DERIVE TECHNOLOGIES

CASE STUDY

Microsoft ADFS: Unifying Major Business Applications for Healthcare and Nonprofit Organizations

Two of **Derive Technologies'** nonprofit organization clients – a Greater NY Metro-area nonprofit hospital (a client of the dedicated Derive Healthcare practice), and an important, NY Metro-area-based nonprofit children's' welfare organization – were seeking solutions to unify access to major business application suites. Previously, users would access, or, for newly-implemented applications, have to begin to access these major business software packages through disparate, cumbersome sign-on credentials over multiple services.

Derive solved this problem by deploying **Microsoft Active Directory Federation Services (ADFS)**, which supports secure access to desktop images, applications and databases through a seamless single sign-on with one set of user credentials, which still enable users to have time-saving, fully secure, uniquely assigned profiles.

Business Challenge

Many of today's businesses and public sector organizations face challenges in the creation of centrolineal, secure processes for user access to systems and data across their enterprises. This is especially important in today's multifaceted working paradigm—with applications and data residing in physical repositories (data centers), and virtual and cloud architectures, accessed in central and satellite offices, and anywhere, anytime, by mobile workforces (through BYOD).

In 2015, two of Derive Technologies' distinguished public sector clients – one, a leading, Greater New York-Area Nonprofit Hospital; the other, a renowned, over century-old, child welfare nonprofit – expanded their business applications and frameworks. Utilizing the Microsoft Windows Server 2012 R2 platform, and Microsoft SQL Server 2012, these clients were implementing, respectively, new Infor cloud apps (Lawson System Foundation, Infor Smart Office, Infor Landmark Technology, Infor ION, Infor Ming.le, and Infor Lawson Analytics for the healthcare client), and PeopleFluent Human Capital Management (HCM)/ERP and related software for the child welfare nonprofit. With disparate machines, access paradigms, etc., management and adoption of these complex applications across each organization would, typically, be particularly demanding.

It was decided by each of these organizations, in consultation with Derive Technologies – Derive is a Microsoft Gold Certified Data Center Partner – to leverage new services for Windows 2012 to deploy, for all of their users (working in all methods), unified access to essential business applications.

Derive's professional services team comprises Microsoft-focused, Systems Management, Virtualization and Cloud practices, in addition to possessing a series of other infrastructure and application specializations.

Derive supported technology projects for both clients prior to 2015—in the case of the Greater New York Metro-area hospital, Derive had a more-than-decade-long relationship with, and supported multiple technology initiatives for, the organization. For these reasons, and because of Derive's experience with the Microsoft platform, and, overall, with complex infrastructure – some of the core systems within each of these organizations were previously implemented for, and are maintained, by Derive – Derive was selected to support the implementation of these centralized, Windows-based access platforms.

Derive Solutions

Derive turned to **Active Directory Federation Services ("ADFS," or "AD FS")**, part of Microsoft Windows Server 2012 R2 to deliver the access management architecture for both nonprofits. According to Microsoft, ADFS, ***"simplifies access to systems and applications using a claims-based access (CBA) authorization mechanism to maintain application security."*** Microsoft continues, stating that ADFS, "is a standards-based service that allows the secure sharing of identity information between trusted business partners (known as a federation) across an extranet."

For the Greater New York-area hospital, the Infor CloudSuite application solution was, and continues to be, capable of accepting Single Sign-On ("SSO") authentication credentials from local domain controllers, and to provide seamless access to resources. This would eliminate the need to re-authenticate, maintain, and manage an additional authentication schema within the mixed technology environment. Through ADFS, Derive would extend Microsoft Active Directory using ADFS for Infor Cloud (and MS SQL Database 2012) access. The hospital comprised three (3) ADFS application servers and Citrix NetScaler NDX 8500 Load Balancers (Derive is also a very long-time Citrix Solution Provider Partner). Using database mirroring — for primary production, for local disaster recovery and for a second production site, a disaster recovery facility located in another state – secure VPN (VDFS) would be run through ADFS site-to-site. The ADFS infrastructure would support authentication to the cloud privately and publicly. in Microsoft's words: ***"In ADFS, identity federation is established between two organizations by establishing trust between two security realms. A federation server on one side (the Accounts side) authenticates the user through the standard means in Active Directory Domain Services and then issues a token containing a series of claims about the user, including its identity. On the other side, the Resources side, another federation server validates the token and issues another token for the local servers to accept the claimed identity. This allows a system to provide controlled access to its resources or services to a user that belongs to another security realm without requiring the user to authenticate directly to the system and without the two systems sharing a database of user identities or passwords."*** When the hospital's users would need need to, per Microsoft, "access a Web application from one of its federation partners," in this case, the Infor CloudSuite, "the user's own organization is responsible for authenticating the user and providing identity information in the form of 'claims' to the partner that hosts the Web application." This was achieved with the Active Directory and ADFS architecture deployed by Derive, with Derive also providing a unified, hospital-branded login page for access to all of the Infor CloudSuite applications and data. The hospital's own team supported the application integration, and Derive managed the entire ADFS authentication process and delivery of the access portal.

