Azure AD Integration (Portal)

(LAB-103-09-03)

Part A: Create Azure AD User with Global Administrator Role

1. Sign in to the Azure Portal
2. Go to the left-side, select "***Azure Active Directory***"
3. Under the manage, select the "**User"**, the select "***+New user***" & fill out the required information:

    a. **Name**: The first and last name of the new user

    b. **User name**: Provide user name "***adconnect***"
    Help: Your user name should be,
    ad*connect@domainname.com*, like

    c. **Directory role**: Select directory role as "***Global administrator***"

4. Copy the auto-generated password provided in the "***Password***" box. You'll need to give this password to the user for the initial sign-in process.
5. Select "***Create***". The user is created and added to your Azure AD tenant.

Part B: Sign-in using Azure AD Id using adonnect user

1. Open the ***portal.azure.com*** from new browser
2. Login with Azure AD "***adconnect***" Id
3. Change the password

Part C: Create Windows Virtual Machine

1. The first thing to do when creating virtual machines with the Azure Portal is log in to Azure with your **root administrative credentials**.

    Note: This is the id you are using since start of the session to login in your account

2. Click the ***virtual machines*** link in the left-hand navigation bar.

3. Click the ***add*** button to start the creation process.

4. You will be required to fill in specific information regarding your virtual machine, including:
    a. ***Subscription***: Select default subscription group

    b. ***Resource Group***: Enter "***AAD-DOMAIN-RG***"

    c. ***Name***: Enter "***AADVM01***"

    d. ***Region***: Select "***East US***"

    e. ***Image***: Select "***Windows Server 2016 Datacenter***"

    f. ***Size***: Select "***B2ms***"

    g. ***Administrator Account***:
        i. Provide "***Username***"
        ii. Provide "***Password***"

    h. ***Inbound Port Rules***: Select "***Port 3389***"

5. Click the "***Next: Disks***" button to continue

6. Click the "***Next***: ***Networking***" button to continue.

7. Click the "***Next: Management***" button to continue.

8. Click on the "***Next: Advance***" config to continue.

9. Click the "***Next: Tags***" button to continue.

10. Click the "***Next: Review + create***" button to continue.

11. Click the "***Create***" button

Part D: Configure DNS to Azure IaaS Virtual Machine

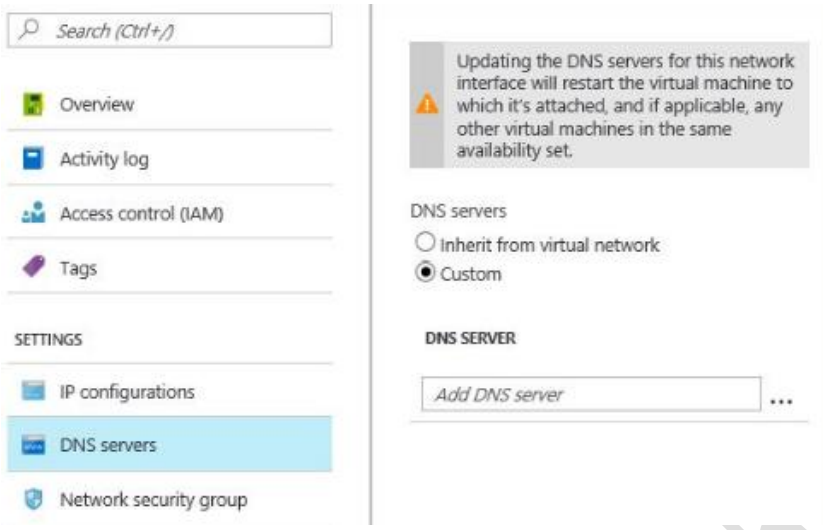
1. From the Azure Portal, go to the left menu, select virtual machines

2. Select the **AADVM01** virtual machine from the list

3. On the right side of the page copy "***Private IP Address***"

4. Select "***Networking***" under settings blade, open the "***Network interface***" name

5. Select "***DNS servers***" under settings, select "***Custom***"



6. Copy "***Private IP Address***" & "***Save***"
7. From the Azure Portal, go to the left menu, select virtual machines
8. Select the virtual machine from the list
9. Restart the virtual machine from portal, once virtual machine in running state
10. Right click on "***Start***" & "***Run***"
11. In the open, write "***cmd***", write "***ipconfig***"
12. Verify DNS Server pointing to virtual machine itself

