TIER Campus Success Program Case Study: Lafayette College

Executive Summary

Lafayette College is a TIER investor campus and the three major TIER components (Shibboleth Identity Provider (IdP), Grouper, and COmanage) are central to its identity management program. Striving for consistency among its identity and access management (IAM) processes and deployment architecture made Lafayette interested in the TIER packages as a path to upgrade component software versions.

The project to integrate local customizations, including support for CAS and the REFEDS MFA Profile (an international SAML profile for multifactor authentication), and deploy the Shibboleth IdP package was successful. Lafayette gained operational benefits from being on a modern platform, and Docker further reduced the deployment environment maintenance burden. With Docker part of the computing infrastructure and experience gained from deploying the IdP container, Lafayette will use the TIER packages to upgrade the other components. Unicon was the consulting partner for the IdP project.

Lafayette's identity management system, while mature, was custom-engineered and had operational gaps. An evaluation of midPoint as a potential replacement revealed a need for customization. Instead, Lafayette focused on midPoint's central capabilities of provisioning and synchronization.

A community of practice grew around the TIER Campus Success Program and was one of the most valuable outcomes for the participating institutions.

Solution Summary

Lafayette's existing IdP implementation included the shib-cas-authenticator to refer authentication to CAS. Unicon modified the Shib-CAS plugin to add support for MFA signaling, then made it available to the Docker image. The Docker image, built locally on each node, contained local configuration files, including the plugin .jar file. An orchestration platform wasn't necessary because of the small deployment. Internet2 Subject Matter Expert (SME), Paul Caskey, helped identify the cause of a Java heap space problem that migrated to the new deployment. The new nodes were initially slow to respond due to the Docker service pointing to Google DNS rather than Lafayette. A DUO MFA roll-out shortly before the IdP deployment revealed a misconfiguration in the Shib-CAS plugin for REFEDS MFA Profile support that prevented certain users from accessing web single sign-on. Working with a consulting partner and the responsiveness of SMEs were instrumental to success. The project contributed optional capabilities and configuration fixes back to the TIER packaging.

Training by Evolveum (midPoint developer) provided familiarity with operating midPoint, but Lafayette had unexpected challenges configuring connectors during installation. Connecting an LDAP resource required the RootDSE be exposed. Resource creation wizards generated broken XML schema files and OpenLDAP and Active Directory couldn't provision DNs. Modified example files allowed disabling an account in midPoint to be administratively locked in LDAP and AD. Reconciliation to resolve inconsistencies also occurred. Because of a shorter than planned timeline, Lafayette considered integrating midPoint between the Accounts Workflow's back-end database and LDAP rather than a replacement for the entire system. Timing factors prevented this. The Banner Identity Provisioning Working Group members, Data Structures/APIs SME, and Campus Success Program (CSP) institutions evaluating or integrating midPoint formed a nascent repository of knowledge within TIER for midPoint.

TIER Feature Supported

Shibboleth Identity Provider (IdP)

midPoint

Collaborators

- Lafayette College: Janemarie Duh, Identity Management Architect; Bill Thompson, Director Digital Infrastructure; Carl Waldbieser, Systems Programmer
- Consulting Partners: Charise Arrowood and Misagh Moayyed (Unicon)
- Campus Success Program SMEs (Subject-Matter Experts): Matt Brookover (Colorado School of Mines); Andy Morgan (Oregon State University)
- Internet2: Paul Caskey and Chris Hubing

Community resources

The Internet2 TIER Slack channels facilitated collaboration among Lafayette, Internet2 staff, and SMEs. Internet2 also created a designated Slack channel for Lafayette and Internet2 SME to use in solving a problem that migrated from our previous VM-based IdP deployment. Lafayette used the Internet2 TIER Slack channels heavily to engage with SMEs for help in overcoming roadblocks with integrating midPoint with our enterprise directories (OpenLDAP and Active Directory). The Banner Identity Provisioning Working Group launched within the CSP gave Lafayette the opportunity to establish working relationships with colleagues at institutions that also use Banner, an enterprise resource planning (ERP) system for higher education.

Supporting media

Lafayette student EXCEL Scholar: https://tiny.cc/lafayette_research

Students with Marquis de Lafayette statue: https://tinyurl.com/marquidelafayette

The Environment

Lafayette College is an independent liberal arts college in Pennsylvania. It offers undergraduate programs in the arts and sciences, as well as engineering, is a full member of the Patriot League, and competes in NCAA Division I sports. Supporting academics, undergraduate research, and student life in a competitive environment requires a mature Identity Management System (IdMS). Lafayette understood the value of the InCommon Federation early, joining in 2007 and registering a Shibboleth IdP run locally. Integrating Grouper and COmanage for access policy governance and digital identity creation and lifecycle management for sponsored accounts added the other two major pieces of the TIER toolset making them key components of the IAM architecture. Due to its commitment to InCommon and Internet2, Lafayette became an investor campus for the TIER Initiative.

