Enterprise Identity

Hybrid Identity Synchronization

Case study

Waheed Anjum

Microsoft Certified Trainer
Azure Solutions Architect
O365 Architect

Introduction:

Spicy Pizza Ltd. is a renowned company in the food industry that specializes in delivering high-quality pizzas to its customers. The company has a large customer base, and it has recently expanded its operations by opening multiple branches across the country. Spicy Pizza Ltd. has a well-established on-prem Active Directory windows server that manages the authentication and authorization of its users. However, the company is now looking to sync its user to Azure AD with Password Hash Synchronization to provide Single Sign-On (SSO) access to its cloud applications registered in Azure AD.

Challenge:

The main challenge faced by Spicy Pizza Ltd. is to sync its on-prem Active Directory windows server with Azure AD using the Azure AD Connect Agent. The company has 1000 users, 200 groups, and 1200 devices that need to be synced to Azure AD. The CTO of the company wants every user to be able to login with SSO in any cloud application registered in Azure Tenant. For redundancy, there should be a Staging Sync Server, and for security reasons, Azure AD Connect Agent must not be installed directly on Domain Controller.

Solution:

To solve the challenge faced by Spicy Pizza Ltd., the following steps need to be taken:

Step 1: Configure the Azure AD Connect Agent on a separate server

To ensure security, the Azure AD Connect Agent must not be installed directly on the Domain Controller. Therefore, a separate server needs to be set up to install the Azure AD Connect Agent. The server should meet the minimum requirements for running the Azure AD Connect Agent. Once the server is set up, the Azure AD Connect Agent can be installed on it.

Step 2: Sync On-Prem AD users to Azure AD

After installing the Azure AD Connect Agent on the separate server, the next step is to sync the on-prem Active Directory windows server with Azure AD. This can be done by configuring the Azure AD Connect Agent to sync the users, groups, and devices from the on-prem Active Directory windows server to Azure AD. The CTO of the company wants every user to be able to login with SSO in any cloud application registered in Azure AD. To achieve this, Password Hash Synchronization can be enabled, which will sync the password hashes of the on-prem AD users to Azure AD, allowing them to log in to the cloud applications with their existing passwords.

Step 3: Set up a Staging Sync Server

To ensure redundancy, a Staging Sync Server can be set up, which will act as a backup server in case the main server fails. The Staging Sync Server should have the Azure AD Connect Agent installed and configured to sync with Azure AD. The Staging Sync Server should be in a different physical location to ensure high availability.

Step 4: Create Guest Users for Collaboration with Burger King Ltd.

To collaborate with Burger King Ltd., their users need to be joined to Spicy Pizza's Azure AD Tenant as Guest users. All the company users must be created in the local AD to sync to Azure AD, allowing them to collaborate with Burger King Ltd. Once the Guest users are created, they can be granted access to the resources hosted on Spicy Pizza's Azure Tenant.

Conclusion:

In conclusion, Spicy Pizza Ltd. faced a challenge in syncing its on-prem Active Directory windows server with Azure AD to provide Single Sign-On (SSO) access to its cloud applications registered in Azure AD. The company has 1000 users, 200 groups, and 1200 devices that need to be synced to Azure AD. To overcome this challenge, the company set up a separate server to install the Azure AD Connect Agent, configured the Agent to sync the users, groups, and devices from the on-prem Active Directory windows server to Azure AD, enabled Password Hash.