda

1. Michael Hodges, Julio Polo: U Hawaii's Event Messaging Architecture Featuring Banner

    - UHawaii evolution to messaging with RabbitMQ
        - 10 campus system w system-wide organization too
        - Several systems of record, Banner students, PS hr, research organization, student employee system; Identity reps can add guests and other affiliates
        - Philosophy in IAM: Each SoR should publish its own messages for whatever list of consumers are interested; Banner has native support for messaging; connectors for other systems like PS, student employment; UH IMS Identity Management System -- Registry
        - Consolidated messages from all SoRs out of the Registry; Data governance is consolidated. Blanket approval is typical; JSON messages are standardized across SoRs

- UHawaii message schema, Banner message schema, encouraged student systems to follow U Hawaii schema
- At present Banner doesn't publish sensitive data; for HR data, only UH IMS is allowed to receive it
- Banner publishes pointers (call-backs) only, up to subscriber to query for details; Julio not a fan of this model; role changes: student -- employee -- faculty followed by query might lead to non-determinative results.
- GaborE: Being able to capture the state of something at rest, you can query that at point the info is required; There is a happy medium, probably.
- Data repair necessary since messages are not 100% reliable in terms of order and delivery;
- Jim Fox: design must take into account that sensitive data is likely to show up in many messages
- Three primary types of message contents:
- 1) Person/identity data: instit id, name dob, SSN,
- 2) Role, home campus,
- 3) Account (NetID)
- But others as well, e.g. contact info
- All go onto RabbitMQ
- Each type of data has its own CRUD methods (add,delete,modify)
- 2 messages are esp. Important: 1) modify this person's institutional identifier; allows other SoRs to keep up with changing identifiers; 2) Modify NetID/Email address; vanity emails also supported, directory can include departmental emails; 1 and 2 are distinguished by message routing key
- RabbitMQ publishes to an exchange with attached queues listening
- If no queues attached you can still publish but no one is listening
- On publication, can tag with a message routing key: e.g. person.add; can subscribe to particular keys and/or include wildcards: #.delete means only messages that delete things
- Challenge: How to bootstrap applications? Csv file was 1st solution and turning on a spigot of messages; Now we keep a separate exchange for bootstrapping: New system comes online, they receive all the messages on that particular exchange: E.g. new system queries for all active students, they are sent to the bootstrap exchange and new system processes the series of messages; After that, new system switches to the incremental exchange;
- End of semester creates lots of messages around termination of students; it's always a challenge, but RabbitMQ itself has never been the failure point; Have seen 500K messages on an exchange;
- Challenge: What to do when a person has a newly added affiliation; system that cares only about carriers of that affiliation; we send a retrofit

so the app will see the person before they get the 'add affiliation' message.
    - Warren: use of messages rather than API callbacks avoids some security issues around great numbers of service accounts to be managed; plus the systems have to know where to go to get the needed information
    - Consumers have to register, so the registration process is a point at which one can manage the access control.
    - RabbitMQ vhost: as a way to partition exchanges;
    - AMQP 0.9.1 to AMQP 1.0: need for bridging;
    - BillT: We've been using RabbitMQ as a Grouper provisioning engine; authZ groups, etc. Exchange, routing keys, drive provisioning engine which fans out provisioning messages to provisioning targets; Looking at mP, maybe mP does the provisioning engine
    - Julio: we don't use Banner messages exclusively
    - BillT: Getting data out of Banner via messages

    - Here are the public links for what we publish for our developer community
    - https://www.hawaii.edu/bwiki/display/UHIAM/UHIMS+Events+-+Message+Specs
    - https://www.hawaii.edu/bwiki/display/UHIAM/Banner+Messages

- Marking up and consolidating deployment guide feedback (BillT)
    - GDG 1.2 Work Plan
    - TIER Grouper Deployment Guide WIP V1.2 DRAFT
    - https://lists.internet2.edu/sympa/arc/grouper-users/2017-12/msg00034.html
    - Standardizing affiliation terminology? Diminishing returns as we go finer grained. Let access policy suggest what your reference groups should be; Lafayette: lifecycle groups: on-track-to-graduate..in addition to affiliation-type groups;
    - Group: students for current semester: is easier or harder depending on how you structure the reference groups and basis groups;
    - Warren: This is a good start, let's have this be a recurring agenda item;
    - BillT: Mary@Duke: We might not be able to make it simple, but we need to make it clear;
    - Venn diagram of overlapping functionality: What's on the page after the venn diagram; three columns (COmanage, Grouper, midPoint) per domain: bullets in the rows for capabilities .

- Review of Tuesday's Banner integration with IAM infrastructure call

    - Wiki page created for ongoing exchange

- Exploring the Okta model for IAM
    - NickR: Is it more than adding AuthN over AD?
    - SteveZ: Don't underestimate the power of a large engineering team plus $$
    - Unicon has done a serious evaluation of the Okta offerings, and they'd be willing to share
    - If it makes sense, we could invite Okta in to discuss further

- Your item here

Next Meeting

Friday, 15 December 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

- Keith start the call
- Hour one Narrative to supplement the Reference Architecture diagram: TomJ
  Registration flow (Warren, Tom)
- Keith has a conflicting TIER meeting until 11 am Eastern: Story points per task

TIER APIs and Registry Working Group Agenda and Notes

Friday, 8 December 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

Participants

Ethan Kromhout - UNC Chapel Hill
Tom Jordan - UW-Madison
Jon Miner - UW-Madison
Bill Kaufman - Internet2
Keith Hazelton - UW-Madison
Warren Curry - UFlorida
Chris Hubing - Internet2
James Babb - UW Madison
Carey Black - tOSU (Very late)

Agenda

1. Identifying tasks on our near-term deliverables (See Primary API and Registry WG Projects Through EoY 2017)
    a. Top 3 priorities (See (JIRA epics, stories and tasks)
        i. Identity Matching API and implementation: See agile board
        ii. Provisioning tools, connectors and best practices
            1. LucidChart scim provisioning and Shib integration
            2. BTAA: Ask for specifics; they are working on best practices as a general problem space: Offer a framework for sections of the Architecture Notebook (TomJ)
            3. SCIM 2 connector for mP
            4. Integrating messaging infrastructure with midPoint, COmanage, Grouper,...EthanK: continue work on pulling in messages formatted for minimal person schema; Messaging coming out of mP? Workflow approval of a role that might want to be broadcast; conflict w mP model: It knows what should happen to other systems based on approvals. Conflicts with the loose coupling/systems only know about themselves. If you manage access controls properly, provisioning is less critical.
            5. Normalization process from source system into identity store
            6. Publishing out onto the queue...maintain order of message
            7. Subscriber receives, invokes IdMatch, pushes results to Registry

iii. Recommended approaches to integrating Systems of Record with an Entity Registry (see above)

b. Next 3 priorities

i. Event-driven messaging and an asynchronous integration architecture
   1. Architecture model needs to be described
   2. Study group on EDM; U Hawaii presentation
   3. JonM: One important event is 'user now has an institutional identity and identifier; One next step would be to provision user with NetID; Create Group subject, and your parochial stuff here

ii. Schema definition and extension mechanisms and practices - ties in with #10

iii. API Development Guidelines including API AuthNZ
   1. Identify audiences (see notes)

2. Internet2 Identity Program we are developing at Internet2 with COmanage, Grouper, midPoint plus some of the Data Syncs/Sources (BillK)
   a. Data Element Relationships
   b. Demo of I2 COmanage and provisioned collaboration tools
   c. Called I2 Identity Program; run by T&I Team + I2 Tech Svcs Group (TSG)
   d. Need to incorporate Grouper and midPoint into the I2IdProgram
      i. Review Grouper Deployment Guide to structure access management
      ii. Plan to leverage midPoint in similar ways to TIER-EntReg
      iii. Link TSG and TIER API/Reg WG: cross attendance
      iv. Add google docs, salesforce, lucidchart, slack,....working on a bi-directional sync between COmanage and Salesforce (BennO as SME plus ChrisHu); Where the data entry takes place is where the data glitches / biz processes need to get fixed.
      v. 1st use case is to roll out to TIER WG to manage resources: github, jira,...Some new versions have nice features: represent Jira content on a wiki page
      vi. Carey: Might want to cook the dog food before you try to eat it. I2IP is an implementation; TIER does not yet have a full set of deployable packages
      vii. ChrisHu: Account linking and provisioning from COmanage; Trying hard to hew to the TIER architecture and recommendations
      viii. We need to show launch of the full TIER packages by TechEx 2018
      ix. Satosa Docker image as deliverable from I2IP;
      x. I2IP plus Campus Success Program are our early adopter group

3. Launching a study group on event-driven services (KeithH)
    a. Java and Spring Cloud Stream (to facilitate the creation of event-driven/ message-driven microservices)
        i. Intro tutorial: http://www.baeldung.com/spring-cloud-stream

    b. AMQP 1.0 and maybe a message bridge between 0.9.1 and 1.0
        i. Amazon now supports AMQP 1.0
        ii. [JimF] I can't make the call, but I am looking into AWS approaches to this.

