Module 12: Implementing AD DS synchronization with MS Azure AD

Lab: Configuring directory synchronization

(VMs: 20742B-LON-DC1, 20742B-LON-SVR1, 20742B-LON-CL1)

Exercise 1: Preparing for directory synchronization

Task 1: Create a trial Office 365 E5 subscription

1. On **LON-CL1**, open the **Internet Explorer** browser from the taskbar.
2. Open the ***https://products.office.com/en-us/business/office-365-enterprise-e5-businesssoftware*** URL, and then click the **Free trial** link.
3. On the **Welcome, let's get to know you** page, in the **Country** drop-down list, select your country/region. If your country/region is not listed, choose **United States**.
4. Enter the rest of your data in the fields. Type ***Adatum*** for the **Company name**, and then select **250-999 people** from the **Your organization size** drop-down list.
5. Click **Next**.
6. On the **Create your user ID** page, type the user name of your choice in the **User name** text box, and then type ***Adatumyyxxxxx*** in the **Yourcompany** text box (for example, **Adatum12332**).

Note: *If the name is not available, try a different name. In the following step, you will create a password for the Office 365 user account. Consider writing down this password with the user ID information to ensure that you can use it later.*

7. Choose a password and type it in the **New password** and **Confirm password** text boxes.
8. Click **Create my account**.
9. On the **Prove. You're. Not. A. Robot.** page type your mobile phone number, and then click **Text me**.

Note: *If you do not have a mobile phone with you, ask your instructor for help.*

10. In the **Enter your verification code** text box, type the code that you received in the text message, and then click **Next**.
11. On the **Save this info. You'll need it later** page, ensure that you save your Microsoft Online user ID data, and then click **You're ready to go**.

Note: *Your user ID will be in the format:*
username@Adatumyyxxxxx.onmicrosoft.com
Ensure that you write it down because you will use this account as a global admin account for your Azure AD tenant.

12. Ensure that the Office 365 portal opens.
13. Leave the Internet Explorer browser window open.

Task 2: Verify the Azure AD tenant and add a domain

1. On **LON-CL1**, in the **Internet Explorer** window, open a new tab, and then go to ***https://portal.azure.com***
2. In the Azure portal, in the left navigation pane, click **Azure Active Directory**.
3. In the **MANAGE** options list, click **Custom Domain names**.
4. Verify that you can see your **adatum***yyxxxxx***.onmicrosoft.com** domain that you created in the previous task.
5. Click **Add Custom Domain**.
6. In the **Custom Domain name** pane, type ***Adatum.com*** in the **Custom Domain name** text box, and then click **Add Domain**.
7. On the page to verify domain, review the content, and then close the **Adatum.com** window.
8. Leave the Azure portal open.

Results*: After completing this exercise, you should have created the Azure AD tenant.*

Exercise 2: Configuring directory synchronization

Task 1: Configure a synchronization account

1. On **LON-CL1**, in the Azure portal, in the middle navigation pane, click **Users and groups**.
2. Click **All users**. You will see only your account.
3. Click **New user**.
4. In the **User** pane, type ***SYNC*** in the **Name** text box.
5. Type ***sync@adatum****yyxxxx****.onmicrosoft.com*** (where **adatum***yyxxxx***.onmicrosoft.com** is your domain name that was defined in Exercise 1, Task 1) in the **User name** text box.

6. Click **Directory role**.
7. In the **Directory role** pane, click **Global administrator**, and then click **Ok**.
8. Click **Show Password**. Copy the password shown in the text box to Notepad.
9. Click **Create**.
10. Right-click the **Internet Explorer** icon on the taskbar, and then click **Start InPrivate Browsing**.
11. In the new browser window, go to ***https://portal.azure.com***
12. Sign in as ***sync@adatum****yyxxxx****.onmicrosoft.com*** with the temporary password that you copied in step 8.
13. On the **Update your password** page, type your temporary password in the **Current password** text box, and then type a new password in the **New password** and **Confirm password** text boxes. Click **Update password and sign in**. Document the password for the SYNC account.
14. Verify that the Azure portal opens. Close the **Internet Explorer** window. Keep Internet Explorer, where you are signed in with your account, open.

Task 2: Install and configure Azure AD Connect

1. On **LON-SVR1**, sign in as **Adatum\Administrator**.
2. Open **Internet Explorer** from the taskbar, and then go to ***https://portal.azure.com***
3. On the **Microsoft Azure** page, sign in with the global administrative credentials that you created in Exercise 1, Task 1.
4. In the Microsoft Azure portal, click **Azure Active Directory** in the left navigation pane.
5. In the middle navigation pane, click **Azure AD Connect**.
6. On the **adatum-Azure AD Connect** page, click **Download Azure AD Connect**. A new tab will open in Internet Explorer.
7. On the **Microsoft Azure Active Directory Connect** webpage, click **Download**.
8. When prompted to run or save the file, click **Run**. Minimize the **Internet Explorer** window.
9. 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**.
10. On the **Express Settings** page, click **Use express settings**.
11. On the **Connect to Azure AD** page, in the **USERNAME** text box, type the ***SYNC***

account user name. In the **PASSWORD** text box, type the password that you assigned to the SYNC account, and then click **Next**.
12. On the **Connect to AD DS** page, in the **USERNAME** text box, type ***Adatum\Administrator*** In the **PASSWORD** box, type ***Pa55w.rd*** and then click **next**.
13. On the **Azure AD sign-in configuration** page, select **Continue without any verified domains**, and then click **Next**.
14. On the **Ready to configure** page, click **Install**, and when the configuration is complete, click **Exit**.
15. 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.
16. Close the **Internet Explorer** window on **LON-SVR1**.

