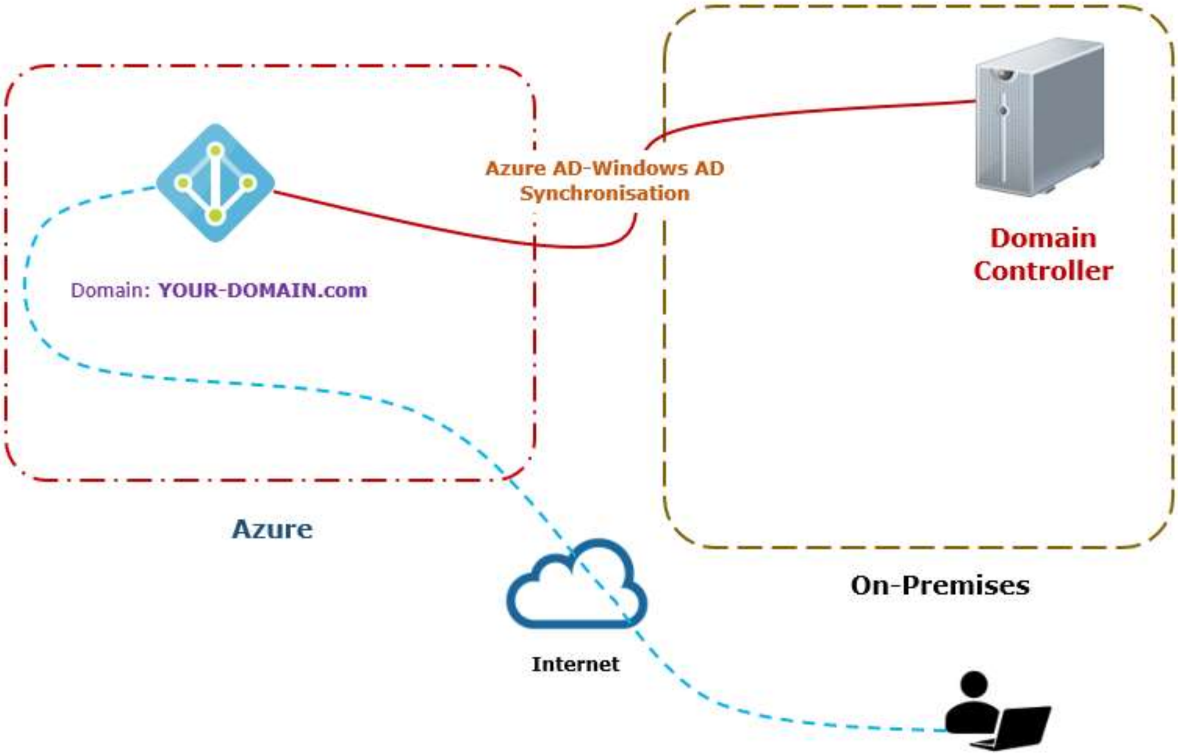
Azure AD Password Hash Synchronization (Portal)

(LAB-103-09-02)



Step 1: Create Windows 2016 Virtual Machine

1. Enable the **Azure Cloud Shell**
2. **Copy** & **execute** the PowerShell Script from Azure Cloud Shell.

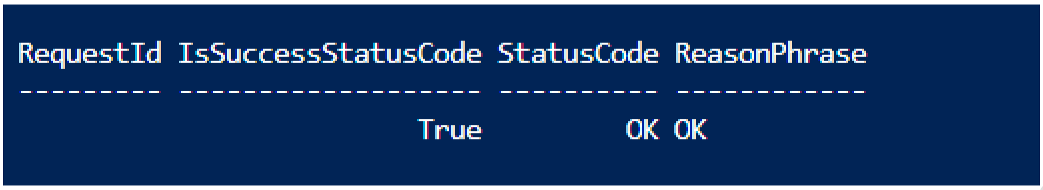
This script creates:

a. Resources group: **RG-103-09-02**
b. Location: **East US**
c. Virtual machine:
   i. **OnP-DC01** [Windows 2016 Data Centre]
d. Virtual network: **OnP-VNeT**

Info: When prompt for username & password, provide below details
Username: **master**
Password: **Lab@password**

Note: PowerShell script **LAB-103-09-02-PowerShell-Script-Deploy-Domain Controller**.txt is provided with the lab manual

