Webster University Adopts Modern Directory Platform

Improving Scalability and Streamlining Integration

Webster UNIVERSITY

University environments require a unique approach to Active Directory design and deployment. This is largely due to the presence of multiple, disparate systems that have been installed and configured over the technical lifespan of the University. When Webster University decided to consolidate their internal systems and adopt a modern directory platform that offered native support for Identity Access Management (IAM), the choice was clear. After working with members of the infrastructure support services (ISS) team at DISYS, Webster University elected to use Microsoft Active Directory in Windows Server 2012 R2.

DISYS engineers partnered with the infrastructure team at Webster to design a highly scalable solution based on a Single Forest, Single Domain, Active Directory model that separates Student, Staff and Faculty Assets and Resources from each other using an OU and delegation model. During the discovery phase, several challenging integration and migration points were identified. These potential hurdles assisted the team in creating a better design and in many cases shaped the core enterprise active directory architecture at Webster University.

The existing system architecture at Webster University consisted of a complex array of legacy components for a variety of services — including authentication, authorization, email, identity management, applications access and file and printer services. Integrating a new network operating system and lightweight directory platform with an existing Novell and Oracle platform presented several unique challenges that required a custom approach to deploying eAD across the enterprise.

Key objectives of the Active Directory design focused on:

- University-appropriate Active Directory Forest Domain design and configuration
- Developing an Identity Management and Automation (IAM) solution
- Building a foundation for future success around platform integration with Virtual Desktop Infrastructure (VDI), Mobile Device Management, Cloud, Presence and Collaboration
- Providing an agile and "future-proofed" IT Environment

To achieve their desired technical and business goals, Webster University based their enterprise Active Directory (eAD) design and deployment on Windows Server 2012 R2. This modern server operating system includes several new features and includes native support for the following:

- Simplified deployment and administration of Active Directory
- Improved virtualization functionality
- Enhanced Group Policy capabilities
- Native integration with Cloud (Azure), Collaboration (Sharepoint) and messaging (Office365)

Future Integration with Existing Active Directory forests:

Active Directory forests exist inside the current Webster University infrastructure. Integrating with existing domains and forests is accomplished through bi-directional trust relationships that connect legacy domains with the new production Active Directory. Other legacy domains and directories (e.g. Library, Registrar) may also be migrated into the new enterprise Active Directory as the long-term solution for consolidation and simplification.

Future Migration of Applications:

Upgrading a server Operating System and adopting a new directory platform are very different tasks with respect to complexity and level of effort. After adopting Server 2012 R2, application teams at Webster University had to ensure that existing productivity tools would comply with Server 2012's 64-bit architecture. Application rationalization and remediation was a major focus that heavily influenced the scope of the project.

Short Term Coexistence and Migration of Novell:

A key requirement of the analysis and discovery phase was ensuring the careful coexistence of the Novell environment with the newly-created enterprise Active Directory on Windows Server 2012 R2. Due to the importance of this system, an entire sub-project was created around user files/data on legacy Novell servers and migrating that data onto Windows 2012 File Server clusters. This was a critical factor in eliminating the need to synchronize accounts and passwords between AD and Novell.

Integration of Oracle Directory Service Enterprise Edition:

Both Active Directory and Oracle provide centralized security administration services. DISYS collaborated with Webster engineers to develop, design, and deploy custom synchronization agents that synchronized user data between the two systems. DISYS leveraged Microsoft's Forefront Identity Manager (FIM) 2010 R2 to provide a seamless, natively-supported solution.

Why FIM?

There are many commercial IAM solutions available on the market today. Due to the unique nature of the Education vertical, and the particular challenges often associated with Colleges and Universities, Webster focused on a solution that provided seamless integration with their newly deployed enterprise Active Directory (eAD) while catering to their existing Oracle LDAP and Novell environments. Webster's specific requirements regarding authentication, role transitions, and dynamic group membership — coupled with a legacy student database platform — presented DISYS engineers with many challenges and required several custom management agents. After many weeks of analysis and discovery, Microsoft Forefront Identity Manager 2010 was chosen as the IAM solution.

Microsoft Forefront Identity Manager 2010 R2 delivers self-service identity management for users, automates lifecycle management across heterogeneous platforms for administrators, and provides a rich policy framework for enforcing corporate security policies.

Common identity is an important tool that ensures users have appropriate access to corporate information regardless of where it is located—in a datacenter or in the Cloud. FIM

2010 R2 helps enterprises resolve these issues by providing self-service identity management for its users, automated lifecycle management across heterogeneous platforms for its administrators, and a rich policy framework for enforcing corporate security policies and detailed audit capabilities.

