TIER Campus Success Program Case Study: University of California, Merced

Executive Summary

UC Merced is participating in the TIER Campus Success Program to accelerate our adoption of a permanent, robust IAM solution that can scale and grow with the organization. Currently in its 13th academic year, UC Merced is maturing from a start-up campus to an established research institution – grappling with significant growth in an environment of constrained resources. Strategic investment in technologies to better manage the identity and lifecycle of our students and employees has become a critical consideration.

After an IAM assessment conducted by Internet2 and Unicon in 2015, UC Merced became a TIER investor campus and developed a multi-year roadmap to migrate from the existing legacy solution to TIER. At the core of this effort is the adoption of the midPoint person registry to replace the current home-grown solution. UC Merced plans to utilize midPoint to fulfill this core need, while also developing the functionality necessary to seamlessly integrate midPoint into our existing IAM environment. UC Merced is working with Unicon to develop API enhancements for midPoint that will allow our community-facing self-service portal to interact with midPoint directly, maintaining the look, feel, and functionality expected by the organization.

Additionally, UC Merced is pursuing a “cloud first” strategy and has used the TIER Campus Success Program to drive that agenda. UC Merced plans to deploy midPoint in the AWS cloud, and is actively developing the code and templates necessary to manage the infrastructure automatically.

Solution summary

Primary Objective: Adopt midPoint to replace our current homegrown identity registry with a TIER-maintained component. Develop necessary methods and logic to import existing user data (student, applicant, and employee) and connect our existing self-service and admin screens to manipulate that data.

Secondary Objective: Develop the skills and experience necessary to deploy TIER solutions in a containerized format consistent with TIER packaging standards, ensuring conformity and supportability moving forward. Starting with midPoint allows us to learn while fulfilling an immediate need, and enables the creation of an environment to eventually support additional TIER products on our roadmap (specifically Grouper). Develop cloud formation templates in AWS to automate the provisioning and maintenance of the infrastructure environment.

TIER Feature Supported

midPoint

Collaborators

- UC Merced
- Unicon ('Misagh Moayyed' <mmoayyed@unicon.net>)

Community resources

TIER workgroups: Banner Identity Provisioning, TIER API and Registry, TIER CSP Slack channel #tier-midpoint

UC Merced chose to partner with Unicon due to their extensive knowledge of both the TIER components and our specific IAM environment. Unicon took the lead on developing the desired midPoint enhancements, including Shibboleth SSO integration and the development of REST endpoints for UC Merced’s account management portal to interface directly with midPoint.

blocked URL

The Environment

UC Merced is the 10th and newest campus in the University of California system. While we are part of a large organization, we are a relatively small campus with less than 10,000 students. Many of our legacy systems were put into place quickly in response to immediate campus demand, without much thought about maintainability. We have two main systems of record: Ellucian Banner for students and applicants and a UC-wide PeopleSoft system for employees. Incoming data from systems of record must be put through a matching algorithm before a new account is created in midPoint. Administrators and departmental designees also have the ability to directly create Affiliate accounts and/or pre-create an employee account directly in the Identity Management system. These accounts also need to be matched with the data from the systems of record.

All of this provisioning and matching logic was originally developed in Waveset XPRESS and migrated to Java in 2016 to facilitate the decommissioning of the original IAM system (Sun Identity Manager). This was always intended as an interim solution, a stop on the road to a permanent IAM architecture comprised of TIER components.

The Problem

Our current identity registry was quickly developed so that we could migrate off an old Sun Waveset-based system. It lacks basic IdM functionality like workflow and auditing and reporting.

Our current business logic was converted from Waveset XPRESS into Java, but is still somewhat of a black box to our end users. UC Merced needs to document this business logic in human readable process flow diagrams and use that to implement in midPoint.

Since being deployed in 2017, the limitations of the current interim solution have become apparent, particularly as our upstream system of record for employees has undergone a complete replacement. Specific issues include, but are by no means limited to:

- Lack of auditing of user access data in existing system
- Lack of workflow engine
- No security standards
- Troublesome and error-prone account matching algorithms
- Limited role-based permissions require most issues to be resolved by IDM developers

The Solution

UC Merced has deployed midPoint to our Dev and Test environments, implementing an SQL connector to import identities from a Banner database for students and applicants and an Oracle database for employee data. We have also configured an LDAP connector to export identity attributes to downstream directories. Unicon has helped us implement SSO with Shibboleth and contributed the code back to Evolveum to include in future releases of the product.

