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

# Lab: Implementing and managing Azure AD synchronization

### Scenario

Adatum Corporation users access on-premises applications by authenticating once, during initial sign-in to their client computers. While evaluating Azure for Adatum, you must verify that Adatum users can continue using their existing credentials to access Azure resources. In addition, you must verify that attribute changes to Active Directory user and group accounts will 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: **20533E-MIA-CL1**

User name: **Student**

Password: **Pa55w.rd**

## Exercise 1: Configuring directory synchronization

### Scenario

Adatum plans to integrate its AD DS with Azure AD. To test this plan, you need to deploy and configure Azure AD Connect to synchronize your test Active Directory environment 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 and create test Active Directory objects.
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 and create test Active Directory objects.

1. Sign in to MIA-CL1 as **Student** with the password **Pa55w.rd**.
2. Open the file **F:\Labfiles\Lab10\Starter\Set-20533E1001Lab.ps1** in WordPad and copy all lines to Clipboard.
3. In the Microsoft Edge window, navigate to the Azure portal and, when prompted, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
4. If necessary, in the Azure portal, switch to the Azure Active Directory tenant associated with the Azure subscription that you chose when running the provisioning script at the beginning of this module.
5. Initiate a Remote Desktop Protocol (RDP) session to **20533E1001-vm1**, and then sign in as **ADATUM\Student** with the password **Pa55w.rd1234**.
6. In the Remote Desktop session, start Windows PowerShell ISE as administrator, paste the content of Clipboard into the script pane and run the pasted commands.
7. From the Windows PowerShell ISE window, run the **Get-ADUser** cmdlet to verify that the list of Active Directory user accounts includes **Beverly Beach** in the **AccountsToSync** organizational unit and **Darwin Shivers** in the **AccountsNotToSync** organizational unit.
8. Close the **Administrator: Windows PowerShell ISE** window.

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

1. Within the Remote Desktop session, from Server Manager, disable IE Enhanced Security Configuration for administrators.
2. Open Internet Explorer and navigate to the Azure portal. If prompted to set up Internet Explorer 11, ensure that the **Use recommended security, privacy, and compatibility settings** option is selected and click **OK**.
3. From the Azure portal, create a new Azure AD tenant with the following settings:

* Organization name: **AdatumSync**
* Initial domain name: a unique, valid name
* Country or region: **United States**

1. Refresh the Microsoft Edge window, in the Azure portal, switch to the newly created Azure AD tenant, and create a new Global Admin user with the following settings:

* Name: **SyncAdmin**
* User name: **syncadmin@*domain-name*.onmicrosoft.com** where ***domain-name*** is the unique name you assigned to the AdatumSync Azure AD tenant earlier in this task
* First name: **Sync**
* Last name: **Admin**
* Directory role: **Global administrator**
* Show Password: enabled

1. Take the note of the autogenerated temporary password.
2. Open an Internet Explorer InPrivate Browsing session, sign in to the Azure portal as **SyncAdmin**, and change the password to a new value. Take a note of the new value.
3. Sign out as SyncAdmin and close the InPrivate Microsoft Edge session.

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

1. From the Remote Desktop session to 20533E1001-vm1, switch to the Internet Explorer displaying the Azure portal. Use the **Download Azure AD Connect** link on the **Azure AD Connect** page of locate the download page of Azure AD Connect MSI file and download it the **Downloads** folder.
2. Install the Azure AD Connect tool, select custom settings, and then ensure that **Password Hash Synchronization** is selected as the Sign On method.
3. Set the credentials for Azure AD tenant AdatumSync to the **SyncAdmin** Global Administrator account.
4. Set the AD forest account to **ADATUM\Student** with the password **Pa55w.rd1234**.
5. On the **Domain and OU filtering** page, limit synchronization to the **AccountsToSync** 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:** Installation will take a few minutes.

1. In the Azure portal, on the **AdatumSync** blade, navigate to the **All Users** blade of the **AdatumSync** Azure AD tenantn and confirm that the list of users includes **Beverly Beach** from the **AccountsToSync** OU but does not include **Darwin Shivers** from the **AccountsNotToSync** OU.

**Result**: After completing this exercise, you should have installed and configured Azure AD Connect, and have performed initial synchronization.

## Exercise 2: Managing synchonization

### Scenario

Adatum wants to test Azure AD synchronization by changing a few attributes of a synchronized 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. Remove the lab environment

#### Task 1: Modify attributes of an Active Directory user and initiate delta synchronization

1. On 20533E1001-vm1, start **Windows PowerShell ISE** as Administrator.
2. From the Windows PowerShell ISE console, check the value of the **Title** and **Department** attributes of the user **bbeach** by using the **Get-ADUser** cmdlet.
3. From the Windows PowerShell ISE console, use the **Set-ADUser** cmdlet to set the value of the **Title** and **Department** attributes of the user **bbeach** to **VP** and **Marketing**, respectively.
4. From the Windows PowerShell ISE console, import the module **'C:\Program Files\Microsoft AZure AD Sync\Bin\ADSync\ADSync.psd1'** and check the current synchronization settings by running the **Get-ADSyncScheduler** cmdlet.
5. From the Windows PowerShell ISE console, start delta synchronization by running **Start-ADSyncSyncCycle -PolicyType Delta**.
6. From the the **Users and groups - All Users** blade in the Azure portal, verify that the changes that you made to the user accounts have been synchronized to Azure AD. If you do not see any changes, wait for a few minutes, and then refresh the page.
7. Close the 20533E1001-vm1 Remote Desktop session.

#### Task 2: Remove the lab environment

1. On MIA-CL1, close all open windows without saving any files.
2. Start **Windows PowerShell** as Administrator and, from the **Administrator: Windows PowerShell** window, run **Remove-20533EEnvironment**.
3. When prompted, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
4. If you have multiple Azure subscriptions, select the one you want the script to target.
5. If prompted, specify the current lab number.
6. When prompted for confirmation, type **y**.
7. Start Microsoft Edge, browse to the Azure portal, and sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
8. In the Azure portal, reset the dashboard to the default state.
9. Start **Windows PowerShell** as Administrator.
10. Use the **Connect-MsolService** cmdlet to authenticate to the AdatumSync Azure Active Directory tenant by using the SyncAdmin credentials.
11. Use the **Set-MsolDirSyncEnabled** cmdlet to disable directory synchronization to the AdatumSync Azure Active Directory tenant.
12. Close all open windows.

**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.