IAM Committee
Meeting Notes
01/08/2018

Attending: Dash Ballarta, CW Belcher, Michael Bos, Graham Chapman, Tom Fackler, Ed Horowitz, Olu Kole-James, Felipe Lee, Ty Lehman, Jason Mayhew, Mike McIntosh, Dustin Slater, Charles Soto

Absent: Cam Beasley, Cesar de la Garza, Alison Lee, Darin Mattke, Shelley Powers, Steve Rung

IAM Team Members Present: Michele Graham, Justin Hill, Mario Leal, Reece Price, Aaron Reiser, Autumn Shields, Caroline Taylor

1. IAM Initiatives in 2018 – Review (CW Belcher)

Reference handout.

In 2018 the IAM Team will primarily be focused on four major initiatives:

1. Top priority is Workday readiness
2. Bringing the new UTLogin environment online
3. Upgrading the SailPoint IdentityIQ software version
4. Technical Resource Account Control (TRAC) retirement

Q: Could you explain the “+Integration Support” designation on the IAM Roadmap handout?
A: Integration support had previously had its own line item, but it is now part of the team’s ongoing operations/sustainment process. As such, it was moved into the Sustainment category.

The team will not be focusing on adding major new functionality in SailPoint this year. The focus will be on customer integrations and the software upgrade.

Q: Given that focus, what will you not be focusing on?
A: The original plan was to begin work on retiring the uTexas Identity Manager (TIM), but based on available resources and other priorities that work will be delayed. We will, however, be working to simplify password policies and improve password security this year.

2. UTLogin Stability Roadmap Progress – Update (Mario Leal)

Reference handout.

There were two UTLogin outages on December 9, 2017. Both of these outages were due to memory exhaustion on the load balancer. An incident report has been published (see https://wikis.utexas.edu/x/EsS7Cg).

The Design phase of the project to replace the UTLogin environment will be completed once external parties finish their final reviews of the design documents. Work is in progress to build out the Test environment. Marta Lang has joined the project team and is helping to rebaseline the effort.
In the past three months, all UTLogin outages were due to upstream dependencies and not due to UTLogin itself.

3. Legacy Authorization Roadmap – Update (Michele Graham)

Reference presentation.

The project team held a town hall a few months ago with users of Apollo. Apollo users expressed an interest in improving how Apollo authorizations are managed, accessing Apollo data outside of the mainframe, and tools to help review existing authorizations.

The team’s top priority for this year is Workday readiness. The team will review potential improvements once Workday readiness work is complete.

The project team also met with stakeholders for the Organizational Hierarchy System Contacts (OHSC). Their primary interest was in making it easier to keep contacts up-to-date.

Workday readiness development work has begun for Apollo. This includes coding to batch-replace role-based authorizations with person-based authorizations. The same development work for OHSC is in progress. Next month, the team will start work on interface changes. The team anticipates promoting these changes into the Quality Assurance environment at the beginning of June and into the Production environment at the end of July, which would be approximately three months prior to the scheduled Workday go-live.

Q: What data will be imported from Apollo into SailPoint?
A: This has not yet decided but the team is currently reviewing the data and doing exploratory work. Importing group membership information is straightforward, but authorization information will be more complicated.

Q: Given the age (and likely deprecation) of the data in Apollo, would it make sense to perform opt-in or ad hoc data imports as opposed to a batch import of all the data?
A: The project team will review that as an option.

Q: Could the same review be done with OHSC data?
A: Yes. Our discussion with stakeholders has already revealed that some of the contact types can be retired.

Q: In advance of a deprecation of OHSC data, it would be helpful to know what the data is being used for.
A: Some contact types are obsolete, but others are still being used. A key to obtaining this information will be to implement a better process for ensuring that the contacts are up-to-date.

Q: The presentation states that data will be published to the uTexas Enterprise Directory (TED) or Active Directory (AD). Has that decision been made?
A: Not yet. The decision will depend on customer need. OHSC data is already being published to TED. If
there is a customer need to publish some or all of the data in AD, then the project team will review and consider that need (in partnership with the AD team).


Status update on the password security enhancements.