4. NOTE: Former contents of Handy Links footnote for reference:

    Overview Timeline and Deliverables for TechEx 2017; Roadmap Through 2018 (Google Doc); TechEx Demos: Expanded / Updated Provisioning, Event-Driven Messaging: Grouper, Event-Driven Messaging: SoR to Registry, Client / Service Registry, API Access to Person Data

Future Meetings

- **Special add-on meeting: Tues. 12 Dec, 1:30 pm Eastern**
    - Video: https://bluejeans.com/678543210/browser
    - Banner Data Integration Patterns
        - How sites with Banner as SoR integrate with their IAM and LMS infrastructure

- **Wednesday 13 December 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC**

    Michael Hodges, Julio Polo: U Hawaii's Event Messaging Architecture

    - Here are the public links for what we publish for our developer community
    - https://www.hawaii.edu/bwiki/display/UHIAM/UHIMS+Events+-+Message+Specs
    - https://www.hawaii.edu/bwiki/display/UHIAM/Banner+Messages

TIER APIs and Registry Working Group Agenda and Notes

Wednesday 6 December 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

Participants

Ethan Kromhout - UNC Chapel Hill
Jim Fox - UDub
Michael Hodges - U of Hawaii
James Babb - UW Madison
Jon Miner - UW Madison (~~running late~~ here!)
Keith Hazelton - UW-Madison
Benn Oshrin - SCG
Bill Kaufman - Internet2
Warren Curry - UFlorida
Gabor Eszes - Old Dominion
Tom Jordan - UW Madison

Agenda

1. Jim Fox: OpenAPI 3 documentation for UDub's group service https://urizen.s.uw.edu/gwsapi
    a. Aimed at API customers as the API documentation
    b. Swagger-ui is an installable dist.; If you want to use the 'try it out' functions you need to configure to allow Cross-site requests. Access control: allow-origin foo.bar
    c. Possibly push this to Git for folks to access but would not be able to 'try it out' there

2. IdMatch: What steps follow human decision on identity quandaries? (BennO)
    a. See p. 3 of diagram: https://www.lucidchart.com/documents/edit/a7596396-5885-4048-b43f-9c9d66166e84/0?shared=true
    b. How exactly the match service handles things once they're in the human resolution phase? E.g., how do we feed in the resolved identity data?
    c. An HR person who has permission to look at person data across all the Systems of Record; There's a multi-system aspect; Do we ever want to send back to SoR admins for resolution and replay
    d. Match will have to have a 'resume processing at step x'

e. JimF: Ideally all the business logic is externalized into a 'rules engine' + workflow engine-like component such as one of the following: https://www.trustradius.com/products/drools/competitors
f. Next steps
    i. Warren: It's reasonably close. I'll create a narrative for each step of the diagram
    ii. Tom: Narrative with callouts on assumptions and questions
    iii. BennO: Add capability to the Match Engine to publish a message: benefit: for currently scoped pilot over next couple months, let's not tackle this. Phase I; will support synchronous request-response mode; Response may be here's a claim tag, come back later and ask; JimF: IdMatch doesn't have enough context to assert useful messages; BennO: Merge/Split events? ID Change events?
    iv. Keith: comment on practicality of externalizing business processes (taking them out of code) to something like a rules/workflow engine.
    v. Is there a tension between loose coupling and having externalized business logic? When you're inside one component, loose coupling means you don't have the bigger picture.
    vi.

3. Further thoughts on choreography/orchestration (TomJ)
    a.

4. NOTE: Special add-on meeting: Tues. 12 Dec, 1:30 pm Eastern
    a. Banner Data Integration Patterns
        i. How sites with Banner as SoR integrate with their IAM and LMS infrastructure
    b. BlueJeans Video Conference - https://bluejeans.com/678543210?src=calendarLink

Next Meeting

Friday, 8 December 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

Future Meetings

- Special add-on meeting: Tues. 12 Dec, 1:30 pm Eastern
    - Banner Data Integration Patterns
        - How sites with Banner as SoR integrate with their IAM and LMS infrastructure

    - BlueJeans Video Conference - https://bluejeans.com/678543210?src=calendarLink

- Dec. 13: Michael Hodges, Julio Polo: U Hawaii's Event Messaging Architecture
    - Here are the public links for what we publish for our developer community
    - https://www.hawaii.edu/bwiki/display/UHIAM/UHIMS+Events+-+Message+Specs
    - https://www.hawaii.edu/bwiki/display/UHIAM/Banner+Messages

TIER APIs and Registry Working Group Agenda and Notes

Friday, 1 December 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

Participants

Keith Hazelton - UW-Madison
Jon Miner - UW-Madison (in transit, running late)
Warren Curry - U Florida
James Babb - UW Madison
Bill Thompson - Lafayette College
Jon Finke - RPI
Dean Lane - Rice

Agenda

1. SoR to Registry case study: Banner to midPoint, first thoughts (KeithH, BillT)
    a. Mention messaging SIG on Tuesday
    b. BillT: Campus Success Program, Lafayette College is participating, they have taken an assignment to evaluate midPoint integrated into an IAM infrastructure
        i. How do you get credentials, get a Lafayette identity
        ii. SoR Banner, COmanage, munge identity, push out to LDAP leveraging midPoint
        iii. Other participants in Campus Success are interested in same set of components; Learning what those schools are doing currently
        iv. Banner has a module to do NetID management, but not a lot of us have experience with it yet
        v. WarrenC: Banner & COmanage as SoRs?
        vi. BillT: Banner sources identities for fac/staff/student, COmanage is for everyone else: Sponsored Accounts, folks who need a Lafayette credential set; identity lifecycle; L number (public, unique id) currently sourced managed in Banner; Account workflow picks up there to assign credentials; This part of the architecture is likely to be kept in subsequent models; Sponsors look in Banner for an L number, if not found, request one. Way they get into Banner: Banner has existing processes for fac/staff/student onboarding; minimal person record that has L number and not much more; It's possible to get L numbers without coming in through standard business processes; This is a manual process at present; Request for sponsored account goes to Banner admins who do search/match/insert process, Banner admins send the L number back to the midPoint folks;
        vii. WarrenC: So Banner is your identity 1st component;

viii. JonF: we have Banner, but challenges because students and HR systems don't actually enter people immediately, so we have to do a work-around; The minimal record is really only an identifier plus an L number
ix. U FI has similar issues w HR and SIS putting new folks in 'Just-not-in-time' to get them access to services; We are uncovering early stage necessary steps;
x. BillT: had lots of person entries without L numbers, but with COmanage, we put a stake in the ground: Every person in IAM system MUST have an L number;
xi. WC: What about non-person entries? BillT: I don't know =) But they need sponsors and identifiers, too, right?
xii. JonF: We have a type attribute on our entity tables…
xiii. BillT: Maybe we should partition L numbers or namespace them so we could have a uniform L identifier across all types of entities under management
xiv. JonM: HR just-not-in-time practices is because they are not in biz of identity management; Need a de-bouncer on identity creation since we have cases of deletion/re-creation or creation/immediate deletion;
xv. "Orphaned" identities (where system that created the identity no longer cared) UW-Madison converted them to 'ad hoc, self-managed'
xvi. BillT: Early on-boarding for a long time in Banner; new HR director: "We can't treat them as employees until we have their W-9 on file"; So guess what, people showed up and didn't have phones, computers,....
xvii. WarrenC: The lesson is: Identity is separate from affiliation, from service recipient; We need to articulate the principles we've been uncovering, that would be a big help to campuses building or re-modeling their IAM infrastructure.
xviii. IAM systems have responsibility to construct the person identities, often in cases when there is minimal or partial information