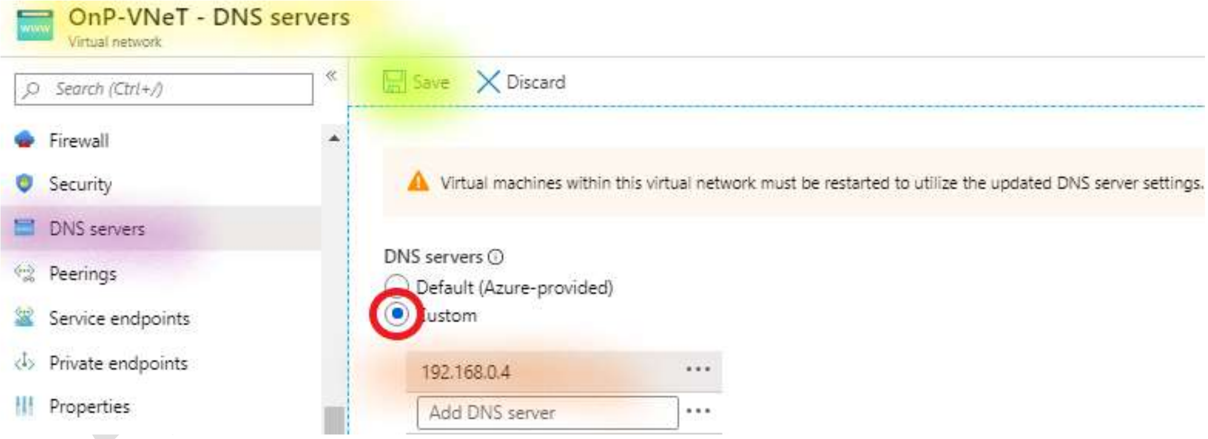
Note: Once PowerShell script executed successfully, you will get below output.



```
RequestId IsSuccessStatusCode StatusCode ReasonPhrase
--------- ------------------- ---------- ------------
                         True         OK OK
```

Step 2: Update the DNS for Windows Server

1. From the Azure Portal, go to the left menu, select **Virtual machine**
2. Open the **OnP-DC01** virtual machine
3. Copy the **Private IP address** of **OnP-DC01** virtual machine
4. From the Azure Portal, go to the left menu, select **Virtual network**
5. Open the **Onp-VNeT** virtual network
6. Open the **DNS Servers**, under **settings**
7. Select the **Custom**, under **DNS servers**
8. Provide the **Private IP address** of **OnP-DC01** virtual machine
9. Select **Save**



Virtual machines within this virtual network must be restarted to utilize the updated DNS server settings.

DNS servers

○ Default (Azure-provided)

