TIER Campus Success Program Case Study: Colorado School of Mines

Executive Summary:

In early 2017, Mines found itself in need of a new Identity and Access Management (IAM) solution after its current IAM vendor went out of business. Mines IAM staff had been watching the development of the Trust and Identity in Education and Research (TIER) project. We believed that participation in the Campus Success Program (CSP) provided an opportunity to deploy a solution that was designed and built by higher education for higher education, and without the significant cost of a commercial alternative. The CSP also provided the chance to be a part of the collaborative effort developing and supporting that solution.

Mines actively participated in the CSP program, deploying its first containerized environment as part of this effort, and contributing to several different CSP working groups. Although our overall project for full implementation of the TIER solution is still in progress, the CSP program was an indispensable catalyst in initiating the project, providing a collaborative and supportive environment in which to learn as well as to provide input.

Mines benefited significantly from the CSP through its ability to move the IAM replacement project forward with face-to-face meetings with IAM staff at other schools, support from subject matter experts, and training for Docker, Grouper, and midPoint.

Perhaps the most significant problem with Mines current IAM system has been its sustainability - we have a strong interest in seeing that Internet2's efforts in the identity management space continues for many years.

Solution summary:

The scope of the Mines CSP project was to deploy and configure the midPoint and Grouper components of the TIER portfolio, integrating both with Ellucian Banner as the system of record for identity. midPoint will replace the current person registry and provide profile and credential management. Grouper will provide a desperately needed access management function that is not available with Mines' current IAM solution.

The goal was to complete the implementation and integration of midPoint and Grouper within the CSP timeframe of one year. Due to lack of Mines resources, the team was not able to get either of the components into production. We will continue to work on the campus IAM project after the close-out of the formal CSP effort.

TIER Feature Supported:

Mines expects to deploy midPoint, Grouper and Docker. Working with Unicon, the Docker environment is now available.

Collaborators:

- the Mines IAM team
- Keith Hazelton, Warren Curry, the TIER Data Structures and API working groups
- the TIER / CSP community via the TIER Slack channels, Grouper and midPoint mail lists.

The Project

The goal for Mines participation on the CSP was the design and implementation of a new identity and access management architecture based on the Internet2 TIER solution stack. As part of the project, we planned to implement a containerized environment based on Docker. The new architecture must integrate with Ellucian's Banner ERP system as the system of record for identity, and provision accounts to multiple services, both on-premise and cloud-based. Project implementation had support from multiple teams within the Mines information technology department: Identity & Access Management, Infrastructure Solutions, and Enterprise Solutions, with executive support from the Office of the CIO. The ultimate goal is to replace the current vendor-based IAM solution with the open-source, community-supported, sustainable IAM architecture. Peripheral goals were to introduce a containerized environment and approach as part of Mines infrastructure, as well as become an active, contributing member of Internet2's Trust and Identity community in support of the TIER solution stack.

https://spaces.at.internet2.edu/display/TIERCSP/Colorado+School+of+Mines

The Problem

Mines currently relies upon a reasonably robust vendor-based solution for identity and access management that includes a person registry, provisioning of accounts across multiple service platforms, role-based access control, and password management. The solution successfully manages 90% of all automated provisioning across a variety of disparate systems. Users are able to utilize a self-service portal to claim an account and manage password changes. Unfortunately – and perhaps most critical - the vendor that provided our current IAM solution has gone out of business and we need to migrate to a new IAM solution.

There are several functional shortcomings in the existing solution. First, all deprovisioning of accounts is done manually. Additionally, account provisioning is based on high-level Banner institutional roles and does not have the granularity required to manage access to resources at the level required. Such requirements include:

- lab and classroom access for students based on major and/or course enrollment
- access to software and services based on institutional affiliation
- membership in various groups and mail lists based on job title, job function, major or department

- various levels of access to Banner and associated applications based on job title and function.