2. Who's interested in joining a small group to work through some tutorials on event-driven services? (KeithH, EthanK)
    a. Java and Spring Cloud Stream
        i. http://www.baeldung.com/spring-cloud-stream

    b. AMQP 1.0 and maybe a message bridge between 0.9.1 and 1.0
        i. Amazon now supports AMQP 1.0

    c. Goal is to gain practical experience with event-driven messaging as an integration pattern

    d. Keith is motivated to do this in part because of a UW-Madison presentation he's doing on January 5

    e. Interested: JamesB, JonM, EthanK, KeithH

    f. Email invitation will be sent to the list so people who want to can get included in the scheduling duels

3. Dockerized midPoint UW-Madison style (JamesB)
    a. Current state: On the I2 Repo, MatthewB, U Colo. School of Mines used it with success
        i. https://github.internet2.edu/TIER/wisc-midpoint

    b. Prep for Monday, Dec. 11 meeting of Packaging WG, JimJ, ChrisHu, Paul Caskey, on a formal TIER midPoint package
        i. Support model where everything you need for an end-to-end demo is packaged up together
        ii. Plus component-by-component packages that can be mixed and matched with existing campus services as needed

Next Meeting

Wednesday 6 December 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

- Jim Fox: OpenAPI 3 documentation for UDub's group service https://urizen.s.uw.edu/gwsapi
- IdMatch: What steps follow human decision on identity quandries? (BennO)
- Further thoughts on choreography/orchestration (TomJ)

Future Meeting

- Dec. 13: Michael Hodges, Julio Polo: U Hawaii's Event Messaging Architecture
    - Here are the public links for what we publish for our developer community
    - https://www.hawaii.edu/bwiki/display/UHIAM/UHIMS+Events+-+Message+Specs
    - https://www.hawaii.edu/bwiki/display/UHIAM/Banner+Messages

TIER APIs and Registry Working Group Agenda and Notes

Wednesday 29 November 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

Participants

Jim Fox - UDub
Michael Brogan - UW
Ethan Kromhout - UNC Chapel Hill
Keith Hazelton - UW-Madison
James Babb - UW Madison
Michael Hodges - U of Hawaii
Jon Miner - UW-Madison
Warren Curry - U Florida
Tom Jordan - UW-Madison

Agenda

1. Review, Extend and Assign API/Registry Epics and issues in Jira
    a. Drawn from Primary API and Registry WG Projects Through EoY 2017

    b. ID volunteers for work items from the growing list. Santa needs more elves this time of year
        i. EthanK: Event-driven messaging: routing from Grouper, etc.
        ii. Keith OAI 3 representations of TIER APIs
        iii. JimF: Group service into OpenAPI Tools available for conversion; Need for an orchestration solution
        iv. Warren: work on the TIER-API channel on the orchestration-choreography capability
        v. Banner-Registry TIER-midpoint slack channel discussions (get Radovan onto a call)
        vi. TomJ: Address the create person / create group memberships for person dance
        vii. Michael Hodges: Messaging around Banner events; Help from Julio on evaluating messaging architecture proposals; Dec 13th presentation

c. Update on TIERAPI-19: Make BennO's 500K person identity data file available for Registry tests

d. TIERAPI-24 Set up WG Github repos and Markdown-based web pages

e. TIERAPI-23 Brainstorm content bullets for Architect's Notebook / Provisioning Deployment Guide

Next Meeting

Friday, 1 December 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

- BennO on IdMatch: What steps follow decision on identity resolution
- TomJ on choreography/orchestration 2nd half

TIER APIs and Registry Working Group Agenda and Notes

Friday, 17 November 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

Participants

Keith Hazelton - UW-Madison
Ethan Kromhout - UNC Chapel Hill
Bill Kaufman - Internet2
James Babb - UW-Madison
Tom Jordan - UW-Madison
Jon Miner - UW-Madison
Bill Thompson - Lafayette College
Warren Curry - UFlorida
Gabor Eszes - Old Dominion
Carey Black - tOSU (a bit late)

Agenda

2. Whiteboard the architectural concepts not yet manifested in the Tech Ex demos;
    a. Provisioning to Slack from midPoint via SCIM, Step one: SoR to Person Registry
    b. Clear up the fuzzy bits of the map
    c. Id Match page, ask BennO to update
    d. Embed LucidChart in a Google Doc
    e. New Hire vs New HR person event sub-types
    f. Has to clear the Matching process before either Registry or Grouper see it
    g. Sending system has it's own representation of the person that the message is about
    h. If Grouper calls back to HR, and HR says 'no institutional identifier yet' then what?
    i. Let's assert that provisioning and grouping processes are downstream of / subsequent to the person (entity) being created in the registry
    j. TJ: The source instance of a person is different (and has different associated message types) than a person disambiguated by the registry
    k. TJ: We will implement thin registry, but almost all of us will immediately fatten it up for our local needs; KH:
    l. We don't want data consumers to have to know which data elements should be pulled from which backend, that should be abstracted away for consumers (Maybe use a "Query message" to/from the message bus and/or REST API?)

m. CB: If you don't make assumptions about which TIER components are in use, then you can't count on that component's functionality being available
n. TJ: People can bring their own components but taken collectively those components do have to provide all the functionality specified in the TIER architecture
o. GE: we don't see messages in the wild that essentially amount to requests for a retrieval of information
p. Is eventual consistency good enough as a substitute for ACID transactions?
q. UW-Msn: problem: system that gets event and goes to query another system that doesn't yet have the data
r. JM, GE: We need to define the behavior of what grouping systems need to do, then problems are resolved as long as we can stipulate what a compliant grouping system will do.

3. Work through example processes requiring orchestration; Identify orchestration strategies
    a. See 1a) as an initial example

4. Review and revise Primary API and Registry WG Projects Through EoY 2017 (Thanks for the work, BillK!)
    a. ID volunteers for work items from the growing list. Santa needs more elves this time of year

- In JIRA, see the EPICs column (toward the left) of the Backlog Page

[Keith] set up call with Ethan on demo packaging, Talk to James Babb for assistance

Next Meeting

No meetings Thanksgiving week; Use slack to get things done

Wednesday 29 November 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

TIER APIs and Registry Working Group Agenda and Notes

TIER APIs and Registry Working Group Agenda and Notes

Wednesday 15 November 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

Participants

Jim Fox - UDub
Jon Miner - UW-Madison
Michael Hodges - U of Hawaii
James Babb - UW-Madison
Keith Hazelton - UW-Madison
Warren Curry - U Florida
Benn Oshrin - SCG
Tom Jordan - UW-Madison
Bill Kaufman - Internet2 (grabbing coffee)
Ethan Kromhout - UNC Chapel Hill
Bill Thompson - Lafayette College

Agenda

1. Person schema review (WarrenC)
    a. Let's compare and contrast the OAI versions of U Florida's API and the OAI version of SCIM;
    b. To use a human-friendly tool, Browse to http://editor.swagger.io click the file menu and choose 'import url', paste in
        i. Either U Fl Person schema: https://drive.google.com/file/d/1t5SW8bCe79AzkUKHL4IynufSxS6bcZ9n/view?usp=sharing
        ii. Or Citrix version of SCIM https://raw.githubusercontent.com/APIs-guru/openapi-directory/master/APIs/citrixonline.com/scim/NA/swagger.yaml
    c. and return
    d. HOMEWORK: Whiteboard the architectural concepts not yet manifested in the demos;

2. Review and revise Primary API and Registry WG Projects Through EoY 2017 (Thanks for the work, BillK!)

a. Please consider volunteering for some work item from the growing list. Santa needs more elves this time of year 
b. In JIRA, see the EPICS column (toward the left) of the Backlog PageNext Meeting