Part E: Connect to Windows Active Directory Virtual Machine

1. From the Azure Portal, go to the left menu, select Virtual Machines.
2. Select the virtual machine from the list.
3. On the right side of the page copy "***Public IP Address***"
4. In the local Desktop/ Laptop (Windows 10), right click on "***Start***" & "***Run***"
5. In the open, write "***mstsc***"
6. Enter in the "***Public IP Address"*** of the Azure virtual machine, and then click "**Connect"**

7. Enter the "***Username***" and "***Password***" of the Azure virtual machine and click "**OK"**

8. Click "**Yes"** to confirm this connection if prompted with the security message

Part F: Install the Windows Active Directory

1. In the virtual machine, right click on "***Start***" & "***Run***"

2. In the open, write "***servermanager***", it opens the new page

3. Select the "***add roles and features"*** wizard, click on next to proceed.

4. Then in next window keep the default and click next, since it's going to be local server, in next window keep the default selection.

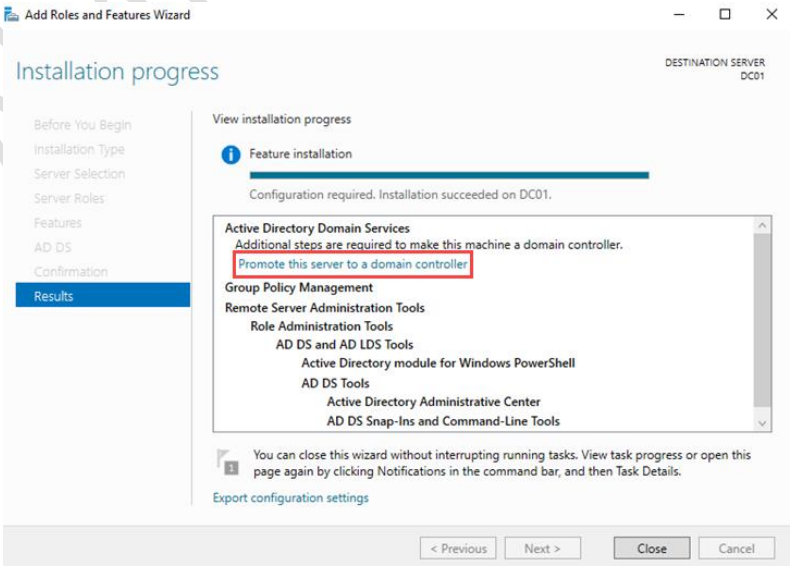
5. In next window from the roles put tick box for ***active directory domain services***. Then it will prompt to show you what are the associated features for the role. Click on add features to add those. Then click next to continue.

6. The features page, keep it default and click on next to proceed.

7. In next windows it gives brief description about AD DS service. Click next to proceed.

8. Then it will give the confirmation about install, click on install to start the role installation process. Once done, it will start the installation process

9. Once installation completes, click on option **promote this server to a domain controller**.



10. Then it will open the active directory configuration wizard, provide the following details

    a. Select "***add a new forest***"

    b. Root domain name: Provide domain name like **ahmad.com**

    c. Click next

11. In next page type a password for DSRM. Then click next. Leave all other options as default

12. For the DNS options, this going to be the first DNS server in new forest. I No changes needed. Click next to proceed.

13. For the NETBIOS name keep the default and click next

14. Next page is to define the NTDS, SYSVOL and LOG file folders. Click next to continue

15. Next page will give option to review the configuration changes. If everything okay, you can click next to proceed or otherwise can go back and change the settings.

16. In next windows it will do prerequisite check. If it's all good it will enable option to install. Click on install to begin installation process.

