Case Study - York University

The Problem

York University's legacy Identity and Access Management solution (Passport York) has reached its limit in terms of group provisioning (e.g. automatic provisioning access to Azure AD resources). More and more, Passport York relies on ad-hoc scripts and manual interventions to try to keep up. This results in reduced productivity, given the manual work required by the various IT departments of the university to fulfill access management needs.

The Solution

The project team decided to join the 2020 Campus Success Program and deploy Grouper, an open-source access management solution that can provide automatic group provisioning, based on attribute, role, or membership of a person. The team set the scope of the project as:

- Deploying the InCommon Trusted Access Platform containerized Grouper into production
- Importing necessary attributes and memberships from the student information system and Passport York.
- Provisioning groups and access into AD and Azure AD
- Developing a framework for future reuse

The Result

The main goal of participating in the CSP was to understand the mindset of open source and what is involved in installing and configuring the software. This goal was met. The team completed a proof of concept for Grouper for access management, but decided more resources and planning would be necessary to move to production.

The proof of concept for Grouper was completed and the team gained an understanding of the value of using a third party to help with the implementation. Competing priorities prevented a developer from being assigned to the project, which prevented going further in the deployment process; so it was not moved to production.

One of the project team's main use cases was using Grouper to provision mail-enabled groups in Microsoft Office365. Even though we were successful to provision to Microsoft Office365 groups with the help of a couple of members of the community, we encountered an issue with the provisioning of mail-enabled groups that we were unable to resolve without developing our own Grouper connector to Microsoft Office365. The project team also gained a thorough understanding of what was involved in implementing another InCommon Trusted Access Platform component to production, which will inform the eventual replacement of the legacy IAM system.

Lessons Learned

Key Takeways

- Learning how the community works
- Access management knowledge including Midpoint, Shibboleth, and Grouper
- Access to the subject-matter experts
- Current system was prone to decentralization, move to centralization
- There is not much in the open source world for Privileged Access Management (PAM)

There was an RFP/RFI occurring simultaneously to investigate other options in addition to the Trusted Access Platform, and the main goal of CSP was to understand the mindset of open source and what's involved. It was clear that one needs to staff internally to support open source.

The CSP experience was positive and we became aware of just how big the community is, and how much time a lot of the experts put into the projects to ensure that the features they want are built. While there is no monetary cost for open source software, one does have to give time and effort to co-create and shape the software.

Lessons Learned

- Plan for and get started on Docker earlier; it took longer than expected to get that going
- Scope can change as you learn new things
- Keep the scope small; it is more than you think it will be
- CSP is really helpful in getting the ball rolling, then it's up to universities to keep it going
- Putting it into production means supportability, and team needs to be in place to support it
- Identity governance in higher education is very challenging
- When looking to replace a new system, plan for how to decommission the old, the transition from old to new takes additional time and planning

About York University

York University is a public research university in Toronto, Ontario, Canada. It is Canada's third-largest university with approximately 55,700 students and 7,000 faculty and staff.

Project Team: Pascal Cantin (York), Chris Russel (York), Chris Hyzer (UPenn), Chad Redmond (UNC), Bill Thompson (Lafayette College), Chris Hubing (Internet2), Erin Murtha (Internet2), Lacey Vickery (UNC-Charlotte)