IAM Committee
Meeting Notes
08/13/2018

Attending: Cam Beasley, CW Belcher, Hatty Bogucki, Tim Fackler, Ed Horowitz, Alison Lee, Felipe Lee, Ty Lehman, Luke McEneny, Mike McIntosh, Chris Owan, Steve Rung, Dustin Slater

Absent: Cesar de La Garza, Darin Mattke, Jason Mayhew, Shelly Powers, Bernie Sanfeliz, Charles Soto

IAM Team Members Present: Mario Leal, Marta Lang, Justin Hill, Reece Price, Autumn Shields

1. Introductions (Including phone attendees)

2. Committee Chair for FY18-19 – Approve
   - Dash will be out of the country until late 2019, so we will need a new chair. Steve Rung has agreed to fill the role for FY18-19.

   Question: Are there any objections to Steve taking on the role of Committee Chair?
   No objections noted.
   - If anyone would like to be Co-Chair, please let CW know. The Co-Chair normally becomes the Chair the following year.

3. Proposal: Move September meeting to September 17th (CW Belcher)
   - This proposal is to move the September meeting back one week from the 10th to 17th because of the Labor Day holiday and staff availability.

   Question: Are there any objections to this change?
   No objections noted.
   - We will send out a revised meeting update

4. Multi-Factor Authentication Expansion Update (Mario Leal & Cam Beasley)

   Cam Beasley:
   - We have talked about this in previous meetings. There is a growing trend of compromised users occurring on campus. This is significantly outpacing the number of compromised computers. Controls around mail and other resources are being exploited.
   - UT System is considering new requirements to expand MFA. We are trying to get out in front of this problem with a proposed MFA strategy for campus.
   - The strategy has been pitched to Internal Audits, Executive Compliance Committee, and was generally endorsed by president and other members.
• The Executive Compliance Committee also suggested MFA become universal for current students/faculty/staff. Up to this point our plan was MFA for “High Risk” Applications. This will make it easier to communicate, but not easier to implement.

• To make the user experience easier, we have proposed a 30-day “remember device” session.

• There are some interesting timing issues around this. We have been trying to implement expanded use of MFA as quickly as possible, because there are concerns from different compliance and audit stakeholders. However, add the 30-day session enhancement will take time to implement (available in early spring).

• At the same time, Workday will be launching with MFA for all users.
  o To avoid overloading the help desk, Workday does not want to be one of the larger services to go MFA first. Candidate applications to go MFA before Workday include Timesheets, HRMS, and FRMS.
  o Workday users will experience MFA at each login until remembered devices is implemented.

Mario Leal:

• The IAM team has reviewed what would be required to make the following changes in our MFA environment:
  o Implementing a 30-day remembered device session
  o Enforcing MFA for current students, faculty, staff, as well as future employees (but not others such as guests)
  o Extending the login session timeout from 1 to 3 hours
  o Enabling MFA for specific applications in advance of the Workday go-live

• Findings:
  o We can implement a 30-day session and require current students/faculty/staff to use MFA in Shibboleth and UTLogin v1. However, making these changes to UTLogin v1 poses a risk to the stability of UTLogin v1 and will delay work on UTLogin v2.
  o We are currently evaluating the work required to UTLogin v2 to add these enhancements.
  o We have confirmed that extending the session timeout to 3 hours is possible
  o We have also confirmed that we can enforce MFA centrally for applications that use UTLogin WPA and Shibboleth SAML. However, applications that use UTLogin SAML will need to request MFA in their requestContext.

Q: What is going to happen if direct LDAP Authentication is being used?

A: We don’t currently have an MFA solution for direct LDAP Authentication.

Cam Beasley:

• We did talk about certain kiosk users and custodial staff services, and housing and food who may use a shared device, we may make that a trusted device
Q: How will the UTLogin v2 implementation schedule be affected by these changes?
A: We are in the process of assessing the impact this week.

Q: How will these changes affect connections to UT Wifi?
A: Cam – Wifi is not in scope for MFA. AD logon to desktops is also not in scope.

UT System is still determining what rules they want for MFA, but it’s likely that the required uses of MFA will be expanded. We are moving forward with expanding our MFA use now so we can avoid having to make a transition mandated by UT System in a short period of time.

Chris Owan: Outside of the IAM stack, MFA for web-based email is coming, as mandated by UT System. The mandated deadline is Nov 9th, but we expect to have it in place by early October to get it done before Workday Go-Live

Q: What about UTMail?
A: Yes, UTMail is in scope for faculty/staff. UTMail uses Google Authenticator rather than Duo.