Building a Common Identity

Common identity is an important tool in ensuring appropriate access to corporate information. Without an efficient method of establishing and maintaining a common identity across complex heterogeneous systems, significant challenges arise. These can include high help-desk costs for password resets and smart card deployment, loss of productivity as users struggle to access the resources they need, and serious risk to the business due to noncompliance with internal and external regulations.

Forefront Identity Manager (FIM) 2010 R2 helps resolve these issues by providing self-service identity management for users, automated lifecycle management across heterogeneous platforms for administrators, and a rich policy framework for enforcing corporate security policies and detailed audit capabilities.

Empower people

Productivity suffers and your IT costs go up when users have to call the help desk to address common identity management problems, such as resetting a password. FIM 2010 R2 provides a self-service portal and embeds capabilities in common Microsoft Office tools so users can readily access the services they need — when they need them. Enabling users to solve simple problems like these quickly and easily both improves user productivity and increases user satisfaction.

Self-service portal:

With the FIM 2010 R2 portal, administrators can define policies that allow users to remediate identity issues themselves — updating their identities, managing groups, and resetting passwords across all of an organization's systems.

Easy-to-use interface:

The FIM 2010 R2 interface makes tasks like resetting a PIN or a password very simple. Common user management experiences are integrated into the Windows operating system, Microsoft Outlook, and Microsoft SharePoint collaboration software so users can easily create an email distribution list or add others to a group.

Simplify identity lifecycle management:

Maintaining identities —provisioning, updating, and de-provisioning — can be extremely complex and expensive. This is especially true when considering the high degree of system integration required to get other solutions to work together on disparate identity platforms. FIM 2010 R2 simplifies management of the identity lifecycle through automated workflows and business rules, and offers easy integration with heterogeneous platforms.

Consolidated, cross-platform identity support:

FIM 2010 R2 can automate identity and group provisioning and management based on business policy and implemented through workflows. This automation across heterogeneous systems lowers IT costs and reduces opportunities for error.

Built-in smart card management:

FIM 2010 R2 centrally manages the process for provisioning smart cards, which dramatically reduces the costs typically associated with deploying multi-factor authentication.

Easy extensibility:

FIM 2010 R2 integrates with familiar developer tools so administrators can easily extend capabilities when business needs change. Extending FIM 2010 R2 to support new scenarios is simple using existing identity management tools, through the Microsoft Visual Studio and .NET development environments.

Improve security and compliance:

When identity management is not automated, controlling access and enforcing corporate policy can not only be expensive and time-consuming, but can introduce error and organizational risk. FIM 2010 R2 improves security and compliance by providing auditing, role-based access control, and deep role discovery.

Role-based access administration:

FIM 2010 R2 enables IT to discover and map permissions to individual, assignable roles across multiple systems. Its role-mining tool helps administrators discover the various permission sets for users throughout the enterprise so later they can be modeled and applied centrally.

Centrally-enforced identity policy:

FIM 2010 R2 automatically maintains consistency of identity information and application of user roles across enterprise identity systems. IT and auditors get a single view of individual users and resources, increasing visibility into the compliance and security state of systems across organizations.

In-depth auditing and reporting:

Administrators can audit and report on all the activities and historical states of each event, stage of a workflow, when it took place, and any associated approvals, using such familiar technologies as Microsoft SQL Server and Microsoft System Center.

Conclusion

As a major presence in the global academic community, Webster University had the foresight to adopt and embrace new and modern directory and security solutions from Microsoft. This measure not only increases user satisfaction and decreases administrative overhead, it places the institution on more solid footing for many years to come. Windows Server 2012 R2 provides a stable, dependable easy-to-manage platform. It is an integral part of the Active Directory landscape and Active Directory is a direct beneficiary of many of its new features and benefits. These technologies, coupled with Microsoft's Forefront Identity Manager (FIM) solution provides a world-class identity access platform that will ensure appropriate access to corporate information and user data. Without an efficient method for end user access to data and other tools, especially as it relates to maintaining a common identity across complex heterogeneous systems, significant challenges arise that can put your organization at risk. Microsoft Forefront Identity Manager 2010 in conjunction with enterprise Active Directory (eAD) on Windows Server 2012R2, provides institutions with a flexible, agile directory and identity access platform that works seamlessly and securely with both existing enterprise and legacy assets.

About DISYS

DISYS, LLC is an IT staffing and consulting company serving Fortune 500 and other global-scale enterprises worldwide. DISYS delivers strategic value by understanding and responding to a client's environment, problems, and challenges either by assembling the most highly talented team for any job or delivering more comprehensive, cost-effective IT solutions. Incorporated in 1994 as a certified Minority Business Enterprise, DISYS is headquartered in McLean, Virginia, with offices and delivery locations worldwide.