17. Then it will start the installation process.

18. After the installation system will restart automatically. Once it comes back log in to the server as domain admin.

Part G: Create new User in Windows Active Directory

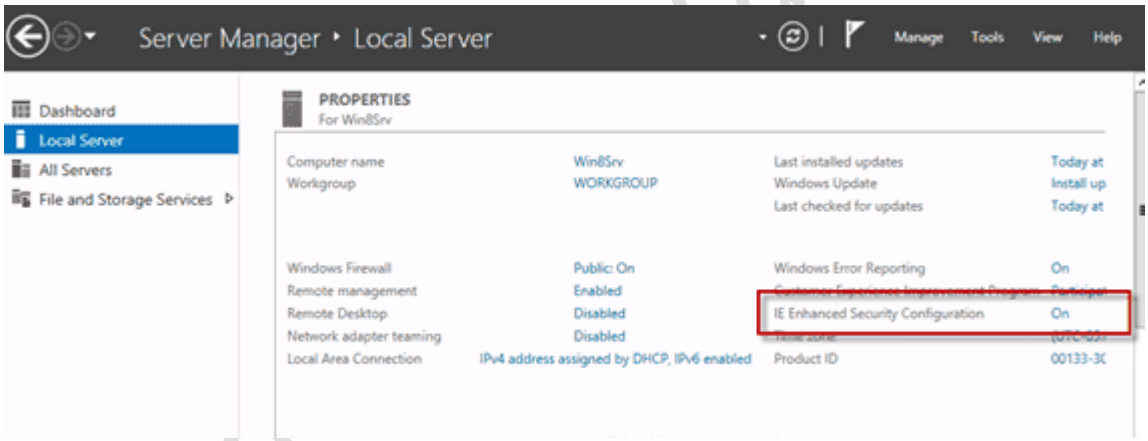
1. Under **Active Directory Users and Computers**, expand your domain and click the **Users** container
2. In the right pane, right click your domain name, select **New,** select **User** from the menu.
3. In the *New Object – User* dialog, enter a *First name*, *Last name*, *User logon name* and then click **Next**.
4. Type and confirm a password, then click **Next**.

Part H: Create new Group in Windows Active Directory

1. Under **Active Directory Users and Computers**, expand your domain and click the **Users** container
2. In the right pane, right click your domain name, select **New,** select **Group** from the menu.
3. In the *New Object – Group* dialog, enter a *group name* and then press OK.

Part I: Install Azure AD Connect in Windows Active Directory

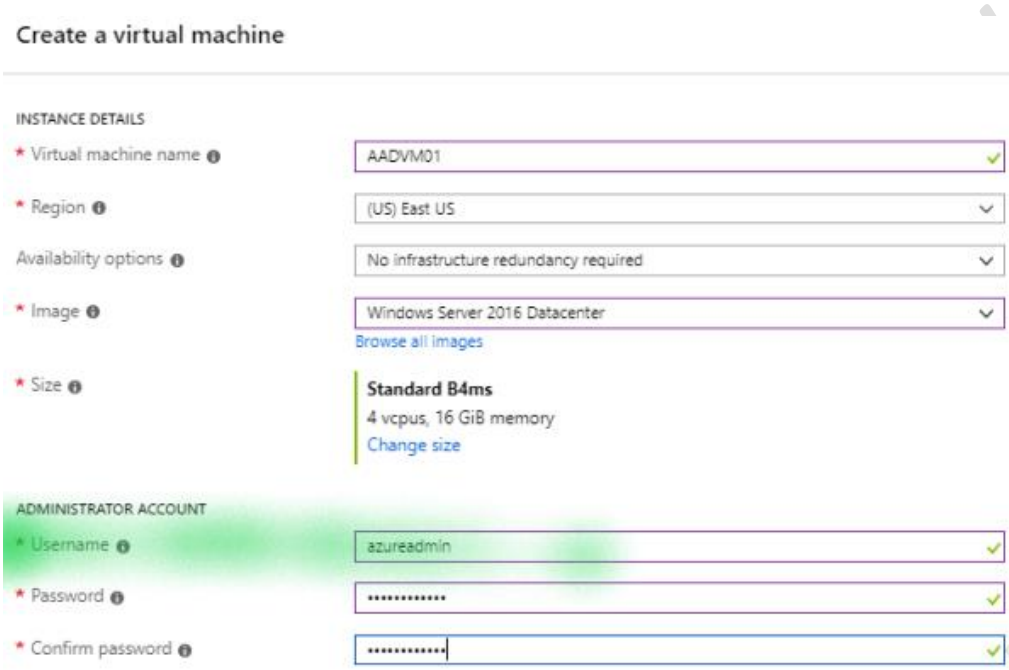
1. Right click on "***Start***" & "***Run***". In the open, write "**Servermanager.exe**"
2. Go to "***Local Server***"
3. Select "***IE Enhanced Security Configuration***" & Select off for "***Administrator***"