● Custom

192.168.0.4

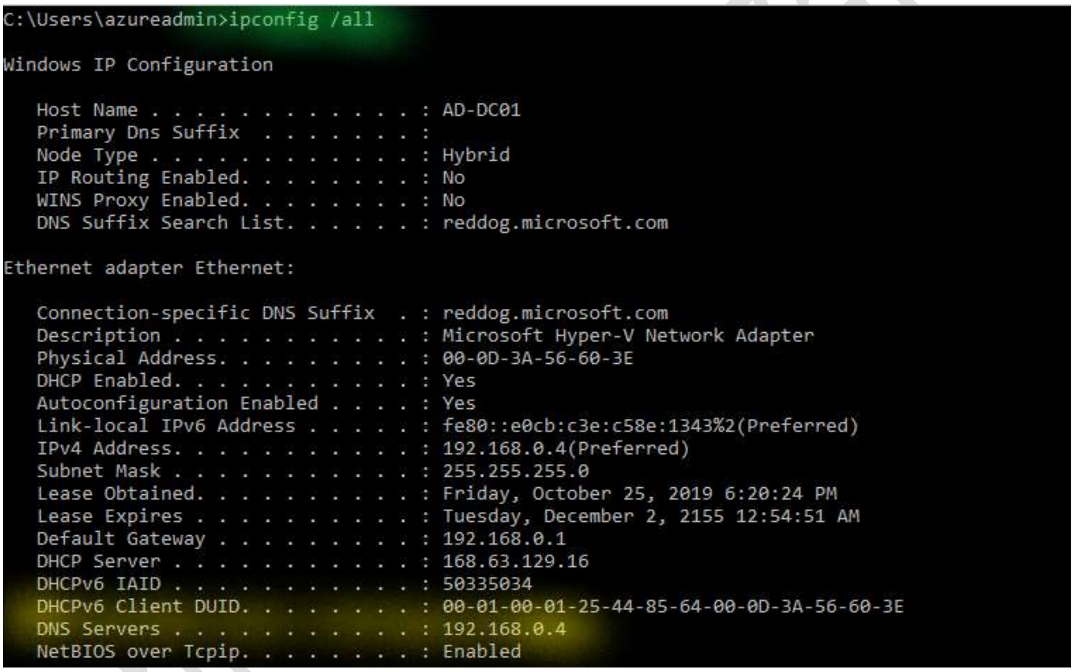
Add DNS server

10. From the Azure Portal, **go to the left menu**, select **Virtual machine**
11. Select the **OnP-DC01** virtual machine
12. **Restart** the virtual machine

Step 3: Install Windows Active Directory

1. From the Azure Portal, **go to the left menu**, select **Virtual machine**
2. Open the **OnP-DC01** virtual machine
3. Copy the **Public IP address** of **OnP-DC01** virtual machine
4. Login into **OnP-DC01** virtual machine via **RDP**
5. From the **OnP-DC01** virtual machine, Go to **Start** menu, right click on **Start** & **Run**.
6. In the open, **write cmd**
7. From the command line, Write **ipconfig /all**

Note: Here you will the **DNS server** pointing to the **Private IP address** of **ONP-DC01** virtual machine.



```
C:\Users\azureadmin>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : AD-DC01
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : reddog.microsoft.com

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : reddog.microsoft.com
   Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Physical Address. . . . . . . . . : 00-0D-3A-56-60-3E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::e0cb:c3e:c58e:1343%2(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.4(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, October 25, 2019 6:20:24 PM
   Lease Expires . . . . . . . . . . : Tuesday, December 2, 2155 12:54:51 AM
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 168.63.129.16
   DHCPv6 IAID . . . . . . . . . . . : 50335034
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-44-85-64-00-0D-3A-56-60-3E
   DNS Servers . . . . . . . . . . . : 192.168.0.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

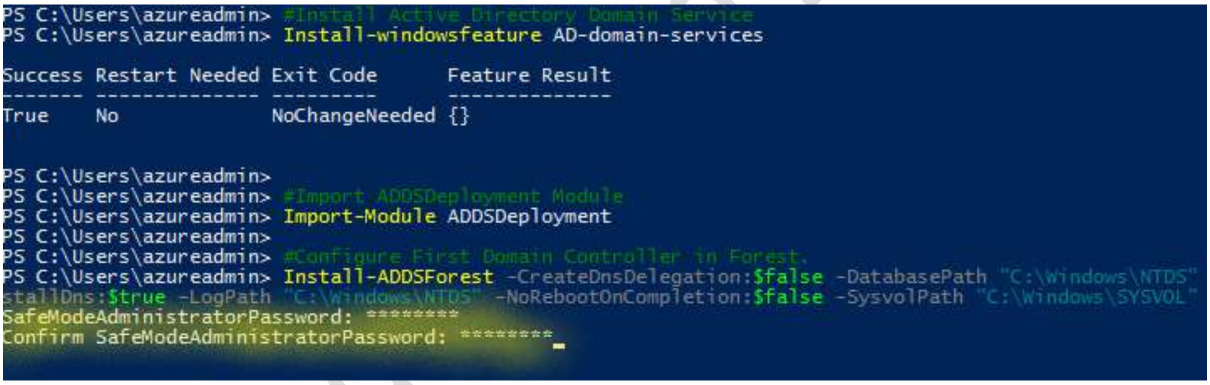
8. From the **OnP-DC01** virtual machine, Go to **Start** menu, right click on **Start** & **Run**
9. In the open, **write PowerShell.exe**
10. **Copy** & **execute** the PowerShell Script

Note: PowerShell script **LAB-103-09-02_PowerShell_Script_Install Active Directory**.txt is provided with the lab manual.

