# Module 10: Managing an Active Directory infrastructure in a hybrid environment

# Lab: Implementing and managing Azure AD synchronization

### Scenario

A. Datum Corporation users rely on SSO to access on-premises applications. While evaluating Azure for A. Datum, you need to verify that A. Datum users can use their existing credentials to access resources in Azure, including non-Microsoft software as a service (SaaS) applications. You need to verify that any password or Active Directory user and group account changes in on-premises Active Directory automatically replicate to Azure AD.

### Objectives

After completing this lab, you will be able to:

* Configure directory synchronization.
* Synchronize on-premises Active Directory with Azure Active Directory.

### Lab Setup

Estimated Time: 60 minutes

Virtual machine: \*\* 20533C-MIA-CL1\*\*

User name: \*\* Student\*\*

Password: **Pa$$w0rd**

## Exercise 1: Configuring directory synchronization

### Scenario

A. Datum plans to implement directory integration. To test the planned implementation, you need to deploy and configure Azure AD Connect to synchronize your on-premises AD with a test Azure AD tenant. To eliminate the need to verify a custom DNS domain, you will be using the default DNS name of the test Azure AD domain.

The main tasks for this exercise are as follows:

1. Sign in to the Azure VM hosting an Active Directory domain controller.
2. Create a new Azure AD tenant and a Global Admin account
3. Install Azure AD Connect with custom settings

#### Task 1: Sign in to the Azure VM hosting an Active Directory domain controller.

1. Sign in to MIA-CL1 as **Student** with the password **Pa$$w0rd**.
2. In the Internet Explorer window, sign in to the Azure portal by using the Microsoft account that is the Service Administrator or a co-admin of your Azure subscription
3. Initiate a Remote Desktop Protocol (RDP) session to **AdatumDC1**, and then sign in as **ADATUM\* with the password** Pa$$w0rd123\*\*.

#### Task 2: Create a new Azure AD tenant and a Global Admin account

1. After the sign-in is complete, open Internet Explorer and navigate to the Azure classic portal.
2. When prompted, sign in to the Azure classic portal by using an account that is the Service Administrator or a co-admin of your Azure subscription.
3. In the Azure classic portal, create a new Azure Active Directory tenant with the following settings:

* DIRECTORY: *Create new directory*
* NAME: **AdatumSync**
* DOMAIN NAME: *Use your initials* + *the* *directory name* + *random numbers* (for example, abcadatum123456). If you get the message **The domain is not unique**, change the numbers until you get a green check mark.
* COUNTRY OR REGION: **United States**

1. In the Azure classic portal, in the newly created Azure Active Directory tenant, create a new Global Admin user with the following settings:

* TYPE OF USER: *New user in your organization*
* USER NAME: **SyncAdmin**
* FIRST NAME: **Sync**
* LAST NAME: **Admin**
* DISPLAY NAME: **Sync Admin**
* ROLE: Global **Admin**
* ALTERNATE EMAIL ADDRESS: *Type the email address of your Microsoft account*
* Enable Multi-Factor Authentication: *Do not select*

1. Change the temporary password of the newly created user to **Pa$$w0rd** by using an Internet Explorer inPrivate Browsing session.
2. Once you change the password, on the **No subscriptions found** page, click **SIGN OUT**.
3. Close the **InPrivate** Internet Explorer session.

#### Task 3: Install Azure AD Connect with custom settings

1. Open Internet Explorer on AdatumDC1, and then download Azure AD Connect from https://www.microsoft.com/en-us/download/details.aspx?id=47594. You will need to add \*\*https://\*.microsoft.com\*\* to the list of Internet Explorer Trusted sites.
2. Install the Azure AD Connect tool, select custom settings, and then ensure that **Password Synchronization** is selected.
3. Set the credentials for Azure AD tenant AdatumSync to the SyncAdmin Global Admin account.
4. Set the credentials for the Active Directory forest to **ADATUM\* with the password** Pa$$w0rd123\*\*.
5. On the **Domain and OUfiltering** page, limit synchronization to objects in the **Accounts** organization unit only.
6. Accept the default values in the remaining wizard pages, and then start the synchronization process. Close the wizard once the configuration is completed. > **Note:** You might need to wait a few minutes for the initial synchronization to complete.
7. In the Azure classic portal, navigate to the **adatumsync** Active Directory page. Click **USERS**, and then confirm that the list of users includes all the names from the Accounts organizational unit (OU).

**Result**: After completing this exercise, you should have installed and configured Azure AD Connect, and you should have it ready for test synchronization.

## Exercise 2: Synchronizing directories

### Scenario

A. Datum wants to test Azure AD synchronization by changing a few attributes of a user account and then performing manual synchronization.

The main tasks for this exercise are as follows:

1. Modify attributes of an Active Directory user and Initiate manual synchronization
2. Reset the environment

#### Task 1: Modify attributes of an Active Directory user and Initiate manual synchronization

1. On AdatumDC1, change the following attributes of some of your users in the Accounts OU of the Adatum directory:

* **Job Title**: **VP**
* **Department**: **Marketing**

1. Start a Windows PowerShell session by using administrative credentials.
2. At the Windows PowerShell command prompt, type the following commands, press Enter after each, and observe the results:

Get-ADSyncScheduler  
Start-ADSyncSyncCycle -PolicyType Delta

1. On the Azure classic portal, check that the changes that you made to the user accounts have replicated to Azure; if you do not see any changes, wait for a few minutes, and then refresh the page.
2. Close the AdatumDC1 remote desktop session, and then click **OK** when prompted.

#### Task 2: Reset the environment

1. On MIA-CL1, close all open applications without saving any files.
2. On the taskbar, right-click **Windows** **PowerShell**, and then click **Run as administrator**.
3. In the **User Account Control** dialog box, click **Yes**.
4. Type the following command, and then press Enter:

Reset-Azure

1. When prompted (twice), sign in by using the Microsoft account associated with your Azure subscription
2. If you have multiple Azure subscriptions, select the one you want the script to target
3. When prompted for confirmation, type **y**.

**Note:** This script might remove Azure services in your subscription. We therefore recommend that you use an Azure trial pass that was provisioned specifically for this course, and not your own Azure account. The script will take 5-10 minutes to reset your Azure environment and make it ready for the next module. The script removes all storage, virtual machines, virtual networks, cloud services, and resource groups. **Important:** The script might not be able to get exclusive access to a storage account to delete it; if this occurs, you will see an error. If you find objects remaining after the reset script is complete, you can rerun the **Reset-Azure** script, or you can use the Azure classic portal to delete all the objects in your Azure subscription manually, with the exception of the default directory.

**Result**: After completing this exercise, you should have changed attributes on a user account, and then forced synchronization.

**Question** How do you configure organizational unit (OU)-level filtering for directory synchronization?

**Question** When do you use Azure AD Connect custom setup?

©2016 Microsoft Corporation. All rights reserved.

The text in this document is available under the [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/legalcode), additional terms may apply. All other content contained in this document (including, without limitation, trademarks, logos, images, etc.) are **not** included within the Creative Commons license grant. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. Microsoft makes no warranties, express or implied, with respect to the information provided here.