Q: Do you have any concerns with Duo being purchased by Cisco?
A: Cam – that same day it was announced we were at a meeting that included Duo and Cisco. The news was still relatively new to them, but they did not expect any immediate major changes to the Duo offering.

5. Project Updates:
   a. UTLogin Stability Roadmap Progress (Marta Lang)
      i. We have received a patch from ForgeRock for several blocker issues we discovered during testing of UTLogin v2. We are currently verifying that the patch has addressed the blocker issues.
      ii. Verification of the Test environment will extend beyond the end of August as was originally planned due to resource constraints and analysis work performed for expanded MFA functions. The team is moving forward with building out the Qual environment, but will not finalize Qual until testing is complete in the Test environment. Significant progress has been made in test automation, which will help accelerate testing in the Qual, Staging, and Production environments.

   b. IAM Workday Readiness Coordination (Marta Lang)
      i. We have completed all Workday End-to-End (E2E) testing for IAM systems.
      ii. Now we are focused on Workday cutover planning, including performing tests to determine how much time it will take to process the initial full file of employee data from Workday, incorporating it into SailPoint and passing the data down to TIM, TED, TOM, WHIPS, and other systems.
      iii. We have also been working on communications about Sup Org data and changes to the merge objection process.

   c. SailPoint IdentityIQ 7.2 Upgrade (Autumn Shields)
      i. The SailPoint upgrade went to production on July 11th. This project is complete.
d. Password Security Improvements (Autumn Shields)
   o The team is working on the changes to EID password rules to allow passphrases. These changes are scheduled to go to Production on September 18th.
   o Test EIDs have been created to allow TED customers who perform direct LDAP authentication to test their systems with a password that is 32 characters long and a password that contains a space. Contact Autumn shields if you would like to test your systems with these EIDs.
   o We will be developing plans for the password change campaign by the end of October. We anticipate kicking off the password change process at the start of the calendar year.

e. Retirement of position-based authorizations in Apollo and OHSC (CW Belcher)
   o Changes to Apollo went into production on schedule.
   o OHSC changes will go into production at the end of September.

6. IAM Roadmap Renewal Update (CW Belcher)
   a. IAM Strategic Roadmap (CW Belcher) – See handout
      o Slide 3 in the handout shows an updated high-level timeline. We will be meeting with the CIO this week to get input and guidance on the roadmap. We anticipate that we will need to gather stakeholder input over the next several months. Our goal is to complete the refreshed roadmap by the end of the calendar year.
      o Slide 4 shows the results of the roadmap objectives prioritization exercise that the Committee completed. The highest priority areas were Protect University Resources and Promote Business Efficiency.
      o The IAM management team has completed an exercise to estimate the value and effort involved with 43 potential IAM initiatives. Slides 7, 8 and 9 show these initiatives plotted to show value vs. effort.
      o Next steps:
         ▪ Meet with the CIO to discuss the roadmap.
         ▪ Identify dependencies and logical sequencing of the initiatives.
         ▪ Gather input on the relative priorities of the “big rocks,” “quick wins,” and other initiatives.
         ▪ Draft the roadmap.

   b. Individual IAM Service Roadmap Reviews (CW Belcher)
      o Roadmaps for all ITS Applications service offerings are currently being updated. You will see these individual operational roadmaps come to the Committee for review via email. If there are significant questions or concerns about any of the roadmaps, we will discuss them in our next meeting.
7. Other Initiatives/Updates
   a. IAM Team Staffing (Mario Leal) – 3 open positions:
      • Project Manager – An offer is in progress
      • Software Engineer – Request to recruit for this vacancy has been submitted to the CIO
      • IT Manager – Request to recruit for this vacancy has been submitted to the CIO
   b. IAM Integrations (Justin Hill)
      • The team completed 6 integrations last month
      • There will probably be a big push in the next month as the semester starts, if you need an integration please get it in as soon as possible.
**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)** - Three blocker issues were identified and escalated with the vendor during the initial verification of the TEST environment. A patched release of the AM product was released on July 30th with fixes to address these blockers. While awaiting the new release, the team made progress on automating test scripts. The next round of verifications in the TEST environment is planned in August. The build of the QUAL environment has continued to progress. Overall, the Planned Finish dates are at risk pending the resolution of the blocker issues and results from testing.

