Sync on-premises AD with Windows Azure AD

Azure AD is a service that provides identity and access management capabilities in the cloud. Azure AD can be integrated with existing on-premises AD for providing single sign-on functionality for their users to access the cloud applications. So, it is essential for organizations to keep the credentials in both on-premises AD and Azure AD to be in sync. To solve the sync issues, we have Azure Active Directory connect tool, which provides one-way synchronization from on-premises AD to Azure AD.

# Prerequisites

* Windows Server 2008R2 SP1 or higher
* Only 64-bit version supported
* .Net framework 3.5 SP1 and .net framework 4.0
* Install Active Directory Domain Services role on your local machine and promote it to a Domain Controller

# Environment

* Active subscription for Azure Active Directory
* On-premises AD server (Windows Server 2012)
* Azure AD connect tool

# Synchronizing on-premises AD to Azure AD involves the following steps

## Create Azure AD and Activate Azure AD Connect

* Login to Azure management console
* From the left-hand bottom portion of the menu, click "New".
* Now a new page opens, through which navigate to NEW > APP SERVICES > ACTIVE DIRECTORY > DIRECTORY and click CUSTOM CREATE.
* Provide the name for your directory, choose your domain name and the country of your choice.
* Now the Azure Active Directory has been created successfully.
* To activate the Directory Sync for the created AD, from the left pane select Active Directory, then on the Active Directory page, click Azure AD and select the DIRECTORY INTEGRATION tab. Then click ACTIVATED and finally click SAVE to confirm the changes.
* Now Azure AD Sync has been activated successfully.

## Download and Install Azure AD Connect tool in on-premises AD

* Login to Windows Azure management console from your base machine.
* In the DIRECTORY INTEGRATION menu of your Azure AD, scroll to bottom section and download the Azure AD connect tool.
* After downloading the Azure AD Sync tool, proceed with the installation steps.
* Agree with the License agreements and privacy rules, click Continue.
* Choose whether you would go with an express installation or a customized installation.
* Now provide the credentials of the user account with Administrator permissions in on-premises AD to grant the permission to install the Azure AD Connect synchronization service and click Install.
* Select the Single Sign On method for user sign in and click Next.
* Connect to Azure active directory providing the credentials of a global admin user pre-existing in the directory and click Next.
* Enter connection information for your on-premises directory or forests and click on Add Directory.
* Since we do not have a verified custom domain, choose the check box saying Continue without verified domains (users will not be able to use on-premises credentials to Azure AD sign-in) and click Next.
* In the next dialog box, you will be provided with the option to sync all the domains or the selected domain.
* Select the domain of your choice and click Next.
* Select how the users should be identified in your on-premises directories and click Next.
* In the opted domain, you can further choose whether to include all users and groups or a selected group and user respectively.
* Type in the Azure group name and click on Resolve to have the parameters auto populated. Click on Next
* Select other enhanced functionality if required by your organization and click Next.
* The Azure AD connect tool in now ready to synchronise the on-premises AD with the Azure AD. Click on Install to complete the process.
* The configuration is now complete, and you can verify in your Azure AD that the user accounts have been created.

To confirm the sync between on-premises AD with Azure AD, login to Windows Azure management console and navigate to Active Directory > Azure AD > Users. In the Users list, we can confirm that the user account created in on-premises AD is synchronized with Windows Azure AD.

Hereby we have synchronized the on-premise AD with Windows Azure AD using Azure AD Connect tool.