The hospital also comprises a separate, for-profit entity—a multispecialty physician practice, with numerous satellite clinical facilities distributed throughout the state where the hospital is located, which are branded extensions of the care model offered by the organization.

These clinical facilities would also need secure access to a number of the hospital's Infor CloudSuite applications, and Derive was able to set up onboarding protocols for custom-designed sign-on to the Infor apps and data that would maintain security throughout these disparate offices.

The other client, the important, nationwide child welfare nonprofit organization, was, in 2015, in the process of implementing PeopleFluent's cloud-based human capital management HCM software suite (HR, ERP) for use by multiple groups of its employees. Like the Infor CloudSuite for the other client – the hospital – the the PeopleFluent cloud suite for this child welfare nonprofit client, has the capacity to accept Single Sign-On ("SSO") authentication credentials from Microsoft ADFS servers. Specifically, SSO would be established when one of Derive's client's users would successfully authenticate to one of the CAS domain controllers, and, without re-authenticating, navigate to a PeopleFluent application to access secure PeopleFluent web-hosted resources.

Again here, the client's internal team implemented the PeopleFluent suite, while Derive architected and deployed the ADFS solution. All employees – comprising nearly 2,000 users throughout the organization – had to manage their access through different platforms, and maintain separate usernames and passwords to access their core desktop image and the PeopleFluent suite. To resolve this issue with one single sign-on protocol, Derive built out a highly-available, scalable ADFS 2012 R2 server infrastructure for the organization, located in two of its data centers: the primary facility in the client's headquarters in Manhattan, as well as in a secondary site in another New York City borough. The organization also leverages managed data support services through a provider in New Jersey – for disaster recovery – requiring a mirrored set of protocols. Overall, the client had, and continues to have three Windows Servers running SQL 2012, with database (DB) mirroring to the other New York borough site and to the external NJ managed datacenter. In this case, Microsoft Windows Server acted as the ADFS proxy (instead of Citrix or other manufacturers' load balancing solutions)— converting the authentication scheme from claims-based authentication to an Active Directory process (Kerberos to LDAP). As in the other engagement, Derive provided a branded login portal page for all users, wherein they would enter their credentials one time only and then be provided with fully-assigned, secure access to all applications merely by clicking on the application icon.

At the conclusion of the engagement for the child welfare services nonprofit client, Derive was able to support one login for every current and onboarded user for the PeopleFluent suite. Previously, the users would sign into their desktop image, then have a desktop icon to log in to PeopleFluent with separate credentials. Derive's ADFS solution enabled single sign-on to the desktop image and PeopleFluent, with no need for second-level sign-on, and with only one username and password per user.

The Results

For the Greater New York Metro area hospital, the implementation of the ADFS solution, using Microsoft and Citrix, took approximately two weeks. Coordination with the internal client team managing the Infor CloudSuite application deployment required additional time as it was an new application to the organization. However, cutover was performed quickly—Infor Lawson Analytics also used a separate interface from the rest of the Infor application suite, but it was cut over quickly to the secure single sign-on protocol, only requiring that the back-end ADFS and Citrix infrastructure was in- place, then authentication would also occur for each user accessing it through their login credentials. This seamless integration for all of the hospital's nearly 2,000 users was seen as a great success by the client, which continues to engage Derive for extended ADFS and onboarding support,

both for the main hospital and for new clinical practices, as well as upgrades and tuning. This has led to a cascading set of additional engagements for Derive in support of the hospital's team—some directly related to secure access and applications; others, in-keeping with Derive's long-time relationship with the organization and as a result in the confidence further built with the client because of the positive outcome of the recent ADFS rollout.

For the child welfare services nonprofit, it took under two weeks to achieve the overall ADFS deployment – across all sites – with, after setup and testing, the final cutover having been performed over a weekend: Friday implementation, cutover testing by Derive and the client over the weekend, and the single sign-on support for the PeopleFluent applications seamlessly available on Monday when primary administrative staff returned to work. This was partially facilitated by Derive's preparative steps prior to the cutover, with documentation sent prior to the cutover— Derive provided a sample page (look-and-feel); internal management email sent (collaborative between the client and Derive – that resulted in a smooth cutover. (Derive receive no phone calls from any users experiencing issues with accessing their applications in this new manner.)

As the organization has to be extremely cost-conscious to meet regulatory, donor-centric, and management guidelines, Derive also trained the client's internal technology and business staff on support of the ADFS solution. The engagement was considered a success, and the organization has retained Derive on a managed service block-of-hours agreement for primary upgrades and tuning of the overall solution, and is currently, in 2016 in discussion with the client about the potential of supporting additional (separate) business-technology projects.