```
#Install Active Directory Domain Service
Install-windowsfeature AD-domain-services -includemanagementtools

#Import ADDSDeployment Module
Import-Module ADDSDeployment

#Configure First Domain Controller in Forest.
Install-ADDSForest -CreateDnsDelegation:$false -DatabasePath "C:\Windows\NTDS" -
DomainMode "7" -DomainName "YOUR-DOMAIN.COM " -DomainNetbiosName "YOUR-
DOMAIN" -ForestMode "7" -InstallDns:$true -LogPath "C:\Windows\NTDS" -
NoRebootOnCompletion:$false -SysvolPath "C:\Windows\SYSVOL" -Force:$true

#End
```

Note: Replace **YOUR-DOMAIN.com** and **YOUR-DOMAIN** with you Domain Name (Like **ahmadmz.cf** and **ahmadmz)**.

Info: When prompt for Safe mode administrator password, provide below details.
Password: **Password@123**



```
PS C:\Users\azureadmin> #Install Active Directory Domain Service
PS C:\Users\azureadmin> Install-windowsfeature AD-domain-services

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             NoChangeNeeded {}


PS C:\Users\azureadmin>
PS C:\Users\azureadmin> #Import ADDSDeployment Module
PS C:\Users\azureadmin> Import-Module ADDSDeployment
PS C:\Users\azureadmin>
PS C:\Users\azureadmin> #Configure First Domain Controller in Forest.
PS C:\Users\azureadmin> Install-ADDSForest -CreateDnsDelegation:$false -DatabasePath "C:\Windows\NTDS"
stallDns:$true -LogPath "C:\Windows\NTDS" -NoRebootOnCompletion:$false -SysvolPath "C:\Windows\SYSVOL"
SafeModeAdministratorPassword: ********
Confirm SafeModeAdministratorPassword: ********_
```

Note: Once Windows Active Directory Installed successfully, virtual machine restart automatically.

Step 4: Create Windows Active Directory Users and Groups

1. Login into **OnP-DC01** virtual machine via **RDP**
   a. Username: **master**
   b. Password: **Lab@password**
2. From the **ONP-DC01** virtual machine, Go to **Start** menu, right click on **Start** & **Run**
3. In the open, **write PowerShell.exe**

4. **Copy** & **execute** the PowerShell Script

Note: PowerShell script **LAB-103-09-02_PowerShell_Script_Create OU, AD Users and Groups**.txt is provided with the lab manual.

This script creates:

a. OU: **Lab103-AD-OU**

b. Groups: **OnPGroup01** and **OnPGroup02**

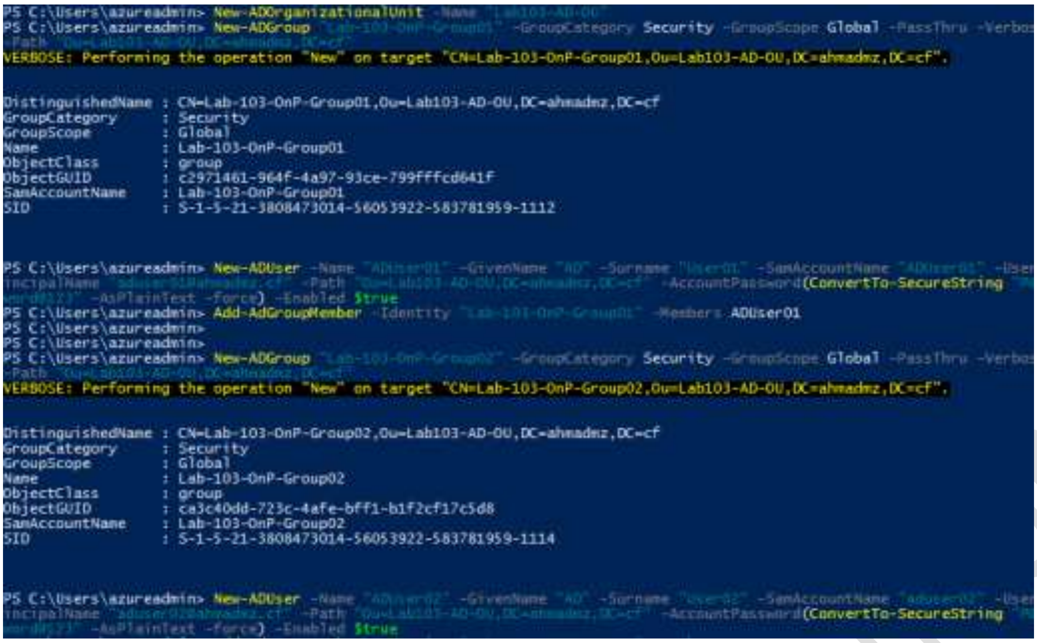
c. Users: **OnPUser01** and **OnPUser02**

d. Users Password: **P@ssword@123**

e. Group Members: **OnPUser01** in **OnPGroup01** and **OnPUser02** in **OnPGroup02**

