Evolveum

CASE STUDY | HIGHER EDUCATION

Deploying a flexible IdM system on top of the legacy one

The University of North Carolina Chapel Hill runs the new identity management system in parallel with the legacy one

Overview

Challenge: UNC needed to fully automate their identity management and integrate new services. This could only be achieved with a new IdM platform that would not affect their in-house system, but would work alongside it.

Process: UNC was looking for a solution that would adapt to them rather than vice versa, and midPoint was a perfect match. They joined the Collaboration Success Program to leverage the assistance of the InCommon community.

Outcome: The university managed to put midPoint, an open source identity management and governance platform, in production in 4 months to administrate 75,000 active identities.

Future: UNC plans to continue expanding their possibilities with midPoint and leverage more of its rich feature set while continually replacing the legacy system.

About The University of North Carolina Chapel Hill

The University of North Carolina Chapel Hill (UNC) is a public research university that is a part of the North Carolina University System. It was the first university in the United States to award degrees in the 18th century, and it is classified among R1: Doctoral Universities - Very high research activity. The university offers a variety of undergraduate, graduate, and doctorate programs within health professions, business, journalism, and more.

Overall, the university administrates 75,000 active identities (e.g., students, faculty) and 350,000 alumni across UNC and UNC Medical Center, which is associated with the university. The IAM team handles large quantities of patient data as well, therefore it needs to pay a considerable amount of attention to privacy concerns.

The Objective

UNC was using in-house built Java applications as their identity management system. Even though this solution was great for managing their core systems like AD, LDAP, and Kerberos, it was extremely complicated, almost impossible, to integrate new systems. Hence, they needed an adaptable solution that would give them the flexibility to meet their requirements, one of which was the integration of new services, in addition to preparing them for future challenges in the IdM field.

They wanted to avoid a monolithic package where the business at the university would have to change to match that package's capabilities, so they instead chose a piece of software that would adapt to them.

The Challenge

The in-house system was built on SPML, and due to the complexities that SPML had associated with it and the in-house codebase, it was almost impossible to extend the provisioning footprint. This resulted in the inability to onboard a single provisioning target, except the ones that already existed when the system was created.

The first challenge was to integrate modern cloud services like Google Workspace and Microsoft Azure and fully automate the process of managing identities for them. Ideally, this new integration wouldn't affect the existing in-house IdM and its integrations, but would work alongside it.

The Process

The internal IAM team is made up of six members, each with a focus on a different aspect of IT experience (e.g., Java developers, TAP, Azure, AD).

The university wanted to stay away from having a single vendor with too much influence over important aspects of the university's business, such as identity management. They preferred to avoid a situation when the business at the university would have to change to match a certain solution's capabilities. That led to them choosing midPoint, as it provided the university with a feature-rich identity management platform with a flexible provisioning engine that would adapt to them.

The university decided to join **the Collaboration Success Program (CSP)** that's organized by InCommon, a community of higher education, research, government entities, and cultural organizations in the USA. Because of the set timeline of the program, the university was able to follow the process, avoid delays caused by their relatively high number of administrated identities and internal security reviews, and move swiftly within the project's timeframe.

Early in the process, the university decided to initially use midPoint only for the integration of new systems. They understood that migrating systems from the current IdM wouldn't bring immediate value. Therefore, they did not try to roll out the new product and replace the entire identity system at once, but rather to take these steps in sequence.

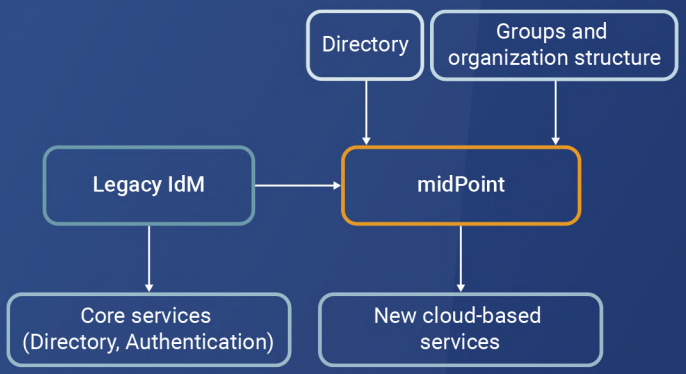
> **"But when it came to something as core as identity management, the university wanted to avoid going into some monolithic package where the business at the university would have to change to match that package's capabilities rather than having something more flexible like midPoint that would adapt to us."**
>
> **Ethan Kromhout**
> Director of Applications Infrastructure at UNC

The process included the following highlights:

- The primary function of midPoint was to gather identities from multiple sources and enable their management in a unified way.
- MidPoint was configured to not only take users, but also groups from source systems and streamline their management and provisioning to target systems.
- The connector framework was used to set up

provisioning to two target systems (Google Workspace, Microsoft Azure).

