**Module 1: Identity**

**Exercise 1: Manage Azure Active Directory Identities**

#### Task 1: Create an Azure Active Directory (AD) tenant

In this task, you will create a new Azure AD tenant.

1. In the Azure portal, search for and select **Azure Active Directory**.
2. Click **+ Create a tenant** and specify the following setting:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Directory Type | Azure Active Directory |
| Organization Name | Contoso Lab |
| Initial domain name | any valid DNS name consisting of lowercase letters and digits and starting with a letter |
| Country/Region | United States |

**Note**: The green check mark in the **Initial domain name** text box will indicate that the domain name you typed in is valid and unique.

1. Click **Review + create** and then click **Create**.
2. Display the blade of the newly created Azure AD tenant by using the **Click here to navigate to your new directory: Contoso Lab** link or the **Directory + Subscription** button (directly to the right of the Cloud Shell button) in the Azure portal toolbar.

#### Task 2: Manage Azure AD guest users.

In this task, you will create Azure AD guest users and grant them access to resources in an Azure subscription.

1. In the Azure portal displaying the Contoso Lab Azure AD tenant, in the **Manage** section, click **Users**, and then click **+ New user**.
2. Create a new user with the following settings (leave others with their defaults):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| User Name | **az104-01b-aaduser1** |
| Name | **az104-01b-aaduser1** |
| Let me create the password | enabled |
| Initial password | **Pa55w.rd124** |
| Job title | **Cloud Administrator** |
| Department | IT |

**Note**: **Copy to clipboard** the full **User Principal Name** (user name plus domain). You will need it later in this task.

1. Switch back to your default Azure AD tenant by using the **Directory + Subscription** button (directly to the right of the Cloud Shell button) in the Azure portal toolbar.
2. Navigate back to the **Users - All users** blade, and then click **+ New guest user**.
3. Create a new guest user with the following settings (leave others with their defaults):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| User Name | **az104-01c-aaduser1** |
| Email address | Paste the value you copied into clipboard earlier in this task |
| Usage Location | United States |
| Job title | **Lab Administrator** |
| Department | IT |

1. Click **Invite**.

#### Task 3: Create and configure Azure AD users

In this task, you will create and configure Azure AD users.

1. In the Azure portal, search for and select **Azure Active Directory**.
2. On the Azure Active Directory blade, scroll down to the **Manage** section, click **User settings**, and review available configuration options.
3. On the Azure Active Directory blade, in the **Manage** section, click **Users**, and then click your user account to display its **Profile** settings.
4. Click **edit**, in the **Settings** section, set **Usage location** to **United States** and save the change.

**Note**: This is necessary in order to assign an Azure AD Premium P2 license to your user account later in this lab.

1. Navigate back to the **Users - All users** blade, and then click **+ New user**.
2. Create a new user with the following settings (leave others with their defaults):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| User Name | **az104-01a-aaduser1** |
| Name | **az104-01a-aaduser1** |
| Let me create the password | enabled |
| Initial password | **Pa55w.rd124** |
| Usage location | United States |
| Job title | **Cloud Administrator** |
| Department | IT |

**Note**: **Copy to clipboard** the full **User Principal Name** (user name plus domain). You will need it later in this task.

1. In the list of users, click the newly created user account to display its blade.
2. Review the options available in the **Manage** section and note that you can identify the Azure AD roles assigned to the user account as well as the user account’s permissions to Azure resources.
3. In the **Manage** section, click **Assigned roles**, then click **+ Add assignment** button and assign the **User administrator** role to **az104-01a-aaduser1**.

**Note**: You also have the option of assigning Azure AD roles when provisioning a new user.

1. Open an **InPrivate** browser window and sign in to the [Azure portal](https://portal.azure.com/) using the newly created user account. When prompted to update the password, change the password for the user.

**Note**: Rather than typing the user name (including the domain name), you can paste the content of Clipboard.

1. In the **InPrivate** browser window, in the Azure portal, search for and select **Azure Active Directory**.

**Note**: While this user account can access the Azure Active Directory tenant, it does not have any access to Azure resources. This is expected, since such access would need to be granted explicitly by using Azure Role-Based Access Control.