Friday, 17 November 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

TIER APIs and Registry Working Group Agenda and Notes

Friday, 10 November 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

Participants

Keith Hazelton - UW-Madison
Rob Crowell - UMD College Park
James Babb - UW Sun Prairie
Jon Miner - UW Madison
Benn Oshrin - SCG
Bill Kaufman - Internet2

Agenda

1. Rob Crowell, UMDCP, fresh from TechEx, working on a new registry
    a. Looking for a better collision detection approach
    b. Registry project: Recognized they needed to step back & refactor; requirements & development

2. Recasting our 2018 roadmap as a set of epics in Jira.
    a. Add notes on approaches to the top six API/Registry epics here
    b. In JIRA, see the EPICS column (toward the left) of the Backlog Page
    c. If you can't access the above, contact wkaufman@internet2.edu

Next Meeting

Wednesday 15 November 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

- Person schema review (WarrenC)

TIER APIs and Registry Working Group Agenda and Notes

Wednesday 8 November 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

Participants

Keith Hazelton - UW-Madison
Ethan Kromhout - UNC Chapel Hill
Jim Fox - UDub
Jon Miner - UW-Madison
Bill Kaufman - Internet2
Warren Curry - U Florida
Chris Hubing - Internet2
Bill Thompson - Lafayette College
Benn Oshrin - SCG (first 30 min only)
Tom Jordan - UW-Madison (first hour)
Michael Hodges - U of Hawaii
James Babb - UW Madison
Carey Black - tOSU

Agenda

3. midPoint provisioning demo: make the config files public
    a. Link to GitHub https://github.internet2.edu/TIER
    b. Make a recorded version of the demo

4. 'TIER-curated' and 'TIER-community' as Github organizations (ChrisHu, TomJ)
    a. How do we organize our aggregation of artifacts? ChrisHubing, TomJordan discussed;
    b. It's an enterprise github, so need to register: email Chris Hubing
    c. CareyB: we use gitlab; you can self-provision on 1st Shib login; good model for I2;
    d. Commit access to Grouper needs explicit approval; We don't want to provision ePPN for Github, but a COmanage issued identifier;
    e. Will licensing for enterprise become a price-point issue?
    f. Create an organization specifically for the campus community; It needs a curator as does the TIER curated one
    g. Next steps
        i. [Keith] Pass on to Ann West: Curation process: Have Campus Success program participants curate the Community Side

TIER APIs and Registry Working Group Agenda and Notes

5. Grouper Visualization session at ACAMP (TomJ)
    a. Ended up more about UI and new concepts in the UX space; Lot of time on how to visualize relationships: subject thru group thru authZ group to resource
    b. Visual tagging of different kinds of groups
    c. Why can't joey get to service X? A hard question; Jon, James working on an approach
    d. Templates for standard sets of groups, AuthZ group plus include/exclude for standard lifecycle of memberships

6. TIER Topics - Scribing Google Doc (JamesB)
    a. Focused around strategy for TIER; provisioning: COmanage / midPoint: (take to Comp Architects. Is product overlap OK? Overall roadmap of products; Is TIER sustainable?

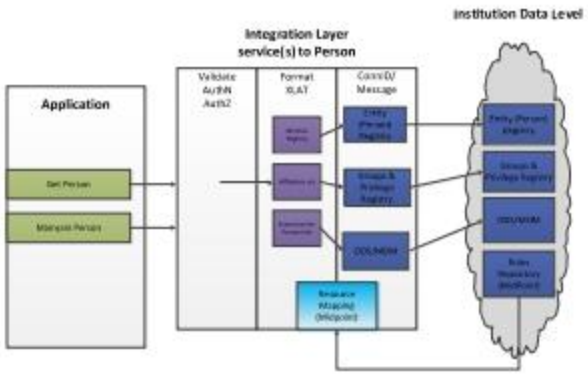
7. Authoritative sources for attribute aggregation/External Identities - Scribing Google Doc (KeithH)
    a. Do we need to convey original asserting party along with an attribute value when it is part of an aggregate from multiple IdPs or Attribute Authorities?
    b. If so, how?
        i.
        ii. Flag via attribute metadata: Have a separate named prefixed XML attribute
        <saml attribute>original issuer=hsww.edu</saml attribute>
        iii. SAML has a standard way to decorate attributes, but it is not used
        iv. SAML lacks capability for transitive trust. Meant to be lightweight. Trust that someone won't decorate. All asserted by a single IdP
    c. For some cross-protocol attributes multiple syntaxes need to be supported
        i. LDAP
        ii. SAML
        iii. JSON Web Token (JWT), pronounced "jot"
    d. In practice very few SPs care about the provenance of the value., They trust the IdPs assertions; People don't care much now, but will start to going forward.
    e. At times IdP may need to take account of where the user wants to go

8. Grouper Provisioning Topics - Scribing Google Doc (WarrenC)
    a. Another example where there are many ways to solve problems with TIER components; We haven't done much yet to define the TIER way to solve things;
    b. CareyB: Provisioning at TechEx: Sounds like a single event at the beginning of time; But much of the conversation was about account management, pushing changes out to keep connected systems in sync;
    c. Concerns around sustainability is real

d. BillT: We need to coalesce on an 80% consensus solution; Potential adopters are looking for guidance on choosing options.
e.

9. JSON for person representation (WarrenC)
    a. Minimal Person Schema
    b. TIER Application View Integration Layer Concept of Person Maintenance and Retrieval (Draft)

- For use by SORs to retrieve and maintain information related to a person entity.
- For use by any consumer application to acquire information related to a person entity
- 2017 Tech Ex Summary - Registry Summary techex 102017.pdf
- Diagram



- Application that is an SOR needs to indicate to the Identity System there is a new or changed person
    - It would invoke the Maintain Person logic that encapsulates the (Minimal registry, Affiliation and perhaps other groups, and other person data that the institution has defined beyond the minimal registry) Need to build this schema.
    - The service: validate the use of the service by the calling party/application
    - Person Schema (encapsulated version)
    - The service maps the data from the encapsulated schema into three subsets:
        - registry
        - groups
        - person detail
    - The service call the Registry rest call (Ethan K demo work)
    - The service call the Group rest call (grouper rest API)

        - The service call the Institution supplied Person rest call (need a sample)
- Review for Wednesday, Nov. 15

10. Primary API and Registry WG Projects Through EoY 2017
    a. Define next steps for each selected item
    b. Recommended first steps on SoR integration (item 10)
        i. Clarifying minimal person schema
        ii. Synthesizing the full person representation from SoR silos
        iii. 3 - 5 schools are Banner schools, so that's an attractive SoR to work with
    c. ID Match API (item 6)
        i. Edit above diagram to insert Id Match process step
        ii. Get IdMatch API up & running so we can build it into demos
    d. Provisioning (item 9)
        i. Written guidance for Campus Success program;
        ii. Coordinate with Lafayette (and others)

11. (Friday) Recasting our 2018 roadmap as a set of epics in Jira.
    a. See, e,g, API Guidelines epic
    b. If you can't access the above, contact wkaufman@internet2.edu

Next Meeting

Friday, 10 November 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

TIER APIs and Registry Working Group Agenda and Notes

Friday, 3 November 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

Participants

Keith Hazelton - UW Madison
James Babb - UW Madison
Tom Jordan - UW Madison
Bill Kaufman - Internet2
Ethan Kromhout - North Carolina (until about 10:50)
Rob Crowell - UMD College Park
Dave Shafer - Internet2
Jon Miner - UW-Madison
Chris Hubing - Internet2
Warren Curry - U Florida

