CAMPUS TECHNOLOGY

Trends in IT Practices | Feature

Small University Pushes ID Management to the Cloud

- By Linda L. Briggs
- 09/30/10

Moving a university's mission-critical ID management solution to the cloud requires something of a leap of faith. For Coppin State University, the leap also required a hands-on, several-months-long proof of concept with a trusted vendor to convince the small university that the solution would work.

It helped that Coppin State has been successfully using the identity management solution, from Fischer International Identity, since 2005 as an on-premise solution. The historically black university based in Baltimore, with more than 4,000 undergraduate and graduate students and another 2,000 or so faculty and staff, has frequently pushed the technology envelope with its solutions. It was awarded a Campus Technology Innovator award in 2005, for example, and has repeatedly been recognized by Computerworld magazine for its use of technology.

Still, according to the university's CIO and vice president of IT, Ahmed El-Haggan, when it came to going to the cloud with a sophisticated identity management system that was used for setting up and managing user IDs across the university's entire network, at least part of his IT staff wasn't convinced.

"Cloud-enabling the security architecture within the university is a huge decision," El-Haggan admitted. Recognizing that, the network management portion of the staff initially questioned the move. The information systems staff, in contrast, generally supported the idea.

Eventually, a full-blown proof of concept--during which every aspect of running the system in the cloud was created and tested--brought everyone in IT around to supporting the decision. Administrators, on the other hand, were generally supportive of the proposal from the start, El-Haggan said, reflecting a general atmosphere of trust in the university's IT department--and Coppin State's solid ongoing relationship with Fischer.

The ID management system is used to manage the identification and passwords of individuals using any aspect of Coppin State's network. Called the Fischer Identity Suite, it handles administrative, maintenance and support tasks around the management of user identities and other security issues. The cloud-based software is exactly the same as the software used on-site by customers, according to Andrew Sroka, Fischer president and CEO, helping make the move to the cloud seamless--and enabling Coppin State to easily move back to an on-site model if it changes its mind.

ID provisioning is also a key part of how Coppin State uses Fischer. Provisioning describes the process of setting up new users to make sure all user passwords are the same for every application the user might access across the network, including Oracle PeopleSoft, which is Coppin State's ERP solution, along with Blackboard, Tegrity, and Microsoft Exchange and SQL Server. For example, when Human Resources adds a new user, the Fischer software makes sure accounts with appropriate access are created in each software package, allowing single sign-on access. When PeopleSoft is updated, El-Haggan said, he expects a much more streamlined process. Blackboard is the only exception to single sign-on and requires a separate login, but users are assigned the same password as in the single sign-on system, El-Haggan said.

Except for its emergency call management system, which Coppin State outsources to a hosting company, this was the university's first experience with a Software-as-a-Service (SaaS) solution.

During the proof-of-concept testing, "We had to go through all the scenarios" possible, El-Haggan said, including "concerns for the network, for security, and [what would happen] if the network went down." A successful outcome would address the biggest question of all, he added: "Do you really want to outsource your passwords and put them somewhere else?"

Since provisioning is such an important part of the identity management system, that function, too, had to be carefully checked in the proof of concept. "We built the whole environment and mimicked how it was going to work," he said. "Fischer was willing to do that for us.... We went through it all and everything worked. That's how we got the buy-in."

Just two months into the move so far, El-Haggan said he is saving the equivalent of two full-time equivalent staff members--resources he has been able to deploy in other directions. Furthermore, his licensing expense with Fischer did not change with the move, although he pointed out that he gained the benefit of having the vendor, not the university, responsible for running, maintaining, updating, backing up, and otherwise supporting the software. "My maintenance costs did not increase, even though Fischer is taking care everything for the same price." The move was so transparent that users remain unaware that the software is now running off site.

Higher education presents an interesting slate of identity management issues, Fischer's Sroka said, because unlike corporations, colleges and universities must deal with at least two sides of the security challenge--keeping a university's operational systems safe and secure and handling personal ID management for students accessing community resources outside the institution's direct control.

About the Author

Linda Briggs is a freelance writer based in San Diego, Calif. She can be reached at lbriggs@lindabriggs.com.