The Problem

The Accounts Workflow is a custom identity registry for Lafayette faculty and staff. It consists of a set of web forms, a database, and Perl scripts that create a digital identity in OpenLDAP. The system creates an email account in on-prem Zimbra, writes the email address back to Banner, and adds maillist subscriptions. Prior to entering personal information on new hires into the web forms, staff in Human Resources and Office of the Provost enter much of the same information into Banner. A record must be entered into Banner in order to generate an identifier (SPRIDEN_ID) that the New Hire Request requires. Duplicate data entry is unpopular and manually entering data into the Accounts Workflow form makes it prone to errors.

An early adopter of Shibboleth, Lafayette ran Shibboleth IdPv3 locally, installed from a tarball on a VM. In general, the IdP was stable, requiring little maintenance. The architecture was recently changed to a multi-node deployment to improve redundancy. Because of our investment in the mission of TIER, we were interested in the Shibboleth IdP containerized package and its features. The package offered ease of deployment to new nodes and default presets for configuring an IdP the “InCommon way.” But we didn’t yet have experience with containerization or support for the Docker platform as part of our computing infrastructure. Another cause for concern was how our requirement for inclusion of the Shib-CAS authenticator would be met. That plugin was necessary due to configuration of the IdP for external referral of authentication to CAS. We also wanted to add support for the REFEDS MFA Profile so we could log into the InCommon Certificate Service Manager using federated identity.

The Solution

TIER Shibboleth IdP Package

The project kicked off with a discovery phase to gain a sense of strategy for implementation. We partnered with Unicon for the project and they guided us in a number of decisions. Local configuration files can be burned in or external to the image used to build the Docker container. Misagh Moayyed (Unicon) recommended burning in our configuration files. Because of our small deployment, an orchestration platform wasn’t necessary. We could just build the Docker image on each node and take advantage of caching.

Internet2’s Shibboleth SME Paul Caskey and Misagh worked out how to incorporate our local requirements to make them available as native options in the TIER package. Misagh first incorporated MFA signaling into the Shib-CAS plugin. To deploy, we built the .jar locally for the plugin and included it in the auxiliary files for the Docker build. The TIER Shibboleth IdP Package and Lafayette College Customizations provides details.

On July 11, Lafayette cut over from its proxied VM-based IdPs to proxied containerized IdP nodes. Everything is unified in the Docker image. We pull the TIER version into our local GitHub repository and merge any changes. The deployment process takes the base dockerfile, which acts like a recipe, and adds the local configuration files. The image is built on the Docker hosts by consuming the dockerfile.

Once in production, a number of problems surfaced. A chronic Java heap space error that affected our original deployment migrated to the Dockerized instance. With Paul Caskey’s help, we discovered Docker wasn’t interpreting the JAVA_OPTS syntax correctly and were finally able to resolve this disconcerting problem.

The new nodes seemed sluggish in their responses. Investigation revealed the Docker service pointed to Google’s DNS service rather than Lafayette’s and the firewall was blocking it. Passing in local settings for Lafayette’s DNS restored normal response times.

Later that week, we realized had not included the REFEDS MFA profile support in the Shib-CAS authenticator. The primary use case for it was to use federated identities to log into the InCommon Certificate Manager. After adding the plugin and modifying users in the platform, we no longer needed separate credentials to access it.

Over the weekend, we received reports that some users could not access several important services. Two days before deploying the IdP package, we rolled out Duo MFA to campus and the affected users were members of cohorts excluded from the MFA requirement. The MFA profile support in the Shib-CAS plugin was the likely suspect. The plugin lacked a condition to require MFA based on asserting authentication context class. Misagh modified the plugin to check whether an SP asserts REFEDS MFA. If it doesn’t, the plugin falls back to password-protected transport. After deploying the modified shib-cas-authenticator, we had a stable Docker-based TIER IdP package in production with local customizations – a major lift and accomplishment.

midPoint

Once the IdP was stable, we refocused on midPoint. The project scope was to evaluate it as a replacement for the Accounts Workflow and evaluate its capabilities for institutional identity lifecycle management like digital identity creation and NetID namespace management. Our architectural design showed midPoint getting identity data from source systems (Banner and COmanage), provisioning to LDAP and AD, with Grouper getting reference data from Banner and subjects from LDAP.

Getting started was more difficult than expected. The training TIER offered early in the year with Evolveum was valuable for gaining familiarity with its operation rather than installation. Connecting midPoint to directory databases wasn’t easy and we hadn’t engaged with a consulting partner for the evaluation. We installed and configured midPoint in the spring, but had trouble getting an LDAP resource working. The OpenLDAP root directory server entry (RootDSE) needed to be exposed in order for midPoint to connect. We succeeded in connecting OpenLDAP and Active Directory, but midPoint could n’t provision DNs.

Adding a resource, a configuration for connecting to systems, is perhaps the most important part of implementing midPoint. An XML schema file tells midPoint what the resource should look like. The wizards for resource creation generated broken configuration files. We copied examples from Evolveum's documentation, removed lines, and added schema handling to match the fields we needed. Valid schema files allowed a disabled account in midPoint to be administratively disabled in OpenLDAP and Active Directory. Reconciliation was in place with midPoint updating DNs based on Banner SPRIDEN_ID.

