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

# Lab: Implementing and managing Azure AD synchronization

## Exercise 1: Configuring directory synchronization

#### 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. Right-click **Start** and click **Run** (alternatively, click **Start** and type **Run** in the Start menu Search box, or press the **Windows key+R**). In the **Run** text box, type the following and press **Enter**:

Write F:\Labfiles\Lab10\Starter\Set-20533E1001Lab.ps1

1. In WordPad, select all lines in the file.
2. In WordPad, click **Copy**.
3. Open Microsoft Edge and browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com).
4. When prompted, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
5. Note the user name entry in the upper right corner of the Azure portal and ensure that you are signed on to the correct Azure Active Direcory tenant. If not, click the **Directory + subscription** filter icon appearing directly to the left of your name in the upper right corner of the Azure portal and, in the **Directory + Subscription** pane, click the name of the Azure Active Directory tenant associated with the Azure subscription that you chose when running the provisioning script at the beginning of this module.
6. In the hub menu of the Azure portal, click **All services** and then, in the service menu, click **Virtual machines**.
7. On the Virtual machines blade, click the ellipsis to the right of the **20533E1001-vm1** entry and click **Connect**.
8. On the **Connect to virtual machine** blade, click **Download RDP File**. When prompted, click **Open**.
9. If a Remote Desktop Connection warning message displays, select **Don't ask me again for connections to this computer**, and then click **Connect**.
10. In the **Windows Security** dialog box, type the following credentials, and then click **OK**:

* User name: **ADATUM\Student**
* Password: **Pa55w.rd1234**

1. If another Remote Desktop Message displays, select the **Don't ask me again for connections to this computer** checkbox, and then click **Yes**.
2. In the Remote Desktop Session to 20533E1001-vm1, click **Start**, right-click **Windows PowerShell ISE**, click **More**, and click **Run as administrator**.
3. In the **Administrator: Windows PowerShell ISE** window, click **View** and, in the drop-down menu, click **Show Script Pane**.
4. Click **Edit** and, in the drop-down menu, click **Paste** to paste the content of **Set-20533E1001Lab.ps1** you copied to Clipboard.
5. Click **Debug** and, in the drop-down menu, click **Run/Continue**.
6. In the PowerShell ISE console, type the following and press Enter:

Get-ADUser -Filter \* | Select-Object DistinguishedName

1. Verify that the list of accounts includes **Beverly Beach** in the **AccountsToSync** organizational unit and **Darwin Shivers** in the **AccountsNotToSync** organizational unit.
2. Close the **Administrator: Windows PowerShell ISE** window.

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

1. In the Remote Desktop Session to 20533E1001-vm1, in **Server Manager**, click **Local Server**.
2. Click the **On** link next to the **IE Enhanced Security Configuration** label.
3. In the Internet Explorer Enhanced Security Configuration dialog box, in the **Administrators** section, click **Off** and click **OK**.
4. Click the **Internet Explorer** shortcut on the taskbar.
5. If prompted, ensure that **Use recommended security, privacy, and compatibility settings** is selected and then click **OK**.
6. In Internet Explorer, navigate to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com).
7. When prompted, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
8. Click **+ Create resource** in the upper left corner of the portal, click **Identity**, and then, click **Azure Active Directory**.
9. On the **Active Directory Enterprise** blade, specify the following settings and click **Create**:

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

1. Wait until the new directory is provisioned.
2. Refresh the Internet Explorer window. Next, click the **Directory + subscription** filter icon appearing directly to the left of your name in the upper right corner of the Azure portal and, in the **Directory + Subscription** pane, click the name of the newly created Azure Active Directory tenant.
3. Ensure that **ADATUMSYNC** appears in the upper right corner of the portal underneath your Microsoft account name and, in the hub menu, click **All services**
4. In the services menu, click **Azure Active Directory**
5. On the **AdatumSync - Overview** blade, in the **Create** section, click the **User** link.
6. On the **User** blade, specify the following settings and click **Create**:

* 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

1. Click **Profile**. On the **Profile** blade, in the **First name** textbox, type **Sync**, in the **Last name** textbox type **Admin** and click **OK**.
2. Click **Directory role**.
3. On the **Directory role** blade, click **Global administrator** and click **OK**.
4. Enable **Show Password** checkbox and note the password.
5. Click **Create**
6. Start an InPrivate Internet Explorer session and browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com).
7. When prompted to sign in, specify the full user name (including the @\*domain name\*.onmicrosoft.com suffix) of the SyncAdmin account and the corresponding temporary password.
8. On the **Update your password** page, in the **Current password** box, type again the temporary password. In the **New password** and **Confirm password** text boxes, type a new password, and click **Update password and sign in**. Take a note of the new password.

**Note:** If you receive the message **We've seen that password too many times before. Choose something harder to guess**, you'll need to modify the password until it is unique enough to be accepted.

1. If prompted to stay signed in, click **No**. Next, if prompted to start Microsoft Azure tour, click **Maybe later**. Next, click the user name in the upper-right corner and, in the drop-down menu, click **Sign out**
2. Close the InPrivate Internet Explorer session.