The IAM Team is preparing a recommendation for changes to the EID password rules. These recommendations are based on new recommendations from the National Institute of Standards and Technology (NIST) which primarily focus on encouraging the use of passphrases.

A draft recommendation is set to be reviewed by the Information Security Office (ISO). The goal is to have a recommendation available to the committee for review by the next meeting.

**Comment:** The Dell Medical School may be held to different standards for password rules. Additional research is needed to determine if this is the case and, if so, what technical solutions might be available to meet those requirements.

5. **1/14 UDC-C Network Maintenance Impact – Review (Mario Leal)**

Network maintenance will take place this Sunday, January 14, 2018, which affects core routing in the University Data Center (UDC). This will result in outages for all services hosted in the data center, including authentication and directory services.

The uTexas Identity Manager (TIM) and UTLogin teams will have technical leads doing pre- and post-maintenance work to prevent synchronization issues which might have resulted from the maintenance. All IAM services will be verified after the maintenance to ensure return to service.

6. **Other Initiatives Updates**
   a. **IAM Team Staffing (Mario Leal)**

The IAM Team has two open positions: a Senior Software Developer/Analyst (SSDA) and a Software Engineer (SE). Applications for the SSDA position are currently being reviewed. The team is hoping to have a hiring decision regarding the SE position by the end of the week.

   b. **IAM Integrations (Justin Hill)**
      i. Starting Backlog (December 1): 25
      ii. 1 New: (Zoom)
      iii. 0 Reopened:
      iv. -3 Completed: (Aeon, DAMS-GLIB2, Information Quest-Tableau,)
      v. 0 Cancelled
      vi. Ending Backlog (December 31): 23

There was a spike in pre-holiday break work, but the number of completed integrations is greater than the number of new integrations. Things are moving well despite the holiday, and the team will be re-engaging with customers.
c. IAM Modernization Program / SailPoint Implementation (CW Belcher)

Phase 1 of the IAM Modernization Program (IAMMP) was formally closed out prior to the holiday break. All Phase 1 deliverables contracted with KPMG have been completed and closed out.

A SailPoint release is scheduled for implementation this month to fix bugs and implement change requests from early adopters.
### IAM Roadmap Initiative Descriptions

