

Case Study:

Enabling a Web Server Migration for a Legacy-Bound Enterprise

SSO/Rest plugins allow a major retailer's web access management platform to support NGINX+

A large, multinational retailer had decided to migrate all of its e-commerce web servers to NGINX+. However, a significant technical obstacle threatened to block the move: the company's enterprise web access management (WAM) platform, CA Single Sign-On was unable to support NGINX.

Swapping to another WAM platform was not a realistic option for the retailer for several reasons:

- The existing solution was otherwise functioning quite well for on-premises systems.
- Its implementation had involved significant time and investment.
- No alternative technology, such as federation, was able to provide the full perimeter security, authorization and session management capabilities required for its solution.

“Walking away from the migration would have resulted in a failure to achieve anticipated gains in performance, reliability, scalability, and ease of maintenance.”

Faced with these considerations, the retailer was considering abandoning its migration plans. But walking away from the migration would have resulted in a failure to achieve anticipated gains in performance, reliability, scalability, and ease of maintenance.

SSO/Rest provided an elegant solution: lightweight, HTTP-based SSO/Rest Plugins for NGINX replaced CA Single Sign-On's heavy, vendor-proprietary web agents. A hardened SSO/Rest Gateway located in the retailer's DMZ securely mediated communication between the NGINX plugins and the retailer's policy servers.

In addition to the desired compatibility with CA Single Sign-On, the plugins (which SSO/Rest provides for most major web servers and application platforms) brought the added benefits:

- They are simple, drop-in replacements for CA Single Sign-On web agents;
- They are self-contained (requiring no external code libraries), enabling them to be installed either at the server level or bundled directly into applications;
- The plugins have the ability to function both inside and outside an enterprise's perimeter;
- They use an HTTP-based protocol, meaning that they required no new firewall holes and minimize network latency issues.

By implementing IDF Connect's SSO/Rest, the retailer was able to accomplish its migration to NGINX+ *and* keep its well-functioning enterprise WAM solution. As an added benefit, it was now well-positioned to use SSO/Rest to Cloud-enable secured applications, should it decide to do so.

Contact us:

Learn more about how IDF Connect's SSO/Rest can increase the reach of your current Access Management platform; both by expanding the range of supported platforms, and by Cloud-enabling your secured applications. Please contact us for more information, or to schedule a demo.

Email: info@idfconnect.com Office: (888) 765-1611 Website: www.idfconnect.com