1. In the **InPrivate** browser window, on the Azure AD blade, scroll down to the **Manage** section, click **User settings**, and note that you do not have permissions to modify any configuration options.
2. In the **InPrivate** browser window, on the Azure AD blade, in the **Manage** section, click **Users**, and then click **+ New user**.
3. Create a new user with the following settings (leave others with their defaults):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| User Name | **az104-01a-aaduser2** |
| Name | **az104-01a-aaduser2** |
| Let me create the password | enabled |
| Initial password | **Pa55w.rd124** |
| Usage location | United States |
| Job title | **Cloud Administrator** |
| Department | IT |

1. Sign out as the az104-01a-aaduser1 user from the Azure portal and close the InPrivate browser window.

#### Task 4: Create Azure AD groups with assigned and dynamic membership

In this task, you will create Azure Active Directory groups with assigned and dynamic membership.

1. Back in the Azure portal where you are signed in with your user account, navigate back to the **Overview** blade of the Azure AD tenant and, in the **Manage** section, click **Licenses**.

**Note**: Azure AD Premium P1 or P2 licenses are required in order to implement dynamic groups.

1. In the **Manage** section, click **Licenses**.
2. Click **+ Try/Buy** and activate the free trial of Azure AD Premium P2.
3. Refresh the browser window to verify that the activation was successful.
4. From the **Licenses - All products** blade, select the **Azure Active Directory Premium P2** entry, and assign all license options of Azure AD Premium P2 to your user account and the two newly created user accounts.
5. In the Azure portal, navigate back to the Azure AD tenant blade and click **Groups**.
6. Use the **+ New group** button to create a new group with the following settings:

|  |  |
| --- | --- |
| Setting | Value |
| Group type | Security |
| Group name | IT Cloud Administrators |
| Group description | Contoso IT cloud administrators |
| Membership type | Dynamic User |

**Note**: If the **Membership type** drop-down list is grayed out, wait a few minutes and refresh the browser page.

1. Click **Add dynamic query**.
2. On the **Configure Rules** tab of the **Dynamic membership rules** blade, create a new rule with the following settings:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Property | jobTitle |
| Operator | Equals |
| Value | Cloud administrators |

1. Save the rule and, back on the **New Group** blade, click **Create**.
2. Back on the **Groups - All groups** blade of the Azure AD tenant, click the **+ New group** button and create a new group with the following settings:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Group Type | Security |
| Group Name | IT System Administrators |
| Group Description | Contoso IT system administrators |
| Membership type | Dynamic User |

1. Click **Add dynamic query**.
2. On the **Configure Rules** tab of the **Dynamic membership rules** blade, create a new rule with the following settings:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Property | jobTitle |
| Operator | Equals |
| Value | System administrators |

1. Save the rule and, back on the **New Group** blade, click **Create**.
2. Back on the **Groups - All groups** blade of the Azure AD tenant, click the **+ New group** button, and create a new group with the following settings:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Group Type | Security |
| Group Name | IT Lab Administrators |
| Group Description | Contoso IT system administrators |
| Membership type | Assigned |

1. Click **No members selected**.
2. From the **Add members** blade, search and select the **IT Cloud Administrators** and **IT System Administrators** groups and, back on the **New Group** blade, click **Create**.
3. Back on the **Groups - All groups** blade, click the entry representing the **IT Cloud Administrators** group and, on then display its **Members** blade. Verify that the **az104-01a-aaduser1** appears in the list of group members.
4. Navigate back to the **Groups - All groups** blade, click the entry representing the **IT System Administrators** group and, on then display its **Members** blade. Verify that the **az104-01a-aaduser2** appears in the list of group members.

**Note**: You might experience delays with updates of the dynamic membership groups. To expedite the update, navigate to the group blade, display its **Dynamic membership rules** blade, **Edit** the rule listed in the **Rule syntax** textbox by adding a whitespace at the end, and **Save** the change.