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

1. In the Remote Desktop session to 20533E1001-vm1, switch to the Azure portal.
2. Navigate to the **Azure Active Directory** blade and under **AdatumSync - Overview**, click **Azure AD Connect**, and then click the **Download Azure AD Connect** link. This will redirect you to the Microsoft Download Center page of Azure AD Connect.
3. On the Microsoft Download Center page of Azure AD Connect, click **Download**.
4. In the pop-up bar at the bottom of the Internet Explorer window, click **Run**.
5. If prompted, in the **Open File - Security Warning** dialog box, click **Run**.
6. On the **Welcome** page, select **I agree to the license terms and privacy notice**, and then click **Continue**.
7. On the **Express Settings** page, click **Customize**.
8. On the **Required Component** page, review the options, and then click **Install**.
9. On the **User sign-in** page, verify that **Password Hash Synchronization** is selected, and then click **Next**.
10. On the **Connect to Azure AD** page, provide the credentials of the newly created SyncAdmin Azure AD Global Admin, and then click **Next**:

* USERNAME: **syncadmin@*domain name*.onmicrosoft.com** where ***domain name*** is the unique name you assigned to the new Azure Active Directory tenant in task 2
* PASSWORD: the corresponding password

1. On the **Connect your directories** page, verify that the **adatum.com** forest is selected and click **Add Directory**
2. In the **AD forest account** window, click **Use existing AD account**, specify the following and click **OK**:

* DOMAIN\USERNAME: **ADATUM\Student**
* PASSWORD: **Pa55w.rd1234**, click **OK**

1. Click **Next**.
2. On the **Azure AD sign-in configuration**, note the message **Users will not be able to sign-in Azure AD using their on-premises credentials**. This is expected since you do not have a verified domain name. Enable the **Continue without any verified domains** checkbox and click **Next**.
3. On the **Domain and OU filtering** page, select the **Sync selected domains and OUs** check box, expand the **adatum.com** entry, clear all checkboxes with exception of the one next to the **AccountsToSync** entry, and then click **Next**.
4. On the **Uniquely identifying your users** page, verify that **Users are represented only once across all directories** is selected, and then click **Next**.
5. On the **Filter users and devices** page, verify that **Synchronize all users and devices** is selected, and then click **Next**.
6. On the **Optional feature** page, verify that **Password hash synchronization** is selected, and then click **Next**.
7. On the **Ready to configure** page, verify that **Start synchronization process as soon as the configuration completes** is selected, and then click **Install**.

**Note:** Installation will take a few minutes.

1. On the **Configuration complete** page, click **Exit** to close Azure AD Connect.

**Note:** You might need to wait a few minutes for the initial synchronization to complete.

1. Switch back to the Azure portal in the Internet Explorer window.
2. In the Azure portal, on the **AdatumSync** blade, click **Users**, click **All Users** 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

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

1. In the Remote Desktop Session to 20533E1001-vm1, in the **Administrator: Windows PowerShell ISE** window, in the console pane, type the following command and press **Enter**:

$user = Get-ADUser -Filter "SamAccountName -eq 'bbeach'" -Properties Department,Title -SearchBase 'OU=AccountsToSync,DC=adatum,DC=com'

1. In the console of the Windows PowerShell ISE window, type the following command and press **Enter**:

$user | Get-ADUser -Properties Department,Title

1. Note the current values of the **Title** and **Department** properties.
2. In the console of the Windows PowerShell ISE window, type the following command and press **Enter**:

$user | Set-ADUser -Title 'VP' -Department 'Marketing'

1. In the console of the Windows PowerShell ISE window, type the following command and press **Enter**:

$user | Get-ADUser -Properties Department,Title

1. Verify that the values of the **Title** and **Department** properties have changed.
2. In the console pane of the Windows PowerShell ISE, type the following command and press **Enter**:

Import-Module "C:\Program Files\Microsoft AZure AD Sync\Bin\ADSync\ADSync.psd1"

1. In the console pane of the Windows PowerShell ISE, type the following command and press **Enter**:

Get-ADSyncScheduler

**Note:** **Get-ADSyncScheduler** displays the current configuration settings for synchronization with Azure AD.

1. At the Windows PowerShell command prompt, type the following command, and then press Enter:

Start-ADSyncSyncCycle -PolicyType Delta

1. Wait until synchronization completes before proceeding to the next step.
2. Switch back to the Azure portal in the Internet Explorer window.
3. In the Azure portal, on the **AdatumSync** blade, on the **Users and groups - All Users** blade, click **Beverly Beach**
4. On the **Beverly Beach - Profile** blade, in the **Job info** section, verify that the values of the **Department** and **Job title** entries match the ones you configured for the Active Directory account. If you do not see any changes, wait for a few minutes, and then refresh the page.
5. Close the **20533E1001-vm1** remote desktop session, and click **OK** when prompted.

#### Task 2: Remove the lab environment

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

Remove-20533EEnvironment

1. When prompted, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
2. If you have multiple Azure subscriptions, select the one you want the script to target.
3. If prompted, specify the current lab number.
4. When prompted for confirmation, type **y**.
5. Start Microsoft Edge, browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com), and sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
6. In the Azure portal, on Dashboard, click **Edit**.
7. Right-click unoccupied area of the dashboard and, in the right-click menu, click **Reset to default state**. When prompted to confirm, click **Yes**.
8. Click **Done customizing**.
9. On MIA-CL1, click **Start**, in the Start menu, expand the **Windows PowerShell** folder, right-click **Windows PowerShell**, click **More**, and then click **Run as administrator**. When prompted by User Account Control for confirmation, click **Yes**.
10. In the Administrator: Windows PowerShell window, enter the following command and press Enter:

Connect-MsolService

1. In the **Sign in** dialog box, enter the full name (including the @\*domain name\*.onmicrosoft.com suffix) of the SyncAdmin account you used in this lab and then click **Next**.
2. In the **Enter password** dialog box, enter the password of the SyncAdmin account and click **Sign in**.
3. At the Windows PowerShell prompt, enter the following command and press Enter:

Set-MsolDirSyncEnabled -EnableDirSync $false -Force

1. Close all open windows.

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

©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.