```
#Create Organisational Unit
New-ADOrganizationalUnit -Name "Lab103-AD-OU"

#Create Group-1 in Organisational Unit
New-ADGroup "OnPGroup01" -GroupCategory Security -GroupScope Global -PassThru –Verbose -Path
"Ou=Lab103-AD-OU,DC=YOUR-DOMAIN,DC=com"

#Create User-1 in Organisational Unit
New-ADUser -Name "OnPUser01" -GivenName "OnP" -Surname "User01" -SamAccountName "OnPUser01" -
UserPrincipalName "onpser01@YOUR-DOMAIN.com" -Path "Ou=Lab103-AD-OU,DC=YOUR-DOMAIN,DC=com" -
AccountPassword(ConvertTo-SecureString "P@ssword@123" -AsPlainText -force) -Enabled $true

#Add User-1 in Group-1
Add-AdGroupMember -Identity "OnPGroup01" -Members OnPUser01

#Create Group-2 in Organisational Unit
New-ADGroup "OnPGroup02" -GroupCategory Security -GroupScope Global -PassThru –Verbose -Path
"Ou=Lab103-AD-OU,DC=YOUR-DOMAIN,DC=com"

#Create User-2 in Organisational Unit
New-ADUser -Name "OnPUser02" -GivenName "OnP" -Surname "User02" -SamAccountName "OnPUser02" -
UserPrincipalName "onpser02@YOUR-DOMAIN.com" -Path "Ou=Lab103-AD-OU,DC=YOUR-DOMAIN,DC=com" -
AccountPassword(ConvertTo-SecureString "P@ssword@123" -AsPlainText -force) -Enabled $true

#Add User-2 in Group-2
Add-AdGroupMember -Identity "OnPGroup02" -Members OnPUser02

#End
```

Note: Replace **YOUR-DOMAIN.com** with you Domain Name. Like **ahmadmz.cf.**



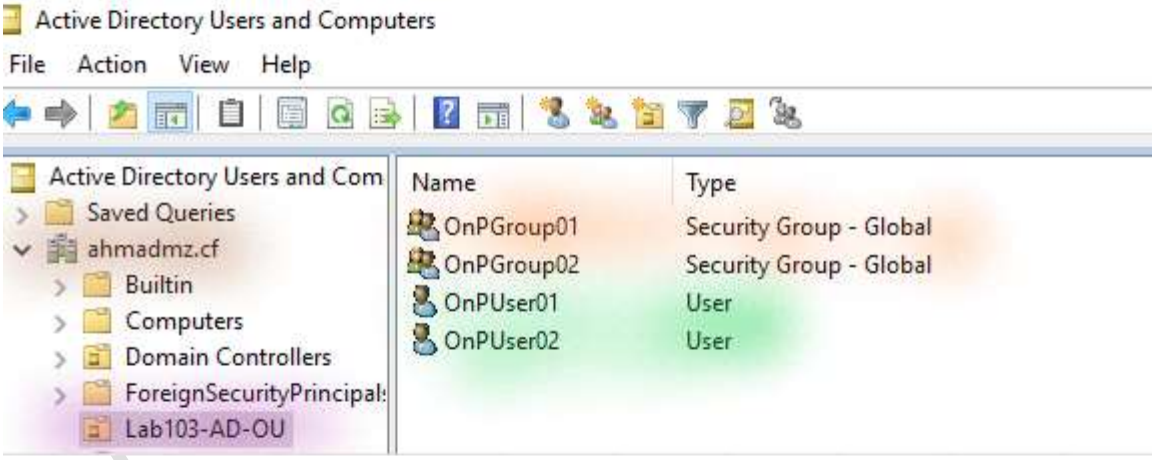
```
PS C:\Users\azureadmin> New-ADOrganizationalUnit -Name "Lab103-AD-OU"
PS C:\Users\azureadmin> New-ADGroup "Lab-103-OnP-Group01" -GroupCategory Security -GroupScope Global -PassThru -Verbos
-Path "Ou=Lab103-AD-OU,DC=ahmadmz,DC=cf"
VERBOSE: Performing the operation "New" on target "CN=Lab-103-OnP-Group01,Ou=Lab103-AD-OU,DC=ahmadmz,DC=cf".


