Case Study - University of North Carolina Chapel Hill

The Problem

The University of North Carolina at Chapel Hill saw the need for an improved and extensible provisioning system to control access to a variety of resources. Specifically, the identity team was looking for faster and easier integration of new resources. In addition, campus stakeholders have repeatedly sought a solution to centralized provisioning and deprovisioning, enabling them to add and remove local accounts. Such a solution would eliminate the need for manual requests and the related delays.

As a large research university with a hospital, it would be paramount to understand the security requirements and ensure the new solution would meet those requirements. The project would also require effective collaboration with campus stakeholders.

The Solution

Given the time frame for the CSP, the identity team chose to scope the solution to implementing midPoint as a provisioning engine to help provide and control access to Google suite applications and Google Cloud Platform (GCP). During the CSP, the provisioning capability will be limited to central IT evaluation and use.

midPoint was chosen because of its wide adoption in the Collaboration Success Program (CSP) cohort, and because it is easily extensible via open source connectors. In addition, support for midPoint is available from CSP subject-matter experts, Evolveum (the vendor), consulting agencies, and peers. midPoint will be used in conjunction with Grouper to manage access to the Google applications and GCP.

The team also planned to gain an understanding of the capabilities of COmanage for possible use for some guest management purposes.

The Result

The project team successfully installed and configured midPoint as a provisioning engine, running in its standard operations matrix for enterprise applications. They met all but one of the goals developed at the outset of the CSP:

- Instantiate a production instance of the provisioning engine, managed by the identity management group, and running in the standard operations matrix for enterprise applications.
- Publish groups in the production G Suite tenant based on authorized groups in Grouper, and via midPoint.
- Associate GCP permissions with the G Suite groups above.
- Gain understanding of COmanage capabilities and overlap with other InCommon Trusted Access Platform components.

The one goal that was not met was the development of a recommendation document for the CIO on using COmanage for some guest management and invitation flows.

The team also spent considerable time thinking about internal collaborations and how the COVID-19 pandemic changed the way they did their work. In-person collaborative troubleshooting did not translate well to remote work and Zoom meetings, where it is easier to multitask and lose focus.

Overall, the project team felt the scope was about right, given competing demands on time.

Lessons Learned

- The project team thought a lot about internal collaborations; specifically the impact of COVID-19 and the lack of in-person brainstorming and troubleshooting sessions.
- The narrow scope of the project was about right, given the time and resources available.
- It was extremely helpful to have a team member with 10 years of experience at UNC and a knowledge of internal hierarchies, and who is also heavily involved with the development of the InCommon Trusted Access Platform.

About the University of North Carolina at Chapel Hill

The University of North Carolina at Chapel Hill is a public research university in Chapel Hill, North Carolina. The flagship of the University of North Carolina system, it also operates a large health sciences program and medical center.

Project Team: Ethan Kromhout (UNC Chapel Hill), Jan Tax (UNC Chapel Hill), Shumin Li (UNC Chapel Hill), Chad Redman (UNC Chapel Hill), Celeste Copeland (UNC Chapel Hill), Paul Caskey (Internet2), Keith Hazelton (Internet2), enhanced access to Evolveum was critical