**Exercise 2: Implementing AD DS synchronization with Microsoft Azure AD (Optional)**

**Lab Environment:**

* Azure Virtual machines: **VM0 & VM1**
* User name: **student**
* Password: **Pa55w.rd1234**



#### Task 1: Create resource groups and deploy resources to resource groups

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. Search for and select **Resource groups**.
3. On the **Resource groups** blade, click **+ Add** and create a resource group with the following settings:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you will use in this lab** |
| Resource Group | **az104-01-rg0** |
| Region | **the name of any Azure region available in the subscription you will use in this lab** |

1. Click **Review + Create** and then click **Create**.

#### Task 2: Deploy virtual machines into the virtual network

In this task, you will deploy Azure virtual machines into different subnets of the virtual network by using an ARM template

1. In the Azure portal, search **Deploy a custom template**.
2. On the **Customs deployment** blade, click **Build your own template in the editor**.
3. On the **Edit template** blade, click **Load file**, select the file named **az104-01-vm-template.json** and then press **Open**.
4. On the **Edit template** blade, click **Save**.
5. On the **Custom deployment** blade, click **Edit Parameters + Load File**, select the file named **az104-01-vm-parameters.json** and then press **Open**.
6. On the **Edit template** blade, click **Save**.
7. On the **Custom** **deployment** blade type the following settings:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you will use in this lab** |
| Resource Group | **az104-01-rg0** |
| Region | **the name of any Azure region available in the subscription you will use in this lab** |
| Name Suffix | **0** |

1. Click **Review + Create** and then click **Create**.
2. Once the Deployment has finished repeat the steps 1-5 only changing the Name Suffix by 1.

#### Task 3: Deploy AD DS Forest

In this task, you will deploy an AD DS Forest.

1. On the resource group named **az104-01-rg0** open the virtual machine named **az104-01-vm0**.
2. On the **az104-01-vm0** blade click Overview and copy the **Private IP address** assigned to VM.
3. Back to the resource group named **az104-01-rg0** open the virtual network named **az104-01-vnet0**.
4. On the **az104-01-vnet0** **settings** blade click DNS servers and type the following settings:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| DNS servers | **custom** |
| IP Address | **Type the IP address copied on step 2** |

1. Click **Save**.
2. Connect to virtual machine named **az104-01-vm0** by RDP connection and then install and setup the Active Directory Administrative Services with the following settings:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Forest Name | **contoso.com** |
| User | **student** |
| Password | **Pa55w.rd1234** |

1. Connect to virtual machine named **az104-01-vm1** by RDP connection and then add it to domain named **contoso.com**.

#### Task 4: Configure a synchronization account

1. In the Azure portal, search Azure Active Directory.
2. In the **Azure Active Directory – Overview**, click **Manage tenants** and then switch to the AAD created in the Exercise 1.
3. In the **Azure Active Directory -** **MANAGE** options list, click **Users and groups**.
4. Click **All users**. You will see only your account.
5. Click **New User**.
6. In the **User** pane, type **SYNC** in the **Name** text box.
7. Type **sync@contoso*yymmdd*.onmicrosoft.com** (where **contoso*yymmdd*.onmicrosoft.com** is your domain name that was defined in Exercise 1, task 1) in the **User name** text box.
8. Click **Directory role**.
9. In the **Directory role** pane, click **Global administrator**, and then click **Select**.
10. Click **Show Password**. Copy the password shown in the text box to Notepad.
11. Click **Create**.
12. Right-click the **Internet Explorer** icon on the taskbar, and then click **Start InPrivate Browsing**.
13. In the new browser window, go to **https://portal.azure.com**.
14. Sign in as **sync@contoso*yymmdd*.onmicrosoft.com** with the temporary password that you copied in step 10.
15. On the **Update your password** page, type your temporary password in the **Current password** text box, and then type **Pa55w.rd1234** in the **New password** and **Confirm password** text boxes. Click **Update password and sign in**.
16. Verify that the Azure portal opens. Close the **Internet Explorer** window. Keep Internet Explorer, where you are signed in with your account, open.