DistinguishedName : CN=Lab-103-OnP-Group01,Ou=Lab103-AD-OU,DC=ahmadmz,DC=cf
GroupCategory     : Security
GroupScope        : Global
Name              : Lab-103-OnP-Group01
ObjectClass       : group
ObjectGUID        : c2971461-964f-4a97-93ce-799fffcd641f
SamAccountName    : Lab-103-OnP-Group01
SID               : S-1-5-21-3808473014-56053922-583781959-1112



PS C:\Users\azureadmin> New-ADUser -Name "ADUser01" -GivenName "AD" -Surname "User01" -SamAccountName "ADUser01" -User
incipalName "aduser01@ahmadmz.cf" -Path "Ou=Lab103-AD-OU,DC=ahmadmz,DC=cf" -AccountPassword(ConvertTo-SecureString "Pa
word@123" -AsPlainText -force) -Enabled $true
PS C:\Users\azureadmin> Add-AdGroupMember -Identity "Lab-103-OnP-Group01" -Members ADUser01
PS C:\Users\azureadmin>
PS C:\Users\azureadmin>
PS C:\Users\azureadmin> New-ADGroup "Lab-103-OnP-Group02" -GroupCategory Security -GroupScope Global -PassThru -Verbos
-Path "Ou=Lab103-AD-OU,DC=ahmadmz,DC=cf"
VERBOSE: Performing the operation "New" on target "CN=Lab-103-OnP-Group02,Ou=Lab103-AD-OU,DC=ahmadmz,DC=cf".


DistinguishedName : CN=Lab-103-OnP-Group02,Ou=Lab103-AD-OU,DC=ahmadmz,DC=cf
GroupCategory     : Security
GroupScope        : Global
Name              : Lab-103-OnP-Group02
ObjectClass       : group
ObjectGUID        : ca3c40dd-723c-4afe-bff1-b1f2cf17c5d8
SamAccountName    : Lab-103-OnP-Group02
SID               : S-1-5-21-3808473014-56053922-583781959-1114