Specifically, Mines would like to move from a role-based access control model to attribute-based access control. Lastly, all sponsored user accounts such as those for visiting faculty, visiting students, vendors and contract employees are manually processed.

midPoint and Grouper are an ideal solution to the above problems. Unfortunately, Mines has not had sufficient staff time to deploy both midPoint and Grouper in the time allotted between TechEx 2017 and TechEx 2018. We will continue to work on the deployment after the CSP has concluded.

The Solution

The currently active IAM project roadmap includes initiatives to address these identified shortcomings, including automated de-provisioning within the system and implementation of Grouper to address institutional requirements surrounding access management. We chose the following to address the identified issues:

- Docker
- midPoint
- Grouper

The Result

Mines made significant progress on understanding the TIER components, the role they will play in a future implementation, and beginning actual implementation of the designed solution. This was not as much progress as initially hoped for and articulated in the project plan, but other benefits were realized that have long-term impact. Mines is in a good position to realize its overall project goals, but on a revised timeline.

The primary factor in project schedule delays was staff resource time. With a single individual serving as architect and implementer who also had other time commitments related to the existing identity system, the project was often starved for technical resources.

Mines did make tangible progress. With the assistance of professional services from Unicon, we implemented a containerized environment with Docker, installed a test platform for midPoint, and made progress in creating a test platform for Grouper.

Mines IAM staff learned a great deal about best practices for self-service applications, integration with systems of record and DevOps.

Further, we feel we have become an active collaborator within the Banner integration and the API & Data Structures design / development conversations. Being an active participant in TIER working groups has contributed greatly to our understanding of how to best utilize various attributes in a system of record for IAM.

Additionally, Mines is contributing to the conversation around long-term support models to ensure the sustainability of the Internet2 TIER initiative and continued growth in community adoption of the solution.

Lessons Learned

Although we acknowledged and articulated that the biggest risk was the limited number of personnel resources knowledgeable about and committed to IAM, we were unable to mitigate this risk successfully. Hence, the scope of our initial project plan was too large and our overall timeline too aggressive.

Given current knowledge, if we were to start the project again we would undoubtedly scope the CSP portion of the IAM replacement project more reasonably. The overall project goals would certainly remain the same.

Resources

- Original IAM components and architecture
- Planned IAM components and architecture based on TIER open-source components

Conclusions

The Campus Success Program was viewed as an important opportunity for Mines to realize its vision of a new identity and access management system. We were hopeful that the community of resources and peer institutions would provide some measure of support, supplementing on-campus resources and helping to realize the success of a project that would otherwise be difficult to achieve. From this perspective, the Mines project and the CSP program were very successful.

The technical work that was completed, the knowledge gained, and the introduction and subsequent active participation in the Trust and Identity community space should all be viewed as positive outcomes of the Campus Success Program for Mines.

About Colorado School of Mines

Colorado School of Mines is a public research university in Golden, CO, with academic programs and research portfolio devoted to engineering and applied science. It has the highest admissions standards of any public university in Colorado and among the highest of any public university in the U.S. Mines has distinguished itself by developing a curriculum and research program geared towards responsible stewardship of the earth and its resources.

In addition to strong education and research programs in traditional fields of science and engineering, Mines is one of a very few institutions in the world having broad expertise in resource exploration, extraction, production and utilization. As such, Mines occupies a unique position among the world's institutions of higher education. The world faces a crisis in balancing resource availability with environmental protection and Mines and its programs are central to the solution.

Mines offers all the advantages of a world-class research institution with a size that allows for personal attention. Enrollment in Fall of 2017 was 6,043 which is comprised of 79% undergraduate and 21% graduate students. Computing, Communications, and Information Technologies (CCIT) offers centralized support for technology strategy and all institution-wide technology initiatives, projects, and services at Mines. This centralized approach works extremely well, particularly given Mines size (student, faculty, and staff population). Among other benefits, it affords an opportunity for standardization around approaches to technology and technology platforms - including identity management, access management, and the integration of disparate systems.