Task 3: Verify the initial synchronization and manage the settings

1. Switch to Internet Explorer on **LON-CL1**. 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 adatum.com domain.
5. Switch to **LON-SVR1**.
6. On **LON-SVR1**, click **Start**, and then click **Azure AD Connect**. Expand **Azure AD Connect**, and then click **Synchronization Service**.
7. In the **Synchronization Service Manager on LON-SVR1** 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.

Note: *It is normal for some tasks to have the* ***completed-no-objects*** *status.*

10. Close the **Synchronization Service Manager** window.
11. On **LON-SVR1**, click **Start**, and then open **Windows PowerShell**.
12. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter: ***Get-ADSyncScheduler***

Note: *If this command returns an error, restart the* ***LON-SVR1*** *computer, and then repeat step 12.*

13. Review the results. Ensure that the **AllowedSyncCycleInterval** value and the **CurrentlyEffectiveSyncCycleInterval** value are set to **30 minutes**.
14. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:
Set-ADSyncScheduler –CustomizedSyncCycleInterval 01:00:00
15. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter: ***Start-ADSyncSyncCycle –PolicyType Delta***
16. Wait for approximately two minutes.
17. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter: ***Get-ADSyncScheduler***
18. Ensure that the new value is applied for the **CurrentlyEffectiveSyncCycleInterval** variable.
19. Close the **Windows PowerShell** window.

Results*: After completing this exercise, you should have installed Azure AD Connect with the customized settings, completed directory synchronization to Azure AD, and verified that the synchronization was successful.*

Exercise 3: Managing Active Directory users and groups and monitoring directory synchronization

Task 1: Add new objects in AD DS

1. Switch to **LON-DC1**.
2. Open **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
3. In the navigation pane, expand **Adatum.com**, right-click **Sales**, 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.rd*** 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 ***Sales*** and then click **OK**.
10. In the **Active Directory Domain Services** dialog box, click **OK**.

Task 2: Verify the synchronization of the new user objects

1. On **LON-SVR1**, 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***
3. Wait for approximately four minutes. Do not close the **Administrator: Windows PowerShell** window. However, you can minimize it.
4. Switch to Internet Explorer on **LON-CL1**, where you have the Azure portal open.
5. Refresh the webpage, click **All users**, and then verify that the user account you just added is present and that it has the **Windows Server AD** value in the **SOURCE** column.
6. Click **All groups**, and then click **Sales**. Click **Members**.
7. Verify that your account was also added to the **Sales** group. Leave the browser window open.

Task 3: Configure Azure AD Connect Health

1. On **LON-DC1**, open **Internet Explorer**, and then go to ***https://portal.azure.com***
2. Sign in with the global admin account that you created in Exercise 1, Task 1.
3. In the Azure portal, click **Azure Active Directory** in the left navigation page.
4. In the middle navigation pane, click **Enterprise applications**.
5. In the right pane, click **Start a free trial to use this feature**. Click the same title again on the next screen.
6. In the **Activate** window, in the **AZURE AD PREMIUM** section, click **Free trial**.
7. In the **Activate Azure AD Premium trial** window, click **Activate**.
8. Wait for a few minutes.
9. In the Azure portal, in the left navigation pane, click **More services**.
10. In the search box, type ***Azure AD Connect***
11. In the results below, click the star beside Azure AD Connect Health and then click **Azure AD Connect Health**.
12. In the **Azure AD Connect Health** window, click **Quick Start**.
13. On the **Quick Start** page, click **Download Azure AD Connect Health Agent for AD DS**.

14. When prompted, click **Run**.
15. In the **Microsoft Azure AD Connect Health agent for AD DS** window, click **Install**.
16. When setup finishes, click **Configure Now**.
17. When prompted for an Azure account, type the global admin account that you created in Exercise 1, Task 1, and then click **Continue**. Use the password that you assigned to the global admin account as the password, and then click **Sign in**.
18. Wait for a few minutes until in the PowerShell window you get the message that Agent registration completed successfully.
19. In the Azure portal, close the **Quick Start** page.
20. On the **Azure Active Directory Connect Health** page, in the **Azure Active Directory Connect (Sync)** section, click your domain name. Review the provided data, and then close the page.
21. On the **Azure Active Directory Connect Health** page, in the **Active Directory Domain Services** section, click **Adatum.com**, and then click **Settings**.
22. On the **Settings** page, click **Property**. Review the provided data, and then close the **Property** page.
23. Click **FSMO Roles**. Review the provided data, and then close the **FSMO Roles** page.
24. Click **Users**. On the **Users** page, click **Add**.
25. On the **Add permissions** page, in the **Role** drop-down list, select **Contributor**.
26. Click the **Select** field, select **August Towle** from the list, and then click **Save**.
27. Close the **Settings** page. Review the rest of the data about your local AD DS, and then close Internet Explorer.

Task 4: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:
1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742B-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 to revert **20742B-LON-SVR1** and **20742B-LON-CL1**.

Results*: After completing this exercise, you should have identified how managing user and group accounts has changed with directory synchronization.*