HARVARD UNIVERSITY
Information Technology

CASE STUDY

Keeping Harvard's Authentication Engine Running

Harvard LDAP Cloud Deployment Improves Agility, Reduces Downtime

As the primary University attribute authority, Harvard LDAP (HLDAP) is a critical hub used by thousands of applications every day as a source for data to authorize user access, populate forms, and much more. That's why it's essential that HLDAP remain secure, rock-solid, and resilient to usage spikes and other unforeseen challenges — some of the primary drivers leading the Identity & Access Management (IAM) program team at Harvard University Information Technology to establish HLDAP in the Amazon Web Services (AWS) cloud in 2015. And while a cloud-based LDAP ushered in a variety of additional benefits in efficiency and cost savings, nowhere was the advantage seen more than in the realm of scalability, particularly as demonstrated in a single incident — or, perhaps, non-incident — in September 2015, when **a combination of automated cloud monitoring, AWS auto-scaling, and the IAM team's nimble DevOps methodology resolved what could have been a major University-wide incident in a remarkable 11-minute time frame**.

The Problem

User login activity on the morning of Thursday, Sep. 24, 2015, was unusually high, spiking from about 5,000 authentications per hour to approximately 10,000 authentications per hour — enough to cause HLDAP in its existing configuration to reach 100% utilization and prevent users from reaching the login screen for applications protected by HarvardKey (previously PIN). Potential causes for the sharp rise in activity included a regular weekly Thursday login spike from hourly employees asked to approve time sheets, authentication by a sizable Alumni population invited to claim HarvardKey credentials after the service's launch three days prior, and a host of other factors; however, regardless of the cause, immediate action was necessary to restore HLDAP service during a time of day generally marked by peak traffic.

9/24/15: BY THE NUMBERS

10:31 a.m. *Alert received*
10:35 a.m. *HLDAP identified as likely cause; scaling initiated*

10:40 a.m. *HLDAP restored*

10:42 a.m. *Alert cleared*

While in the past, the alarm would be raised on such a widespread outage as a result of a sudden uptick in new service desk tickets, the IAM team had an additional early-warning system: automatic alerts triggered by AWS CloudWatch monitoring. This enabled IAM DevOps staff to initiate mitigation procedures that resolved the outage in a substantially tighter time frame than had been possible before the cloud — so quickly, in fact, that the problem was solved in less time than it would have taken to raise a major incident under standard HUIT procedure.

The Solution

What did it take to mitigate the usage spike and get HLDAP back up to full strength? A substantial capacity boost, but very little sweat effort by IAM DevOps thanks to the cloud. Once the need was identified, AWS auto-scaling increased the number of HLDAP slave servers from two to eight, doubling performance and throughput when compared to the same time on the previous day.

In addition, the team spun up a separate LDAP environment to mimic this new production setup for the purposes of additional stress tests — a precautionary measure that would have been cost- and labor-prohibitive outside of the cloud. This ability to quickly instantiate duplicate environments on an as-needed basis without the added cost of physical infrastructure is an invaluable asset for both diagnosing existing issues and preventing future problems from disrupting service.

The Result

As demonstrated by the events in September 2015, "infrastructure as code" isn't just a buzzword; as a result of establishing HLDAP in the cloud, the IAM team can control hardware more than ever before, and at a greatly reduced fiscal and time cost. The result is not only an enormous benefit to HUIT staff, freed from traditional data-center shackles of budgets, physical logistics, and shipment times — but also a huge reliability boost to the 30,000-plus users who use HLDAP every day to gain access to their critical Harvard applications and services.

CLOUD LDAP: THE BENEFITS

Monitoring & Alerting
New Relic alerting and CloudWatch monitoring/alerting replace old hard-coded Nagios solution

Autoscaling
Now can automatically scale up/down based on traffic or load thresholds to ensure robustness

Creating New Environments
New environments can now be created with a few clicks on a pay-as-you-go model