#### Task 7: Install and configure Azure AD Connect

1. Connect by RDP to the Azure’s VM named **az104-01-vm1**.
2. On **az104-01-vm1 (Azure VM)**, sign in as **Student**.
3. Enable **TLS 1.2**, open PowerShell as Administrator and type the below commands:

New-Item 'HKLM:\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319' -name 'SystemDefaultTlsVersions' -value '1' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319' -name 'SchUseStrongCrypto' -value '1' -PropertyType 'DWord' -Force | Out-Null

New-Item 'HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319' -name 'SystemDefaultTlsVersions' -value '1' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319' -name 'SchUseStrongCrypto' -value '1' -PropertyType 'DWord' -Force | Out-Null

New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' -name 'Enabled' -value '1' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' -name 'DisabledByDefault' -value 0 -PropertyType 'DWord' -Force | Out-Null

New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client' -name 'Enabled' -value '1' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client' -name 'DisabledByDefault' -value 0 -PropertyType 'DWord' -Force | Out-Null

Write-Host 'TLS 1.2 has been enabled.'

1. Open this link [**https://www.microsoft.com/en-us/download/details.aspx?id=47594**](https://www.microsoft.com/en-us/download/details.aspx?id=47594) to download the **Microsoft Azure Active Directory Connect**, after that **Run** it.
2. In the **Microsoft Azure Active Directory Connect Wizard**, on the **Welcome to Azure AD Connect** page, select **I agree to the license terms and privacy notice**, and then click **Continue**.
3. On the **Express Settings** page, click **Use express settings**.
4. On the **Connect to Azure AD** page, in the **USERNAME** text box, type the **SYNC** account user name created on Task 1. In the **PASSWORD** text box, type **Pa55w.rd1234**, and then click **Next**.
5. On the **Connect to AD DS** page, in the **USERNAME** text box, type **Contoso\student**. In the **PASSWORD** box, type **Pa55w.rd1234**, and then click **Next**.
6. On the **Azure AD sign-in configuration** page, select **Continue without any verified domains**, and then click **Next**.
7. Click **Install**, and when the installation is complete, click **Exit**.
8. Now, the synchronization of objects from your local Active Directory Domain Services (AD DS) and Microsoft Azure Active Directory (Azure AD) begins. You must wait approximately 5-10 minutes for this process to complete.
9. Close the **Internet Explorer** window on **az104-01-vm1**.

#### Task 8: Verify the initial synchronization and manage the settings

1. Switch to Internet Explorer on **local computer**. You should have the Azure portal open.
2. Click **Users and groups** in the **MANAGE** options list.
3. Click **All users**.
4. Verify that you can see the user accounts from your local AD DS. You should be able to see all users from your local **contoso.com** domain.
5. Switch to **az104-01-vm1**.
6. On **az104-01-vm1**, click **Start**, and then click **Azure AD Connect**. Expand **Azure AD Connect**, and then click **Synchronization Service**.
7. In the **Synchronization Service Manager on az104-01-vm1** window, click the **Operations** tab.
8. Ensure that you can see the **Export, Full Synchronization**, and **Full Import** tasks.
9. Ensure that all the tasks have a current time and date in the **Start Time** and **End Time** columns. Also, ensure that all tasks show **success** in the **Status** column.
10. Close the **Synchronization Service Manager** window.
11. On **az104-01-vm1**, click **Start**, and then open **Windows PowerShell**.
12. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter.

Get-ADSyncScheduler

1. Review the results. Ensure that the **AllowedSyncCycleInterval** value and the **CurrentlyEffectiveSyncCycleInterval** value are set to **30 minutes**.
2. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

Set-ADSyncScheduler –CustomizedSyncCycleInterval 01:00:00

1. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

Wait for approximately two minutes.

1. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

Get-ADSyncScheduler

1. Ensure that the new value is applied for the **CurrentlyEffectiveSyncCycleInterval** variable.
2. Close the **Windows PowerShell** window.

#### Task 9: Add new objects in AD DS

1. Switch to **az104-01-vm0**.
2. Open **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
3. In the navigation pane, expand **Contoso.com**, right-click **IT**, click **New**, and then click **User**.
4. In the **New Object – User** dialog box, in the **Full name** text box, type your name.
5. In the **User logon name** text box, type *your first name*, and then click **Next**.
6. In the **Password** and **Confirm password** boxes, type **Pa55w.rd1234**, and then clear **User must change password at next logon**.
7. Click **Next**, click **Finish**, and then click **Sales**.
8. Right-click your user account, and then click **Add to a group**.
9. In the **Select Groups** dialog box, in the **Enter the object names to select (examples)** text box, type **IT**, and then click **OK**.
10. In the **Active Directory Domain Services** dialog box, click **OK**.

#### Task 10: Verify the synchronization of the new user objects

1. On **az104-01-vm1**, right-click **Start**, and then click **Windows PowerShell (Admin)**.
2. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

Start-ADSyncSyncCycle –PolicyType Delta

1. Wait for approximately four minutes. Do not close the **Administrator: Windows PowerShell** window. However, you can minimize it.
2. Switch to Internet Explorer on **local computer**, where you have the Azure portal open.
3. Refresh the webpage, click **All users**, and then verify that the user account you just added is present.
4. Close the **Internet Explorer** window.

#### Clean up resources (Exercise 1)

**Note**: Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs. While, in this case, there are no additional charges associated with Azure Active Directory tenants and their objects, you might want to consider removing the user accounts, the group accounts, and the Azure Active Directory tenant you created in this lab.

1. Navigate to the **Azure Active Directory Premium P2 - Licensed users** blade, select the user accounts to which you assigned licenses in this lab, click **Remove license**, and, when prompted to confirm, click **OK**.
2. In the Azure portal, navigate to the **Users - All users** blade, click the entry representing the **az104-01b-aaduser1** guest user account, on the **az104-01b-aaduser1 - Profile** blade click **Delete**, and, when prompted to confirm, click **OK**.
3. Repeat the same sequence of steps to delete the remaining user accounts you created in this lab.
4. Navigate to the **Groups - All groups** blade, select the groups you created in this lab, click **Delete**, and, when prompted to confirm, click **OK**.
5. In the Azure portal, display the blade of the Contoso Lab Azure AD tenant by using the **Directory + Subscription** button (directly to the right of the Cloud Shell button) in the Azure portal toolbar.
6. Navigate to the **Users - All users** blade, click the entry representing the **az104-01b-aaduser1** user account, on the **az104-01b-aaduser1 - Profile** blade click **Delete**, and, when prompted to confirm, click **OK**.
7. Navigate to the **Contoso Lab - Overview** blade of the Contoso Lab Azure AD tenant, click **Delete tenant**, on the **Delete directory ‘Contoso Lab’** blade, click the **Get permission to delete Azure resources** link, on the **Properties** blade of Azure Active Directory, set **Access management for Azure resources** to **Yes** and click **Save**.
8. Sign out from the Azure portal and sign in back.
9. Navigate back to the **Delete directory ‘Contoso Lab’** blade and click **Delete**.

#### Clean up resources (Exercise 2)

1. In the Azure portal, open the **PowerShell** session within the **Cloud Shell** pane.
2. List all resource groups created throughout the labs of this module by running the following command:

*Get-AzResourceGroup -Name 'az104-01\*'*

1. Delete all resource groups you created throughout the labs of this module by running the following command:

*Get-AzResourceGroup -Name 'az104-01\*' | Remove-AzResourceGroup -Force -AsJob*

**Note**: The command executes asynchronously (as determined by the -AsJob parameter), so while you will be able to run another PowerShell command immediately afterwards within the same PowerShell session, it will take a few minutes before the resource groups are actually removed.