CASE STUDY– Enterprise Identity Integration and Management

CLIENT : State Department of Developmental Disabilities

Background

Integration and centralization of authentication and authorization between the customer and a third party vendor was resulting in the following technical issues. This was due to exchange of communication between two different enterprise systems containing Identity Managers, Access Managers, Portals and User stores.

1. Certification and key encryption issues
2. Issues with Realm claim values and Reconciliation of User information from Active Directory and ISIM (IBM Security Identity Management)
3. Single Sign on (SSO) issues.

CASE SUMMARY

State Department of Developmental Disabilities

Requirement:

Enterprise Identity Integration and Management

Approach:

Using the Enterprise Identity Model for enabling authentication and authorization integration across the enterprises

Results:

Improved efficiency, increased productivity and reduced helpdesk costs achieved with minimal system configuration changes.

Approach

Three possible models were identified for integrating the enterprise identification systems:

1. *Point to Point Identity Model:* Manage and maintain data within their enterprises and separating the authentication and identity management within their own enterprises. Authentication and authorization would occur independently with both enterprises. The exchange of data between the enterprises will be prepared using tickets. This is a more integrated approach as access control is added in addition to SSO.
2. *Enterprise Identity Model:* Integrating and Centralizing authentication and authorization on one enterprise and let local authorization happen individually at each enterprise based on the policies of each enterprise. It works in a non-intrusive way by capturing the user ID and password for the application when the user logs in. The next time the application is launched, Enterprise Identity will detect the launch, automatically enter credentials on the user's behalf and log them in. It can also be programmed to handle password changes (first time temporary passwords, 90-day password expiration). Since no changes are made to the applications, this provides a relatively quick and all encompassing way to provide SSO to most apps a user would require.
3. *Hybrid Identity Model:* Hybrid identity solutions enable synchronization of the on-premise directory objects with Azure AD while still allowing management of users on-premise. The first decision to make when planning to synchronize an on-premise Windows Server Active Directory with Azure AD is whether to use synchronized identity or federated identity. Synchronized identities, and optionally password hashes,

enable users to use the same password to access both on-premises and cloud-based organizational resources.

Technology

Windows Enterprise Server 2012, Active Directory Federation Services 2016, Relying Party Trust, Forefront Identity Management (FIM) 2010, Kerberos tools, Internet Information Services (IIS), Azure Directory Connect, Azure AD, PowerShell, Active Directory Federation Services (ADFS), and LDAP protocols.

Solution

There were several pros and cons for both solutions to the integration requirement -

When choosing the Point to Point Identity Model

Pros:

a) Less duplication of data, since authentication is centralized for each of the enterprises and data reconciliation can be used to share the data between enterprises when need for auditing. Password maintenance is managed within one enterprise.
b) Sharing of the data between two enterprises through a secure channel.
c) Secure algorithms such as SHA256 and symmetric encryption based on AES can ensure integrity and privacy of the data.
d) In both identity and access management though integration is minimal, low human intervention is needed for customization of workflows.

Cons:

a) Requires greater awareness of each enterprise's security architecture.
b) More project management required on both sides. Longer processes required.
c) Involves upper management approval at every step.
d) Network management investments on both sides.

When choosing the Enterprise Identity Model

Pros:

a) Minimum development and customization of the systems and workflows of each enterprises.
b) Security is done separately for both enterprises without affecting each other.
c) Less investment by each enterprise on acquiring new servers due to separation of the enterprises.

Cons:

a) Duplicate data may exist within both enterprises. More human work force required to verify the data on a daily basis to ensure user data stays unique.
b) User has to authenticate on both enterprises separately - lack of single sign on. Decentralized authorization between the two enterprises.
c) Encryption has to be done completely separately between the two enterprises.
d) Due to difficulties with sharing of data, more resources have to be spent on the certifications on each

enterprise.

Results

The Enterprise Identity model simplified identities and provided an enhanced security profile. This allows easy access, no matter where a user is within the enterprise. This model helped increase productivity and reduces IT costs while improving the user experience. It also contributed to increase efficiency and reduced help desk costs as it greatly reduces the need for changing of passwords.