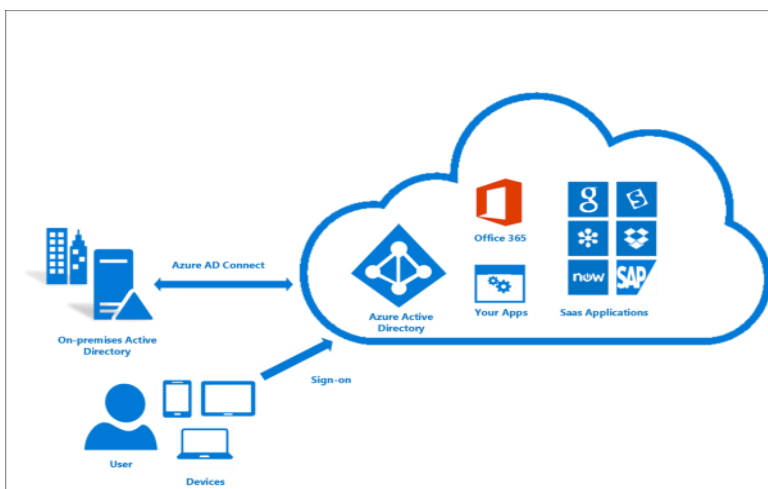# ON-PREMISES AD MIGRATION TO CLOUD AZURE AD

Client

Solution provider to government and industries

Business Overview

- Integrate on-premises directories with Azure Active Directory
- Configure the local Active Directory sync with Azure Active Directory using with AAD connect tool.

Business Challenge

- Spending money for server environment setup and server maintenance and hardware issues.

- Active Directory is difficult to integrate into pre-existing network systems. There is little interoperability between Windows 2000/2003 Active Directory and NetWare or Unix systems
- Active Directory was designed to use a single forest for each organization. Those companies that need multiple schemas or global catalogs must implement multiple forests.
- Multiple forests re-introduce the same problems that occurred with multiple Windows NT domains and they introduce related increases in administrative overhead.
- Separate domains and forests cannot easily be merged together. Instead, you need an arduous migration process to move the important entities from one domain or forest into the other.
- Active Directory relies upon DNS to function, but not all DNS servers are capable of supporting Active Directory. Existing DNS systems may need to be upgraded or replaced before they can support Active Directory

Solution

Creating a Azure active directory on cloud and integrate the On-premises active directory into Azure active directory using AAD connect tool. Integrating On-premises directories with Azure AD makes our users more productive by providing a common identity for accessing both cloud and on-premises resources. Users and organizations can take advantage of the following:

- Users can use a single identity to access on-premises applications and cloud services such as Office 365.
- Single tool to provide an easy deployment experience for synchronization and sign-in.

Benefits

Filtering is used when we want to limit which objects are synchronized to Azure AD. By default, all users, contacts, groups, and Windows 10 computers are synchronized.

Password synchronization synchronizes the password hash in Active Directory to Azure AD. The end-user can use the same password on-premises and in the cloud but only manage it in one location. Since it uses your on-premises Active Directory as the authority, you can also use your own password policy.

Device write back will allow a device registered in Azure AD to be written back to on-premises Active Directory so it can be used for conditional access.

The prevent accidental deletes feature is turned on by default and protects your cloud directory from numerous deletes at the same time. By default it allows 500 deletes per run.

Automatic upgrade is enabled by default for express settings installations and ensures your Azure AD Connect is always up to date with the latest release.