Agenda

1. Did we learn anything at ACAMP that suggests course correction in our work plan?

    a. More demos, detailed samples, technical notes on solving specific problems; Some additions to minimal person registry, add to mP connector; e.g. oldId; What is the TIER Registry is still a question out there; Next six months challenge: as we get more into the technical specifics, it will be important to maintain the big picture. Reference architecture on one side and 1,000 Gists on the other; Evolve GDG into an Architect's Notebook; Make sure we take full advantage of the Campus Success Program, and provide value back to them

    b. [TomJ] Build an outline for the overall TIER Architect's Notebook

    c. (Dave Shafer, Internet2 DevOps) A Global Testbed for Trust and Identity - Scribing Google Doc
        i. DaveS: DevOps for T&I, started August; TechEx was 1st deep dive into T&I conferences; Summary of notes; Convener from Brazilian Federation; They have a local (federation) testbed;
        ii. Started with two attendees, ended with eight and had a very focused conversation, NicoleH, BrookS; EduGAIN testbed: Need a place to learn SAML and wire up some integrations to SPs;
        iii. TIER Testbed got some attention
        iv. FedLab One (not terribly active

v. JaneMarie: TIER does want to set up some kind of TIER federation
vi. DO NOT let the test infrastructure slip into production use; Dave thinks we have enough mechanisms to discourage production use. Lots of options for poison pills, e.g., make display names deliberately ugly.
vii. Information sharing, good documentation
viii. Talent: Hard to grow and maintain our talent pool;
ix. Continuing stream of new countries setting up national scale research and education federations; Nicole will take this back to REFEDS
x. What do we want out of this: Giving newbies a way to learn and experiment with Federated Identity and Access Management
xi. What did we learn from our experience with InQueue
xii. Global test federation will take a while; InC, Brazil, UKAMF, China? Lots of interest, but formal eduGAIN membership is too big a leap; Ethan: Special conditions;
xiii. Dave ("Where Development Meets The Cloud"): DevOps Manager, Trust and Identity: sitting at the intersection of Development and Operations; CI/CD; Building up a cloud infrastructure for Metadata Mgmt, Fed. Admin; Chris, Paul, Jim: using the same technologies, but not tightly integrated yet…
xiv. ChrisH: Testbed has lots of stuff; productiony stuff will go to the workbench.tier.internet2.edu; We need requirements; we can authorize ppl to spin up an environment and go wild; Github artifacts, mature the processes; Moving packaging into swarm; ScottK has a Spherical Cow testbed on a Debian base; Welcome volunteers who want to test things. Hint. Hint. John Gasper working on multi-stage Grouper; You can start with a base image with all the tools; throw the scaffolding out when it's up and running. From A+B+C+D in dev to A+B+D in prod.

d. (Gabor, TomJ, JonM) TIER Minimal Registry Architecture - Scribing Google Doc
   i. Lots of (cautious) support--a recognition that everyone will extent it, but primarily for local purposes; id reconciliation up front schools see value in the minimal registry model right off the bat; minimal reg is around interoperability; JonM: Usual debate around thick/thin. We need to write down the theory and practice; ODS vs Identity need to be expanded Upon; WarrenC: How affiliations were part of a group structure, not necessarily in the Registry; Tom/Jon: Big question we got across: Are you using this for authZ, if so, that should push you toward group/entitlement based access management; We just need to codify in clear documentation; Discussion around key change and identity history generally; Contact/profile info: email, phone#,...vs postal address; How do we manage that and find it? EthanK: But we do make use of 'permanent address'; of course it changes over time;

TIER APIs and Registry Working Group Agenda and Notes

(KeithH for BennO) Identity Collision Detection Scribing Google Doc

ii. UW-Msn Self-link; but sometimes people will not do the full discovery on possible multiple identities; Or ask them to authenticate...Even then ppl won't bother; someone reconnecting with a previous account is much harder than just creating a new identity from scratch;
iii. Source of problem: advisers say "go get a new account"; or person themselves don't want to take the trouble to revive their old account; Esp if the old account is not used for anything; If they later decide it's important, we should make it as easy on us--and them--as possible to make the link. JonM: You won't be able to slow people down; They WILL find the shortest path through the maze to get the cheese.
iv. Shift custodians to supplying affiliations, rather than instantiating identities directly.
v. Figured hourly rate for mergers - 3-4 hours for account reconciliation per merge. Splits were 10-12 hours; Social even longer
vi. It comes down to data sharing agreements. Is it okay for someone else to use data, they are just facilitator and broker.
vii. MDM - data about data, Master Data Management; Scope is ETL + Governance + technical controls; very tough sell.
viii. Huge new customer potential and revenue streams, but also need identity. Best sell for identity management.
ix. Gets back to quality & ingestion. Where are you enforcing quality? Before or after? All three places
x. When you do data quality analysis and show it to data owners, they'll help to solve it. Show statistics, and people will fix.
xi. Huge distance between cause and effect - the HR officer may not be aware of how they coded someone and how it impacts.
xii. Seems like this is more about governance and interaction than technology.
xiii. UC Berkeley summer students: good system, to be open sourced. Talk to Jeremy Rosenberg
xiv. Takeaway: Involve the user themselves in identifying multiple accounts
xv. Question: Worth it to codify a process for implementing identity first + user as authoritative?
xvi. Linking is hard; Detecting in advance is hard; We have an initial model embodied in COmanage (identity first);
xvii. Architect notebook couple pages on what is the problem called Identity Reconciliation? What are the alternative approaches? What are the tradeoffs between them.

xviii. BennO: Do you have a recommended config for the COmanage approach to this?

e. [JamesB] TIER Topics - Scribing Google Doc

f. [Keith] Authoritative sources for attribute aggregation/External Identities - Scribing Google Doc

g. [WarrenC] Grouper Provisioning Topics - Scribing Google Doc

2. Recasting our 2018 roadmap as a set of epics in Jira.
    a. See, e,g, API Guidelines epic
    b. If you can't access the above, contact wkaufman@internet2.edu

3. NOTE: Bill Thompson provided this link to a midPoint presentation at this Spring's ApacheCon: https://www.youtube.com/watch?v=_gPxURDKW7E

Next Meeting

Wednesday 8 November 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

- Grouper Visualization
- WarrenC's JSON?
- Recasting our 2018 roadmap as a set of epics in Jira.

TIER APIs and Registry Working Group Agenda and Notes

Wednesday 1 November 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

Participants

Jim Fox - UDub
Bill Kaufman - Internet2
Gabor Eszes - Old Dominion
Keith Hazelton - UW-Madison
Michael Hodges - U of Hawaii
Ethan Kromhout - UNC Chapel Hill
Bill Thompson - Lafayette College
Benn Oshrin - SCG
Tom Jordan - UW-Madison
James Babb - UW Madison
Jon Miner - UW Madison (apparently skiing?)
Keith Wessel - Illinois
Dean Lane - Rice

Agenda

4. Global Summit
    a. Demos: The one in the session was well received; the ones during breaks and lunch were rushed and a bit jumbled mainly because of timing and location
    b. Request a Track Session and do 2 or 3 demos; plus optional Working Meeting
    c. BillT: missed opportunity: Grouper BoF had 80-100; would get a lot better bang for the buck; we didn't get full value at TechEx; Global Summit was CIO-centric for a while, where is it now? Has it swung back in the direction of technology; JimF has same question; BillK: We had a larger T&I crowd at last Global Summit last time, and CIOs will be curious about TIER real-world readiness; So there has been some shift back from the exclusive focus on C** folks; JimF: Is it something we (TIER worker bees) should make an effort to attend?
    d. BillK: We can expect more architects going forward; If we want Track or Working Group, we'll need to get in the queue; High level demos (one or two) for C** level;
    e. KeithW: If we do the break/lunch sessions, get a better spot
    f. JonM: Recast the break/lunch as 'meet and chat' sessions; this puts us more into a vendor role; Get the main Track Session early in the schedule and pitch the availability of TIER staff during breaks for deeper conversations.
    g. Keep eye on Campus Success presentation possibilities;

h. BennO: Audience: the one with JASIG was smaller and more A in ACAMP; How do we get ACAMP folks to show up at Global Summit; Have an ACAMP at GS, too.