4. Open https://www.microsoft.com/en-us/download/details.aspx?id=47594
5. Download & Install "***Azure AD Connect***"
6. Start Microsoft Azure Active Directory Connect wizard, accept the licensing terms and select continue
7. Select Express Settings
8. When prompted to connect to Azure AD, authenticate by using the credentials of the *adconnect* (like, ad*connect@domainname.com)***,*** created in the Part A, Step 3.b

9. When prompted to connect your directories, add the windows active directory administrator name, and authenticate by using the following credentials:
    a. User name: YOURDOMAIN.com\Your-Login-ID
    b. Password: Your Password

    Note: Your Login Id & Password is the same credentials, which you have created at the time of creating the VM



10. On the Azure AD sign-in configuration page, select "***continue without any verified domain***"

11. Close the Microsoft Azure Active Directory Connect window once the configuration is completed.

Part J: Verified Directory Synchronisation

1. Sign-in to the Azure Portal use **root administrative credentials**.

2. Go to the left-side, select "***Azure Active Directory***"

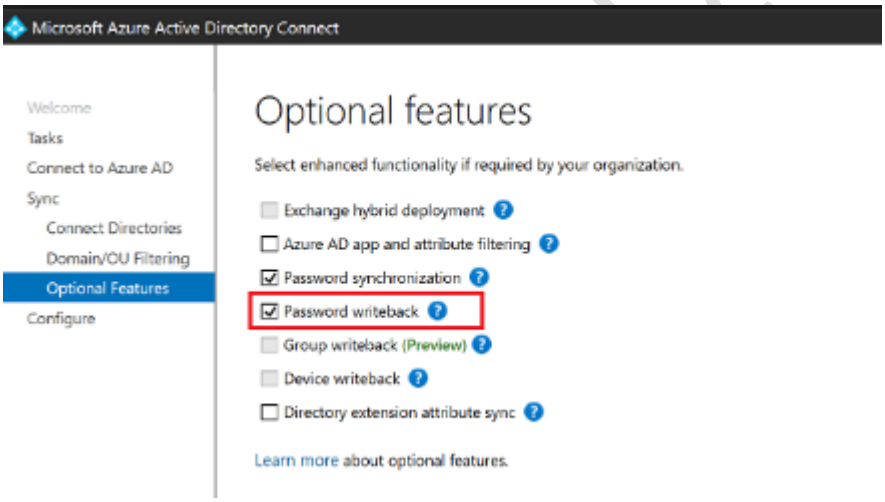
3. Under the manage, select the "***User***", note that the list of user objects includes the users account, with the Windows Server AD appearing in the source column.

4. Under the manage, select the "***Groups***", note that the list of groups account, with the Windows Server AD appearing in the source column.

Part K: Enable Password Writeback

To enable password writeback you need to enable the feature from the server that you have installed Azure AD Connect on.

1. To configure and enable password writeback, sign-in to your Azure AD Connect server and start the **Azure AD Connect** configuration wizard.
2. On the **Welcome** page, select **Configure**.
3. On the **Additional tasks** page, select **Customize synchronization options**, and then select **Next**.
4. On the **Connect to Azure AD** page, enter a global administrator credential, and then select **Next**.
5. On the **Connect directories** and **Domain/OU** filtering pages, select **Next**.
6. On the **Optional features** page, select the box next to **Password writeback** and select **Next**.



7. On the **Ready to configure** page, select **Configure** and wait for the process to finish.
8. When you see the configuration finish, select **Exit**.