- MidPoint pulls information from the homegrown identity system via the SCIM connector, which guarantees compatibility with the existing IdM and all its integrations.
- The initial design of IdM objects and relations was strongly inspired by demo architecture provided by Evolveum for the InCommon community.
- In addition, UNC uses a couple of custom archetypes. For example, the ones associated with their provisioning targets tailored for Google and Azure. In addition, the university created a UNC person archetype. This gives them the opportunity to have an established baseline they can easily expand on when they bring in other types of identities, for example, external users.
- The IdM team is quite happy with midPoint's performance, including the integration with external systems. For example, a full reconciliation of the source LDAP directory containing 600,000-700,000 accounts takes approximately one hour.
- The entire process is fully automated, and the IT team does not have to do any manual changes apart from shifting the data from one system to another.



The MidPoint Community

Evolveum provides midPoint users with numerous resources that are available publicly to everyone.

UNC appreciated the genuine approach to being open source and transparency Evolveum has shown. Apart from midPoint's publicly available source code without any proprietary parts, everything else has open access as well. This includes the Jira product bug tracking system, technical documentation, and design documents.

During the midPoint evaluation and deployment phases, docs.evolveum.com proved to be extremely helpful for UNC. In addition, having an Evolveum representative participating in various InCommon community meetings was greatly appreciated as well. That includes the **InCommon midPoint working group**, which is a great place to share experience with other universities.

UNC has gathered information from examples as well, such as demo environments that showed different ways to initialize at container infrastructure, including Kubernetes.

> "Evolveum's attitude on open source and the transparency that comes with that has been extremely helpful. A lot of companies claim to be open source, either they have a freemium model, or the source code has proprietary parts. The genuine open source and transparency that Evolveum has shown us has been huge."
>
> **Ethan Kromhout**
> Director of Applications Infrastructure at UNC

Thanks to having Java developers on the IdM team, UNC has been able to develop new connectors with ease. Therefore, they are ready to swiftly integrate any systems or extend the integration capabilities of the existing connectors.

UNC has developed a couple of connectors that they have contributed back to the midPoint community. The availability of the connectors suite with open code and the flexibility of configuring the system to match the university's needs and not vice versa has been very important in bringing the system into production.

The Outcome

MidPoint was deployed and put into production within four months from start to finish.

UNC can now fully enjoy having all the necessary identities in a single place and provision them to target services in the cloud. It especially came in handy for provisioning to Google Cloud, as more people were starting to use the Google Cloud Platform (GCP) and Google Workspace. In addition, having integrated Azure makes populating the groups possible there directly from midPoint without the need for manual labor.

Having this baseline deployment of midPoint allows UNC to flexibly react to any new requirements on IdM that are raised in the future.

The Future Plans

UNC would like to continue replacing the legacy system. They are planning on using midScale to bring in a larger user population when the timing is right.

Moreover, they want to start connecting additional systems, which will most likely include the development of new connectors.

UNC wants to start expiring authentication tokens, for example, the tickets issued by the Kerberos server. Therefore, they need to implement a user life-cycle that will trigger deprovisioning, leading to the expiration or invalidation of relevant authentication tokens.

The university is currently considering a bigger project, which would involve the creation of a central mail registry. Currently the email addresses are managed in several systems (e.g., PeopleSoft, Office365, Google Workspace). The goal is to gather all the email addresses in a central registry that can make decisions about what email address should get published and used by the university as a user's primary email address.

The university is entertaining the idea of using midPoint to carry out security reviews. MidPoint can give them complete visibility of all the accounts across their whole infrastructure including the life-cycle status and expiration dates as well as detailed audit logs.

In addition, UNC would like to focus on the midPoint notification feature. This would allow UNC to automatically notify leaving students in a timely manner that their account will expire. The same information would be delivered to relevant departments as structured reports.

For the future, UNC would also like to track what piece of data came from where. Such information would be interesting to both business analysts and IT security staff. The data provenance feature developed under the midPrivacy initiative would be useful there.

> "In midPoint there are clearly things like keeping track of what piece of data came from where. I think it will be interesting both to our business analysts and our IT security staff."
>
> **Ethan Kromhout**
> Director of Applications Infrastructure at UNC

Evolveum is a globally recognized EU-based organization that was established in 2011. With its dedicated team of professionals, Evolveum is the creator and maintainer of the leading open source identity platform midPoint. MidPoint's feature and connector set, in addition to Evolveum's openness, values, and lively community, confirm that Evolveum has always had a strong connection to higher education. That's why Evolveum is proud to be one of the inaugural Catalysts in **InCommon Catalyst Program**, which has a goal of supporting higher education institutions, research organizations, and sponsored partners.

Evolveum academia@evolveum.com