5. Tech Ex and ACAMP: Did we learn anything that suggests course correction in our work plan?
    a. HOMEWORK: Please scan the following list of ACAMP sessions and if you attended any of them, please review the notes for the session and put your initials in parentheses like this: (kh)
    b. Grouper Deployment Guide 2.0 - Scribing Google Doc
        i. JamesB: Audience spilling out the door; use more concrete example; didn't really get into what should be in GDG 2.0; Danielle's comment on user-oriented materials; BillT: Could provide more guidance on basis and reference groups; Long list of input from community based on 1.0; Figure out next steps; Global SUmmit would be a great opportunity to roll out 2.0; Easy to imagine more fleshed out examples of reference and basis groups: "Here's what it could look like in detail"; Permissions model for native Grouper objects; JamesB: Config example: Creating reference groups via loader, example of an actual subject source.
        ii. Grouper-dev discussions on GDG: Grouper-Dev is more tactical and developer-oriented, but they and we should make sure we're in sync;

    c. CACTI what should we focus on for the community? - Scribing Google Doc
        i. TomJ: CACTI meeting and ACAMP session: Discussed FIM4R meeting in Montreal; TomB put together a functional description of researcher's unmet requirements; CACTI is chewing on 'where do we go next with MACE-Dir; more generally the data and schema interoperability questions;

    d. OAUTH and crisis of static scopes Scribing Google Doc
        i. JimF led, JonM scribed: Direction going forward is to look at Roland Hedberg's OIDC Federation doc and see what we might take into the OAuth space; JonM: Line between the AuthZ server and Resource server is blurry, and they tend to get more tightly coupled; They will need some way to know their clients (see Roland's doc); As long as people insist on static scopes, OAuth will have a tough time gaining traction. GaborE: If you've given this any amount of thought, you recognize there's a crisis. If not, not. EG of a tightly coupled AuthZ/Resource server might help;
        ii. TIER is in the role of consumers here and we just need to do our best to keep up; perhaps generate a dynamic scope demo service

iii. Client/Service registry work might need some additional resource if it is to move forward; Some of it depends on the other federation work...

e. TIER Topics - Scribing Google Doc

f. Authoritative sources for attribute aggregation/External Identities - Scribing Google Doc
g. (Gabor, Tom, John) TIER Minimal Registry Architecture - Scribing Google Doc
h. (forthcoming) Grouper Provisioning Topics - Scribing Google Doc
i. SCIM Schemas - Scribing Google Doc
    i. GaborE: GailL would like a central place to catalog SCIM extensions; they'd like to adopt rather than invent; Discussed how it might be spun up; Survey of the groups working in the schema mongering space; discussion of correct venue candidates;
    ii. Keith Wessel is going to kick off a discussion over email with Gail, Gabor E, Keith W, Bill K, Ethan K and others?

j. TIER Provisioning/ SOR to registry Scribing Google Doc
    i. Ran over demos again, lots of questions

k. Identity Collision Detection Scribing Google Doc (TomJ)
l. (forthcoming) Privileged Access Management Scribing Google Doc
m. (forthcoming) Grouper Visualization Scribing Google Doc
n. VOPerson for collaborative orgs - Scribing Google Doc
    i. Goal was just to get it out there quick and informal first; short term it's under CILogon OID arc; After a couple of weeks of review is proof of concept feature complete, then deploy it in a real case; What's the best permanent home? REFEDs seemed reasonable at 1st glance;
    ii. https://voperson.org/
    iii. Draft: https://github.com/voperson/voperson/blob/master/voPerson.md
    iv. AARC2 conversation that Niels is leading also bears on this: https://aarc-project.eu/
o. Dockerizing Grouper- Scribing Google Doc
    i. General dockerization going forward; They seem set on Docker Swarm; but other container folks think Kubernetes is the future; PaulC: Example scripts is about as far as their commitment goes; JonM: Trust in ChrisHubing's take on issues like this; Docker Swarm comes with Docker and is free, so good choice for a TIER reference implementation;

Kubernetes version as a great idea for a community contribution; UW-Madison likely to move to Kubernetes at some point;

ii.

p. A Global Testbed for Trust and Identity - Scribing Google Doc
   i. Dave Shafer, new DevOps guy for Internet2, can give a report out
   ii. CareyB: Management of TIER as a project/product combined with the testbed/playground should be woven into the TIER maintenance/sustenance story; Big problems around moving to ++v1; The core issues are around the SDLC and core environments

6. Recasting our 2018 roadmap as a set of epics in Jira.
   a. See, e,g, API Guidelines epic
   b. If you can't access the above, contact wkaufman@internet2.edu

Next Meeting

Friday, 3 November 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

TIER APIs and Registry Working Group Agenda and Notes

Friday, 13 October 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

Participants

Warren Curry - UFlorida
Keith Hazelton - UW-Madison
Bill Kaufman - Internet2
Tom Jordan - UW-Madison
Bill Thompson - Lafayette College
James Babb - UW-Madison

Agenda

1. Short pre-TechEx check-in
    - Launch Status Check
        - Community Library folder is locked for write access,
        - Grouper four hour training on Sunday will morph into a two-day repeatable training event
        - Put Demos and Developer Face-to-Face materials in the TIER Community Library, “Technology Exchange Demos 2017” folder on Box. Scanning This QR code will also take you there
        - email materials to Bill Kaufman, he’ll get them into the folder

2. Demo snippet:
    - midPoint ⇐=> SCIM Slack Connector ⇐=> Slack user accounts
    - COmanage will be there for TechEx,

Next Event:

Internet2 Technology Exchange **Sunday Oct. 15 - Thursday, Oct. 19 2017**

TIER APIs and Registry Working Group Agenda and Notes

Next WG Meeting

Wednesday 1 November 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

TIER APIs and Registry Working Group Agenda and Notes

Wednesday 11 October 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

Participants

Keith Hazelton - UW-Madison
Gabor Eszes - Old Dominion
Jim Fox - UDub
Michael Hodges - U of Hawaii
Benn Oshrin - SCG (first hour only)
Bill Kaufman - Internet2
James Babb - UW Madison
Jon Miner - UW-Madison (technical difficulties…)
Chris Hubing - Internet2
Warren Curry - UFlorida
Carey Black - tOSU
Tom Jordan - UW Madison

Agenda

1. Confirm direction on event-driven messaging
    a. Do Component Architects agree to the following TIER assertion?
        i. The core messaging protocol, the one used internally between different TIER components, is AMQP 0.9.1, with support for external endpoints of various types: AMQP 1.0, STOMP, MQTT, JMS (SDK), AWS messaging and others.
        ii. The reference messaging implementation for TIER is RabbitMQ. That is, when we demo or deliver running code for messaging, the support will be provided by RabbitMQ. From the interoperability perspective, the TIER standard is around the protocol and not the particular implementation.
        iii. MichaelHodges: RabbitMQ in use for 2 yrs at Hawaii; Few years ago there were few deployments in edu; Jim Fox add AWS.

2. Discuss, confirm direction on storage/access of identity information
    a. for minimal person registry identity data
    b. for additional person identity information
    c. “Information switchboard” capability (implemented initially with configurable midPoint Resource definitions (sources and sinks))Beyond minimal registry.
        1. Need to be able to provide
            - Affiliation / group and robust person info (if desired).

- Using diagram I dug out yesterday let's discuss how /if this idea has merit.
- Not something we should do..
- Or something that can be moved to professional help status.