<table>
<thead>
<tr>
<th>Initiative</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IAM Solution Selection (Complete)</strong></td>
<td>Select and procure new IAM software to support and enable the roadmap goals.</td>
</tr>
<tr>
<td><strong>IAM Solution Implementation Planning (Complete)</strong></td>
<td>Complete high-level planning for the implementation of the software selected in the IAM Solution Selection project.</td>
</tr>
<tr>
<td><strong>IAM Modernization Program</strong></td>
<td>IAM Modernization Program includes IAM ASMP Integration Strategy (Complete): Support authentication and identity data integration with University strategic projects, including Workday, TAI, application modernization, and ServiceNow. (Incorporated into Sustainment in FY17-18)</td>
</tr>
<tr>
<td><strong>IAM Web Central Migration (Complete)</strong></td>
<td>Migrate IAM web site content off of the end-of-life Web Central platform.</td>
</tr>
<tr>
<td><strong>UTLogin Transition / CWA Retirement (Complete)</strong></td>
<td>Transition Central Web Authentication &amp; Fat Cookie customers to UTLogin and retire the CWA/FC authentication system.</td>
</tr>
<tr>
<td><strong>UTLogin OpenAM v11 Upgrade (Complete)</strong></td>
<td>Upgrade UTLogin to the current version of OpenAM software to address bugs, implement session management enhancements, and stay current with vendor support.</td>
</tr>
<tr>
<td><strong>UTLogin Realm Policy Manager Enhancement (Complete)</strong></td>
<td>Enhance the UTLogin RPM to allow delegated administration of sites on shared hosting environments like UT Web and Windows Web Hosting.</td>
</tr>
<tr>
<td><strong>UTLogin Stability &amp; AMS Upgrade</strong></td>
<td>Stabilize the UTLogin environment and upgrade to current version of OpenAM software to address bugs, implement policy management enhancements, and stay current with vendor support.</td>
</tr>
<tr>
<td><strong>Identity Assurance Framework Development (Complete)</strong></td>
<td>Implement a framework to assist campus departments in assessing risks and selecting an appropriate level of assurance to mitigate those risks.</td>
</tr>
<tr>
<td><strong>Toopher Pre-generated OTP Enhancement (Complete)</strong></td>
<td>Add the ability to use pre-generated one-time-passwords (OTPs) with Toopher.</td>
</tr>
<tr>
<td><strong>Duo Implementation</strong></td>
<td>Implement two-factor authentication using the Duo Security solution.</td>
</tr>
<tr>
<td><strong>Lightweight Authentication &amp; BYOId</strong></td>
<td>Implement a lightweight identifier and authentication service and integrate with external identity providers (Bring Your Own Identity).</td>
</tr>
<tr>
<td><strong>Central Authentication Resiliency Enhancement</strong></td>
<td>Improve the resiliency of central authentication services by leveraging off-campus hosting.</td>
</tr>
<tr>
<td><strong>Shibboleth v3 Upgrade (Complete)</strong></td>
<td>Upgrade the Shibboleth federated authentication solution to the currently supported version.</td>
</tr>
<tr>
<td><strong>Legacy Authorization Services Roadmap Planning</strong></td>
<td>Define the transition and retirement roadmaps for Apollo, OHS Contacts, and DPUSER Department Contacts systems and communicate with campus stakeholders.</td>
</tr>
<tr>
<td><strong>Legacy Authorization Services Workday Preparation</strong></td>
<td>Implement changes in Apollo, OHS Contacts, and DPUSER Department Contacts systems required by the transition to Workday.</td>
</tr>
<tr>
<td><strong>TIM Server Refresh &amp; Database Migration (Complete)</strong></td>
<td>Retire out-of-warranty servers and migrate to virtual server infrastructure and enterprise Oracle service.</td>
</tr>
<tr>
<td><strong>IAM ASMP Integration Strategy (Complete)</strong></td>
<td>Define high-level plan for maintaining required integrations while source systems and IAM system are being replaced.</td>
</tr>
<tr>
<td><strong>Administrative EID Creation User Interface</strong></td>
<td>Provide a user interface for administrative creation of EIDs (required to support Workday Hire process).</td>
</tr>
<tr>
<td><strong>Password Security Enhancement</strong></td>
<td>Improve the security of EID password storage infrastructure.</td>
</tr>
<tr>
<td><strong>TED Server Refresh (Complete)</strong></td>
<td>Retire out-of-warranty servers.</td>
</tr>
<tr>
<td><strong>WHIPS OS Upgrade / VM Refresh (Complete)</strong></td>
<td>Migrate to supported OS version and refresh virtual server infrastructure.</td>
</tr>
<tr>
<td><strong>Directory Services Roadmap</strong></td>
<td>Document new and evolving TED use cases and requirements and plan approach for addressing</td>
</tr>
<tr>
<td></td>
<td>issues as they arise.</td>
</tr>
<tr>
<td><strong>TED via Web Services (ESB) - Phase 1 (Complete)</strong></td>
<td>Implement an initial set of TED services on the ESB (public directory information lookup, group membership lookup, confidential directory information lookup).</td>
</tr>
<tr>
<td><strong>ID Photos OS Upgrade / VM Refresh (Complete)</strong></td>
<td>Migrate to supported OS version and refresh virtual server infrastructure.</td>
</tr>
<tr>
<td><strong>ID Card System Replacement</strong></td>
<td>Modernize ID Card System and remove mainframe dependency. (Deferred)</td>
</tr>
<tr>
<td><strong>TRAC Saturn/Gemini Retirement (Complete)</strong></td>
<td>Retire use of out-of-warranty servers.</td>
</tr>
<tr>
<td><strong>TRAC UTS Retirement (Complete)</strong></td>
<td>Migrate TRAC functions off end-of-life UTS service.</td>
</tr>
<tr>
<td><strong>SDS UTS Retirement (Complete)</strong></td>
<td>Migrate SDS functions off end-of-life UTS service.</td>
</tr>
<tr>
<td><strong>TRAC Replacement (ServiceNow)</strong></td>
<td>Replace TRAC functionality using ServiceNow.</td>
</tr>
<tr>
<td><strong>Apps Build Server Maintenance (Complete FY14-15)</strong></td>
<td>Maintenance and enhancements required to support ITS Applications software build and testing infrastructure.</td>
</tr>
</tbody>
</table>
Items for Management Attention

During the ITS Networking UDC-C network outage on Sunday, January 14, 2018, 8:00 AM – 11:00 AM, UTLogin authentication will experience disruptions while network equipment is being replaced.