We are currently working with Unicon to develop REST Endpoints in midPoint to allow the use our current self-service IDClaim and password reset pages

We have used this effort to kickstart our desire to deploy new production services in Amazon Web Services and adopt the containerization/devops model championed by TIER. Specifically, we aim to adopt, or come as close as possible to adopting, the AWS Well Architected Framework (https://aws.amazon.com/architecture/well-architected/), where we will automate as much as possible, treating the web, middle, and load balancing tiers of our infrastructure as ephemeral components that can be discarded and re-launched as necessary using simple cloudformation templates, autoscaling groups, and ECS service definitions, with little to no service disruption. We also plan to utilize service offerings whenever possible rather than run our own services (e.g. elastic load balancers, relational database services, etc.), and create self-healing and horizontal scaling solutions wherever possible (e.g. Autoscaling groups and ECS Services). We believe that by following the five pillars of the well architected framework, we will be able to deploy a geographically redundant solution which is trivial to maintain and scales to our demand, hopefully automatically.

The Result

Work continues on all fronts as we build familiarity not only with the product but the packaging environment and deployment to AWS. We have midPoint running in our test environment using the Evolveum Docker image. The environment can be completely built using Docker commands with configuration files in GIT source control. We've setup an SQL import connector from an Oracle database, and an LDAP export connector to Oracle Directory Services. We continue to collaborate with the Banner Identity Provisioning group on specifications for a midPoint connector for Banner. We're looking forward to implementing the TIER identity match program into the midPoint import sync.

AWS infrastructure has been set up and documented in cloud formation templates to deploy a complete midPoint environment to the AWS cloud through code. Unicon has successfully integrated Shibboleth SSO into the midPoint console and work continues on the REST endpoints to connect our self-service page.

As of October 2018, the culmination of these efforts is a solid proof of concept that demonstrates end-to-end functionality and will allow us to continue efforts toward a production implementation. The UC Merced project team has developed a project plan to carry forward our CSP work into next year, hoping to deploy to production in Summer 2019.

Lessons Learned

Jumping in head first, it was difficult to scope the project without having any experience with midPoint. Our long-term strategy of aligning with TIER and other campuses is solid, but our ambitions got ahead of us given all of the other campus initiatives in flight. Some specific challenges UC Merced faced this year:

- SMEs and community support are great, if you have the local resources to engage them. While it seems obvious, nobody can do this project for you. UC Merced got a slow start due to competing priorities for our limited IAM and development resources. The TIER community has been fantastically helpful, but we would have gotten even more out of the program if we had more space to deliberately engage.

- DevOps is a way of life, not a deployment strategy. Understanding and internalizing the complexities of containerization, infrastructure as code, and the deployment methodology of the TIER packaging standard is not for the faint of heart. Getting the right resources and expertise here is a critical foundational component for project success. UC Merced has a fairly classic "sysadmin" IT shop and the road to adopting TIER packaged components in the cloud has not been without its obstacles. This is a critical skill set for a modern IT shop and the successful deployment of TIER.

Resources

IDM TIER Arch diagram: https://www.lucidchart.com/documents/edit/8c9eaaf5-0810-45a3-9d60-68de50000079/

Conclusions

We are very excited to continue partnering with Internet2 and other institutions to develop an identity management ecosystem for higher education. Participating in this program has given us the hands-on training and perspective necessary to be more practical (and ultimately successful) on our slow march toward IAM maturity. Most importantly, it has built a closely-knit cohort of incredibly smart people with invaluable perspective on an intractable problem.

About UC Merced

UC Merced opened Sept. 5, 2005, as the newest campus in the University of California system and the first American research university of the 21st century. Situated near Yosemite National Park, the campus significantly expands access to the UC system for students throughout the state, with a special mission to increase college-going rates among students in the San Joaquin Valley. It also serves as a major base of advanced research, a model of sustainable design and construction, and a stimulus to economic growth and diversification throughout the region.