2. Gabor: Are we sticking to our commitment to TIER APIs delivering TIER schema? We don't have consensus beyond the minimal registry schema
   - We would perhaps recommend defining schema beyond the minimal registry attributes as extensions
3. BennO: COmanage: minimal schema is implementable as a subset; COmanage has its own expanded schema that mapping from COmanage in/out is based on the TIER APIs.
4. Model for switchboard: COmanage wired to midPoint: COmanage is inbound switchboard,

3. WG Update handouts for Developer Face-to-Face Thursday afternoon

   a. Messaging
   b. Schema
   c. Ref architecture diagrams, base, big pipe and demo overlays
   d. URL for OAI definitions/documentation of defined TIER APIs

4. TechEx demo updates

   a. TBD: Grouper ⇐⇒ SCIM Connector⇐⇒ Slack group data
   b. Friday: Self-service profile management in mP ⇐⇒ SCIM Connector⇐⇒ Slack user profile
      i. See https://wiki.evolveum.com/display/midPoint/Resource+Configuration
   c. Ethan's code is already in GitHub;
   d. Rather than handouts, we'll have a repository of presentations
   e. At Global Summit: 1) Slides of what the demo will show 2) then do the demo

   f. Customized Reference Architecture Diagrams
      i. Base Reference Architecture Diagram (template)
      ii. Internet2 COmanage Demo pipeline overlay
      iii. See the demo link below for more on COmanage https://spaces.internet2.edu/x/oQP9Bg
      iv.

   g. Handouts (QR codes as well as / rather than URLs)

TIER APIs and Registry Working Group Agenda and Notes

Next Meeting

Friday, 13 October 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

3. Short pre-TechEx check-in
4. Couple demo previews

TIER APIs and Registry Working Group Agenda and Notes

Friday, 6 October 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

Participants

Tom Jordan - UW Madison
James Babb - UW Madison
Keith Hazelton - UW-Madison
Jon Terrones - UW-Madison
Bill Kaufman - Internet2 (on till 10:30 and hopefully back around 11)
Ethan Kromhout - UNC Chapel Hill
Carey Black - tOSU
Jon Miner - UW-Madison
Gabor Eszes - Old Dominion
Benn Oshrin - SCG
Bill Thompson - Lafayette College

Agenda

1. Review the fat arrow version of the expanded ref arch diagram an official TIER graphic

2. Canvas Provisioning Demo dry run; (JamesB, TomJ)
    a. PResentation: Back to GS points: Overall AuthZ flow thru GDG; institutional data drives data-driven gr, institutional meaningful cohorts. Enterprise AuthZ policy; AuthZ groups; provisioner is a thin layer to get the policies
    b. Messaging for loose coupling unix philosophy small things doing one task

3. Drupal Provisioning Demo dry run; hr->midpoint->openldap->grouper->midpoint->Drupal (EthanK)

4. JSON API and JSON Schema as additional TIER guidelines; Relationship to OAS 3.0 (was Swagger)
    a. This is Alan Crosswell's choice at Columbia U.
    b. HOMEWORK for Wednesday: Do these JSON specs clash with OAS 3.0
    c. JSON Schema is a way to specify the way the payload looks on the wire, it's used by SCIM, so we have inherited it.
    d. JSON API is a barebones way of laying out an API; may restrict our structures, and this is contrary to a more strictly RESTful approach
    e. It is a hypermedia API (simpler end of the spectrum, at least); see their notion of relationship; two ways to refer to other things; We've inherited much of the machinery from SCIM which addressed these issues already.

   f. OpenAPI gives structure of endpoints, relationship between them & definitions of the resources.

5. Grouper
   a. 35-6 For the Sunday Grouper Seminar; will show breadth of what a 2-day Grouper training event would cover
   b. ACAMP session for GDG next steps; plan a revision forGlobal Summit
   c. Carl Waldbieser will propose an ACAMP session on routing keys, RabbitMQ;

6. If BillK wants screenshots from the demos just have him ask EthanK

Next Meeting

Wednesday 11 October 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

TIER APIs and Registry Working Group Agenda and Notes

Wednesday 4 October 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

Participants

Jon Miner (UW-Madison)
James Babb (UW-Madison)
Keith Hazelton (UW-Madison)
Warren Curry (U-Florida)
Bill Kaufman (Internet2)
Jim Fox (UDub)
Michael Hodges (U of Hawaii)
Gabor Eszes (Old Dominion)
Carey Black (tOhio State)
Tom Jordan (UW-Madison)

Agenda

1. COmanage->openldap->midpoint and more (BennO)
    a. Potential ‘demo’
    b. Screen share: COmanage provisioning screen; midPoint UI screen
    c. Testbed midPoint LDAP source
    d. On midPoint side; fake student sys - csv - match engine - match identifier (system-to-system identifier) - prov to midPoint ldap;
    e. next step is to sync with midPoint registry
    f. Matching process demo could make an ACAMP session
    g. BennO has a spreadsheet of metrics for the match engine performance; 45-55 ms per match; if you add more matching rules, goes up linearly with number of rules (fuzzy matches, etc.)
    h. Matching up front (pre-registry) could be done post-registry
    i. COmanage as a research support service integrated somehow with the traditional institutional IAM platform
    j. COmanage COU is parallel to the notion of System of Record in traditional IAM flows
    k. Data sync issues need solution
    l. COmanage as identity registration service, feeding to a bespoke ‘directory’ that is also a source for midPoint Enterprise registry and provisioning engine; registration tags with the ‘system-to-system’ identifier
    m. A hybrid architecture with COmanage and midPoint; enterprise scale, it makes more sense to use best of breed solutions
    n. Latent capabilities for provisioning in many components, so for people in the market for a provisioning; if Grouper provisioner solves your provisioning

problem, use it, likewise COmanage; midPoint for more complex provisioning scenarios

1. Any more ideas for ACAMP session proposals?
    o. UMA 2;
    p. JimFox and the coming disaster of static scopes
    q. Out there: GraphQL vis-a-vis HTTP verbs and resource representations (KeithH)
    r. Event-driven messages beyond Grouper
    s. Integrating OAuth AuthZ Server into an entity registry so clients don't have to register with multiple AuthZ Server
    t. Discussion on minimal registry; maintain person from multiple sources; One logical source of person identity and permission data
    u. Could one outcome of ACAMP sessions be proposals for TIER component design changes? (minimal registry and person APIs review)
    v. Aug. 25th notes: SoR to Registry as an ACAMP session
    w. Matching process demo/discussion as an ACAMP session per item (1)
    x. Handling identifier crosswalks; see https://tools.ietf.org/pdf/draft-grizzle-scim-pam-ext-00.pdf

7. Other TechEx prep items?
    a. [Demo leads] Get the demo whitepapers done in time
        i. as we've done at TechEx and Global Summit; include a walking tour through the demo flow. Reinforce the connection between reference architecture and reference implementations
    b. Note: We have 198 registered for the Trust and Identity track for TechEx (not counting Internet2 staff). Last year the number was 171.
    c. Formal OIDC/OAuth WG session at TechEx from Steve Carmody's TAC WG; Wednesday at 4:50 pm
    d. **Reminder: TIER F2F at 2017 Tech Ex is Thursday, October 19, 2017, 12:30 -- 4:00 pm...REGISTER HERE**

8. (Friday) Canvas Provisioning Demo dry run; hr->midpoint->openldap->grouper->midpoint->Drupal (JamesB, TomJ)

9. (Friday) Drupal Provisioning Demo dry run; hr->midpoint->openldap->grouper->midpoint->Drupal (EthanK)

10. (Friday) Quick Look: Proposed SCIM Schema that could be used to carry identifier crosswalks

11. (Wednesday) Confirm the fat arrow version of the expanded ref arch diagram an official TIER graphic

TIER APIs and Registry Working Group Agenda and Notes

Next Meeting

Friday, 6 October 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

TIER APIs and Registry Working Group Agenda and Notes

Friday, 29 September 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

Participants

Jon Miner UW-Madison
James Babb UW-Madison
Ethan Kromhout - UNC Chapel Hill
Bill Kaufman - Internet2
Keith Hazelton - UW-Madison
Benn Oshrin - SCG, etc.
Tom Jordan - UW-Madison
Jon Terrones - UW-Madison
Chris Hyzer - Penn
Warren Curry - UFlorida

Agenda

1. Update: SCIM-based provisioning mP to Slack

2. The Reference Architecture Pipe
    a. See attachments to Warren Curry's email just now, "[tier-api] updated with larger / fewer arrows pipe diagram for architecture detail."
    b. A pdf is available

3. Unicon and midPoint: What's brewing?
    a. Packaged version a la TIER Packaging WG
    b. Connectors for SCIM v2 and messaging endpoints
    c. WarrenC: Maintain/Get person (full identity info, not just the minimal schema elements) See diagram from July) CRUD operations
        i. Affiliation type data managed via Grouper
        ii. Other person data can be found in 'another data store'
        iii. Configuration for which attributes go to / come from which repository
    d. JonM: Orchestration aspect of this problem, probably a local task to set this up
    e. Iterative approaches to development with TIER and Unicon parties involved
    f. Longer term: RFP for OIM replacement; share info so we can enrich our requirement set;
    g. How can the external config data be injected into a CI model; Unique object identifiers are a challenge moving through Dev/Test/Prod

h. UI components of request workflows need work, resource catalogs, etc.; user making a request how can we show what they can request and gather their input.
i. TechEx presentations: Ask Steve what words we should put around the place and status of midPoint as a component in TIER
    i. **midPoint is an Emerging TIER Component that compliments COmanage and Grouper to handle provisioning/de-provisioning as well as provide the SCIM api template we need to perform registry services**