UTLogin Roadmap Status

**Action 1: Stabilize Current UTLogin Environment (Complete)** - As of June 8, 2017, the IAM team disabled the self-service Realm Policy Agent and put the existing UTLogin environment in a “critical fix only” mode. Efforts will now focus on Action 2.

**Action 2: Simplify & Standardize UTLogin Environment (In Progress)** - Team is currently in Design and Build TEST environment phase. The design documentation is final review with external team. While we continue to build the TEST environment, we are working to rebaseline the phase and develop the plan for the verify TEST Environment phase.

**Action 3: Measure & Report Progress (Ongoing)** - KPIs have been identified and are being published on a weekly basis (See: [http://iamservices.utexas.edu/projects/utlogin-stability-report/](http://iamservices.utexas.edu/projects/utlogin-stability-report/)). Monthly status updates will be provided outlining incidents, KPI’s, and project status.
UTLogin Availability

This graph represents UTLogin’s overall availability since September 14, 2017 along with UTLogin’s published SLO of 99.42%. This data shows that since UTLogin was put into critical/fix only mode on June 8, 2017, the number of service disruptions has decreased. However, the service did sustain an issue on December 9, 2017 due to memory exhaustion of the load-balancer.

Historical data and other Key Performance Indicators (KPI’s) which reflect the stability of UTLogin are published every Friday. The weekly report is viewable here: https://iamservices.utexas.edu/projects/utlogin-stability-report/.
Legacy Authorization Systems Roadmap (LASR) Update

IAM Committee Update
Monday, January 8, 2018
Update on Apollo Roadmap

• Solicited input from the community via a town hall meeting

• There was interest in making improvements to:
  • Reduce effort to manage authorizations
  • Access Apollo data off of the mainframe
  • Facilitate timely reviews of access
Guiding Principles for Apollo Roadmap

- Workday readiness is top priority
- Focus on ways to make it easier to manage and use the data – avoid changes to core Apollo functionality
- Do simpler SailPoint integration steps first, then move on to more complex
Prioritizing Apollo Work

**Priority 1:** Prepare for Workday go-live
- Switch to “DY” modules
- Remove position-based authorization functionality

**Priority 2:** Import Apollo data into SailPoint (read-only interface)
- Enable SailPoint reporting on Apollo authorizations
- Publish Apollo data in TED and/or AD
Prioritizing Apollo Work

Priority 3: Push data from SailPoint to Apollo (read/write interface)
  • Automate Apollo group assignments
  • Allow bulk updates

Priority 4: Configure certification campaigns
  • Enable periodic reviews of authorizations to meet policy and audit requirements
Apollo Work Timeline

- FY17-18 will focus on Priority 1: Workday preparation
- Will reassess timeline for Priority 2-4 work once Workday preparation is completed
Update on OHSC Roadmap

- Solicited input from the OHSC users:
  - Contact type owners
  - Consumers of OHSC data
  - Business users
- There was interest in making it easier to keep contact assignments updated
OHSC Work Timeline

• FY17-18 will focus on Workday preparation
• Will reassess timeline for other work once Workday preparation is completed
Timeline for Apollo and OHSC Workday Changes

- Apollo Data Conversion Development: 6/1/2017 - 7/25/2017
- Apollo System Interface Changes: 7/25/2017 - 10/27/2017
- OHSC Data Conversion Development: 11/24/2017 - 2/7/2018
- OHSC System Interface Changes: 2/8/2018 - 4/20/2018
- QUAL Data Conversion and Deployment: 6/1/2018
- PROD Data Conversion and Deployment: 7/29/2018

Workday Go-Live: 11/1/2018
Questions?