**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.

<table>
<thead>
<tr>
<th>Project</th>
<th>Planned Start</th>
<th>Actual Start</th>
<th>Planned Finish</th>
<th>Actual Finish</th>
<th>Status against Schedule</th>
<th>BUDGET</th>
<th>ACTUAL</th>
<th>ETC</th>
<th>ACT + ETC</th>
<th>VAC</th>
<th>BUDGET - EAC</th>
<th>Status against Budget</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM Project - UTLogin Stability Roadmap</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Complete</td>
<td>2044</td>
<td>774</td>
<td>0</td>
<td>774</td>
<td>1270</td>
<td>Complete</td>
<td></td>
</tr>
<tr>
<td>Simplify and Standardize - Design</td>
<td>6/20/2017</td>
<td>6/19/2017</td>
<td>12/1/2017</td>
<td>1/12/2018</td>
<td>Complete</td>
<td>2587</td>
<td>2535</td>
<td>0</td>
<td>2535</td>
<td>52</td>
<td>Complete</td>
<td></td>
</tr>
<tr>
<td>Simplify and Standardize - Build TEST Environment</td>
<td>9/25/2017</td>
<td>9/25/2017</td>
<td>5/11/2018</td>
<td>5/11/2018</td>
<td>Complete</td>
<td>20.4%</td>
<td>1338</td>
<td>886</td>
<td>827.5</td>
<td>1663.5</td>
<td>-325.5</td>
<td>24.3%</td>
</tr>
<tr>
<td>Simplify and Standardize - Verify TEST Environment</td>
<td>4/9/2018</td>
<td>4/9/2018</td>
<td>8/24/2018</td>
<td>8/21/2018</td>
<td>100.4%</td>
<td>283.75</td>
<td>370.25</td>
<td>5.75</td>
<td>370.25</td>
<td>5.75</td>
<td>1.5%</td>
<td></td>
</tr>
<tr>
<td>Simplify and Standardize - Build QUAL Environment</td>
<td>6/11/2018</td>
<td>6/11/2018</td>
<td>8/24/2018</td>
<td>10/4/2018</td>
<td>55.4%</td>
<td>370</td>
<td>94.5</td>
<td>283.75</td>
<td>370.25</td>
<td>5.75</td>
<td>1.5%</td>
<td></td>
</tr>
</tbody>
</table>
UTLogin Availability
This graph represents UTLogin’s overall availability since April 5, 2018 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. There were no service disruptions for the month of July.

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/.
IAM Roadmap Planning Process

**Objectives**
- What do we want to achieve?

**Initiatives**
- What projects will address the objectives?

**Action Plan**
- What actions do we need to take now, next, later?

Problems & Needs

Aspirational / Strategic

Specific / Tactical
IAM Roadmap Planning Timeline

May:
Brainstorm problems & needs

June:
Review problems & needs

July:
Review objectives & prioritize

August:
Review proposed initiatives; estimate value v. effort

September-November:
Draft & review roadmap

December:
Finalize updated roadmap

Quarterly:
Check progress and adjust roadmap

08/13/2018
Roadmap Objective Prioritization

IAM Committee Objective Weighting

Enhance End User Experience

- Faculty, students, and staff can perform research and easily collaborate with colleagues at UT and other institutions

Enable Research & Collaboration

- Modern and well-supported tools are used to maximize reliability and functionality while minimizing technical debt and maintenance effort

Improve IAM Technical Environment

- Access to resources and information is regularly reviewed and revoked promptly when no longer needed. Rigor of authentication matches the risk associated with access

Protect University Resources

- New and transferring employees are productive quickly, manual processes are minimized, redundant stores of identity data are reduced, cross-system integrations are enabled

Promote Business Efficiency

- All user populations can access the resources and information they need both inside and outside UT

08/13/2018
Initiatives Review

• 43 initiatives identified through input from:
  – IAM Committee
  – IAM team members
  – Original IAM roadmap stakeholder interviews
  – “Federated Identity Mgmt for Research Collaborations” whitepaper
Initiatives Review

• IAM team managers estimated the value of each initiative in advancing the 5 IAM objectives
• Composite value scores were weighted by the IAM Committee objective weighting factors
• IAM team managers estimated the effort required for initiatives (extra-small to extra-large)
IAM Initiatives - Lower Value / Lower Effort Quadrant
IAM Initiatives - Higher Effort Quadrants

- Rationalize Tools/Tech Used for Similar Services (AuthN, Directory Svcs)
- Adopt Standards-Based AuthN and Retire Policy Agents
- Use Cloud to Provide Resiliency for AuthN Services
- Upgrade Critical Systems to Current Support Versions (UFLogin)
- Migrate to AD/Azure for AuthN/AuthZ
- Replace Custom Identity Data Provisioning with SailPoint IQ Connectors
Next Steps

• Review roadmap plans with CIO
• Identify dependencies and logical sequencing of initiatives
• Draft roadmap