4. Quick Look: Proposed SCIM Schema that could be used to carry identifier crosswalks

> Let's take a quick look-over of this new Internet Draft during our Friday WG meeting.
> https://tools.ietf.org/pdf/draft-grizzle-scim-pam-ext-00.pdf
>
> For one thing, note the new Linked Object resource. A non-normative example is
>
> "urn:ietf:params:scim:schemas:pam:1.0:LinkedObject":
> { "source": "Corporate Active Directory",
> "nativeIdentifier": "cn=Barbara Jensen,ou=Users,dc=example,dc=com" }
>
> This seems useful for representing and sharing identifier crosswalks among other things.
>
> Another proposed construct to look at: "Privileged Data" in a "Container" can include, e.g., credentials and access control lists can be defined over Containers.
>
> --Keith

Next Meeting

Wednesday 4 October 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

TIER APIs and Registry Working Group Agenda and Notes

Wednesday 27 September 2017, at 3:00 pm Eastern, Noon Pacific, 8 pm UTC

Participants

Keith Hazelton - UW-Madison
Ethan Kromhout - UNC Chapel Hill
Jim Fox - UDub
Benn Oshrin - SCG
Gabor Eszes - Old Dominion
Brian Savage - Boston College
James Babb - UW Madison
Jon Miner - UW Madison
Tom Jordan - UW-Madison
Bill Kaufman - Internet2
Carey Black -tOhio State
Warren Curry - UFlorida

Agenda

1. Grouper TIER API updated to OAI 3.0 (thanks, BrianS!)

> FYI, the swagger/OAI specification for the work Chris and Vivek did integrating SCIM-like operations with Grouper has been hydrated again in two forms on SwaggerHub (freemium account) - feel free to move them if you want/need:
>
> 1. The original spec (had to revise for a response format conflict see *** below) is now at:
>
> https://app.swaggerhub.com/apis/bsavage/grouper_scim_OAI3/v2
>
> This works in the editor and UI at this address.
>
> You can, in real-time, interact with this spec (assuming the grouperdemo server is up an running - it has been)
>
> There is a test credential (test, test123) that Chris provided for it.
>
> Just click the "Authorize" button on the UI to enter the basic auth credential above. I always then try the

GET /Groups by id

As in the doc for that operation there is a group id that can be used: *b32e826380ea42c69dbf59cc262584f8*. I can't vouch for all the other operations but they used to work. It neatly shows you the curl request, and the full response and headers.

2. This spec was also converted to OAI v3 (using SwaggerHub's conversion option) and can be accessed here:

https://app.swaggerhub.com/apis/bsavage/grouper_scim_OAI3/v2-oas3

As OAI is working on the UI for the OAI v3 spec, one can't yet interact in real-time.

Cheers,

Brian

*** minor problem, but there is an unfortunate conflict that caused the spec to no longer load in these spec editors; specifically, a response field in the json called "$ref" causes confusing with its $ref schema syntax in the spec editor; for the time being, this property is now called just "ref" - could cause some responses to be considered invalid in swagger tools I suppose

- You can enter examples into the source file.
- RAML is still in use for modeling APIs, but some convergence is happening
- Mulesoft has announced a shift in emphasis, they want the best of both worlds; They will support RAML in their tooling; RAML as an intermediate format that they recommend be used in the design stage;
    - https://blogs.mulesoft.com/dev/api-dev/open-api-raml-better-together/
    - https://github.com/raml-org/api-modeling-framework

2. Integration pipe diagram layout: Review and decide
    a. See email thread “the diagram from last Friday morning’s workgroup meeting”
    b. integration pipe
        i. LDAP placement ?
        ii. SHould small arrows be replaced with larger less detail (bIll intention)

iii. Floating section Authentication… (use large arrow to right an from the Integration pipe)
iv. Pull out Demo support as a separate issue

3. midPoint assistance from Unicon (initial discussion tomorrow)
    a. What are the most urgent features or enhancements?
    b. How do we work with the Campus Success partners?
    c. No object ancestor that could be used to represent non-person entities; mP plans to evolve; Igor provided a link to their approach; See mP Slack channel
    d. Representing the person schema in mP?

4. ACAMP Prep
    a. Demos
        i. Flow
        ii. Making it less dull: Some form of the “You are here now” flow
        iii. Split screen showing console logs for the more technical
        iv. Logging the message and showing the schema
        v. COmanage: storyline is around the tasks of a VO manager spinning up a research team, pulling in person data from Internet2 Salesforce and providing team members with tools like Wiki, Jira, Sympa and data resources, as well as managing access appropriately.
            1. Internet2 COmanage architecture
        vi. TIER Session and demo of Canvas: Event-based messaging with query-back to the API; then provisioning it out to Canvas.
        vii. OS HR system in Docker containers; create an new emp. AMQP with minimal schema; mP connector creates a mP user, project that to LDAP, Grouper can do allow/deny authorization group; Processed into provisioning
        viii. Next Wednesday Screen share dry-run of
            1. mP ⇒ demo ⇒ Slack/LucidChart (mP logging issue: barfs on JSON
            2. Event-driven provisioning to Canvas

    b. ACAMP Session Ideas and volunteer leads
        1. Out there: GraphQL vis-a-vis HTTP verbs and resource representations (KeithH)
        2. Event-driven messages beyond Grouper

3. Integrating OAuth AuthZ Server into an entity registry so clients don't have to register with multiple AuthZ Server
4. Discussion on minimal registry; maintain person from multiple sources; One logical source of person identity and permission data
5. Could one outcome of ACAMP sessions be proposals for TIER component design changes? (minimal registry and person APIs review)
6. Aug. 25th notes: SoR to Registry as an ACAMP session

ii. Note: OIDC-OAuth WG meeting at TechEx Wed at 4:50 - see https://meetings.internet2.edu/2017-technology-exchange/detail/10004957/

Next Meeting

Friday, 29 September 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

TIER APIs and Registry Working Group Agenda and Notes

Friday, 22 September 2017 at 10 am Eastern, 7 am Pacific, 3 pm London, 4 pm Amsterdam

Participants

Keith Hazelton (UW-Madison)
Warren Curry - UFlorida
Jon Miner - UW-Madison
Ethan Disabb UFlorida
Bill Kaufman - Internet2
Carey Black (tOSU)
Tom Jordan - UW\-Madison
James Babb - UW Madison

Agenda

1. For the first hour, we are invited to join the inaugural call of the InCommon OIDC Deploy WG
    a. Working Group Summary and Charter: https://spaces.internet2.edu/x/jJiTBg

    b. OAuth-OIDC Friday agenda and call-in info: https://docs.google.com/document/d/1w_r_JhZX-lzPWjL0H9PWrTeY9efaII1K9TDnp3qtz9I/edit

The first meeting of this new InCommon Working Group on OIDC deployment overlaps the first hour of our API/Registry WG call Friday morning. I'd like to listen in on this and encourage others to do so as well. We'll still meet as API/Registry WG for 1/2 hour, from 11:00 to 11:30 am Eastern --Keith

1. Drill-down on the 'integration pipe' in the Reference Architecture (Warren Curry)
    a. LDAP is what? TJ: A connected system that already exists on most campuses
    b. What is the starting point for this diagram?
        i. https://www.internet2.edu/media_files/2809
        ii. https://spaces.internet2.edu/display/TIERENTREG/IAM+Functional+Model+and+IAM+Glossary?preview=/94896405/113247708/IdentityEcosystem(3).pdf
        iii. https://spaces.internet2.edu/display/TPD/TIER+101

c. HOMEWORK: Email sketches of revised versions in whatever format suits, and we will review them on Wednesday