Lafayette participated in the Banner Identity Provisioning Group and, along with other members, identified required data fields for the midPoint data schema. We planned to debug a query from our enterprise data team to pull Banner data into midPoint, but it was already August. Projects needed to wrap up so Campus Success Program participants could prepare to present their work at the Internet2 Technology Exchange.

Rather than replacing the Accounts Workflow in its entirety, we considered integrating midPoint between the back-end database and OpenLDAP. Doing so would allow us to gain familiarity with the component and time to consider how we might make use of it more broadly. We sketched out the architecture and planned to scope phase one of a production deployment. It was late August by then and the semester was starting in less than a week. We concluded that even the smallest deployment of midPoint would be a worthy endeavor. A narrower scope for the future might envision using midPoint for password syncing to OpenLDAP and Active Directory.

The Result

TIER Shibboleth IdP package

One year after hosting the Shibboleth training where an option to use Docker was available for the first time, Lafayette is running its production IdP in a Docker container built from the TIER packaging. Because of our local customizations and lack of familiarity with Docker, engaging with Unicon was critical to the success of the project.

The biggest operational impact the TIER packaging has on Lafayette is the surrounding execution environment no longer is a concern. Prior to the TIER IdP, we needed to consider JVM and Tomcat versions. The compute platform the IdP runs on no longer matters. The containerized IdP simplifies things and we expect upgrades to cause less anxiety. Everything is handled now by TIER. Lafayette only has to worry about one version. We just run the Docker image. Everything the Shibboleth IdP needs is in one tidy package.

We deployed the package using existing infrastructure. Deployment architecture changed from two hosts, one active and one passive, behind an NGINX proxy that pointed to one active node to three active nodes behind NGINX+, which acts as a reverse proxy. The nodes are stateful and use IP hashing.

It is important to consider the operational benefits that being on a modern platform provides. Docker further reduced our deployment environment maintenance burden because of its native support for Splunk logging. Before TIER, we had to configure a forwarder on each host to send logs to Splunk.

Docker has a health checks capability that can be specified in the base dockerfile or overridden on the command line. The Docker container checks against the IdP status URL and, if a node goes down, Splunk notifies us.

The IdP project gave us the opportunity to incorporate support for REFEDS MFA via CAS for federated services in the shib-cas-authenticator and make the plugin available as an option in the TIER packaging. Finally, with TIER's help, we solved the long-standing Java memory allocation problem that affected both old and new IdP deployments.

midPoint

Going into the evaluation, we had expectations that we would use midPoint to replace the Accounts Workflow. Integrating the IdP package took longer than expected and left us with half as much time as planned for midPoint. We soon found that it couldn't do what we hoped it could without customization.

MidPoint is strongly geared towards account provisioning out of the box. So, instead, we focused on evaluating its provisioning and synchronization capabilities by connecting it to OpenLDAP and Active Directory. Leaving the Accounts Workflow in place, we used the staging environment database as a source for users and pulled user data attributes and request status and had midPoint do the provisioning.

MidPoint is flexible, but it wasn't the solution for closing Lafayette's operational gap. The evaluation revealed midPoint needs something like the Accounts Workflow database in front of it to make it aware of subjects. It could prove to be a partial replacement in the future, but a clear path forward wasn't evident in the time we had for the Campus Success Program.

Lessons Learned

We found our approach to the project to generally be reasonable. In hindsight, more frequent blog posts would have made putting together the case study easier. Keeping a running document of the bi-weekly updates we provided to the Campus Success cohort also would have facilitated it by having content already collected and available for use.

Resources

- Lafayette College Campus Workspace
- Lafayette College and the TIER toolset
- Lafayette IdP customizations and packaging
- Shib-cas-authn3 Gitlab repo
- Evolveum midPoint documentation
- Banner Identity Provisioning Working Group

Conclusions

One of the most valuable outcomes of the TIER Campus Success Program was the underlying community of practice that developed during the course of the year. TIER SMEs and Unicon helped us overcome challenges we faced. Because of these opportunities for collaboration, Lafayette College was able, in turn, to make contributions in the form of optional capabilities and configuration fixes that were added back to the Shibboleth IdP packaging.

We served as Grouper SMEs although we had not committed to deploying the Grouper package during the project. Sharing how we use the component based on the Grouper Deployment Guide and engaging with deployers within the CSP through the Grouper Deployment Enhancement Working Group helped solidify the thinking about our own implementation.

The vision of TIER is future-leaning. We look forward to the Grouper and COmanage packages based on our experience with the Shibboleth IdP package. With Docker now part of our computing infrastructure and TIER packaging no longer unfamiliar, integrating the other TIER packaged components will be that much easier. When it comes time to upgrade our Grouper and COmanage deployments, we'll do them using the TIER packages.