PS C:\Users\azureadmin> New-ADUser -Name "ADUser02" -GivenName "AD" -Surname "User02" -SamAccountName "aduser02" -User
incipalName "aduser02@ahmadmz.cf" -Path "Ou=Lab103-AD-OU,DC=ahmadmz,DC=cf" -AccountPassword(ConvertTo-SecureString "Pa
word@123" -AsPlainText -force) -Enabled $true
```

5. From the **OnP-DC01** virtual machine, Go to **Start** menu, right click on **Start** & **Run**

6. In the open, **write dsa.msc** (Active Directory Users and Computers)

7. Expand **YOUR-DOMAIN.com** and select the **Lab103-AD-OU** Organisational Unit

   Note: Here you can see the Groups & Users created via PowerShell.



Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
ahmadmz.cf
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Lab103-AD-OU

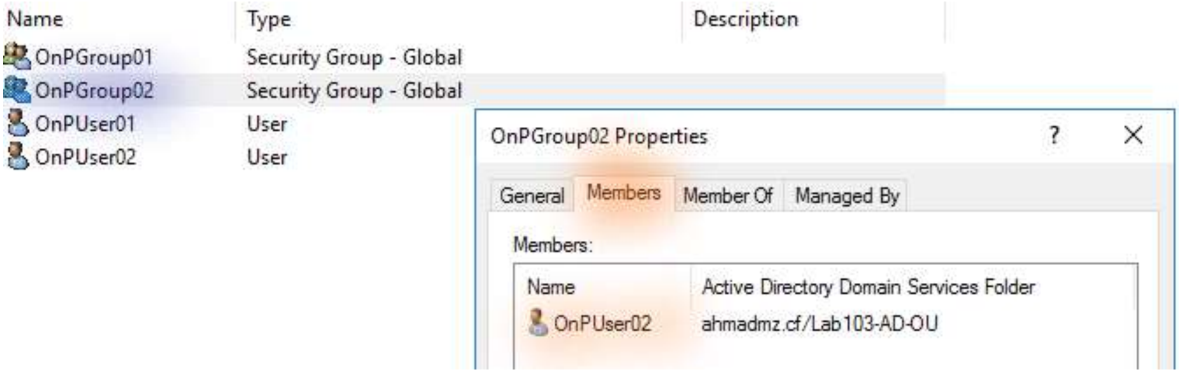
Name	Type
OnPGroup01	Security Group - Global
OnPGroup02	Security Group - Global
OnPUser01	User
OnPUser02	User

8. Open the **OnPGroup01** and click on the **Members**

   Note: Here you can see the **OnPUser01** added in the Group.

9. Open the **OnPGroup02** and click on the **Members**

   Note: Here you can see the **OnPUser02** added in the Group.



Name	Type	Description
OnPGroup01	Security Group - Global	
OnPGroup02	Security Group - Global	
OnPUser01	User	
OnPUser02	User	

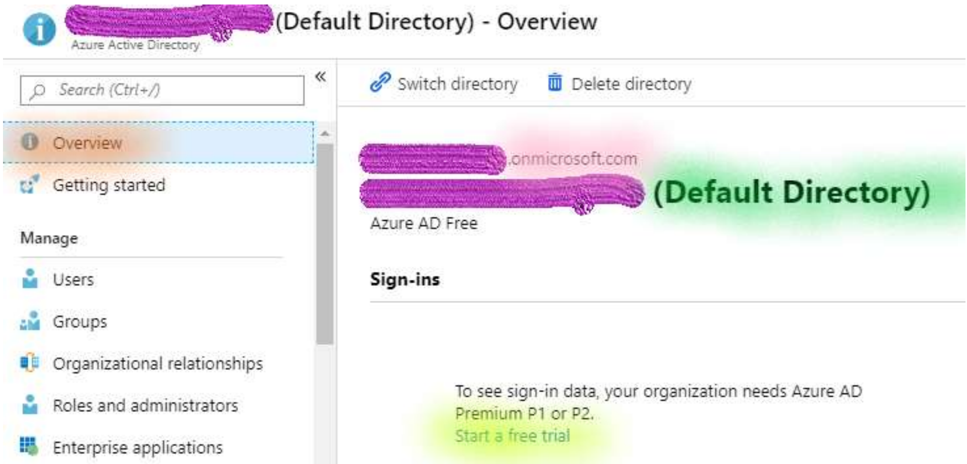
Members:

Name	Active Directory Domain Services Folder
OnPUser02	ahmadmz.cf/Lab103-AD-OU

Step 5: Create Azure AD User with Global Administrator Privileges

I. Identify your Azure AD Domain name

1. Go to the left-side, select **Azure Active Directory**
2. Under the **Overview**, check your **default directory domain name**



[redacted](Default Directory) - Overview

[redacted].onmicrosoft.com

[redacted] (Default Directory)

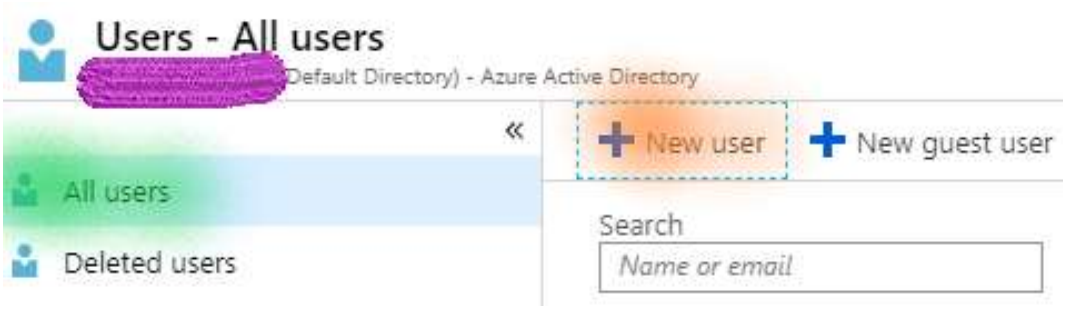
Azure AD Free

Sign-ins

To see sign-in data, your organization needs Azure AD Premium P1 or P2.
Start a free trial

II. Create Azure AD User with Administrator Privileges

1. Select the **Users**, under the **manage**
2. Select **New user**



Users - All users

[redacted] Default Directory) - Azure Active Directory

3. Select **Create user** & fill out the required information:

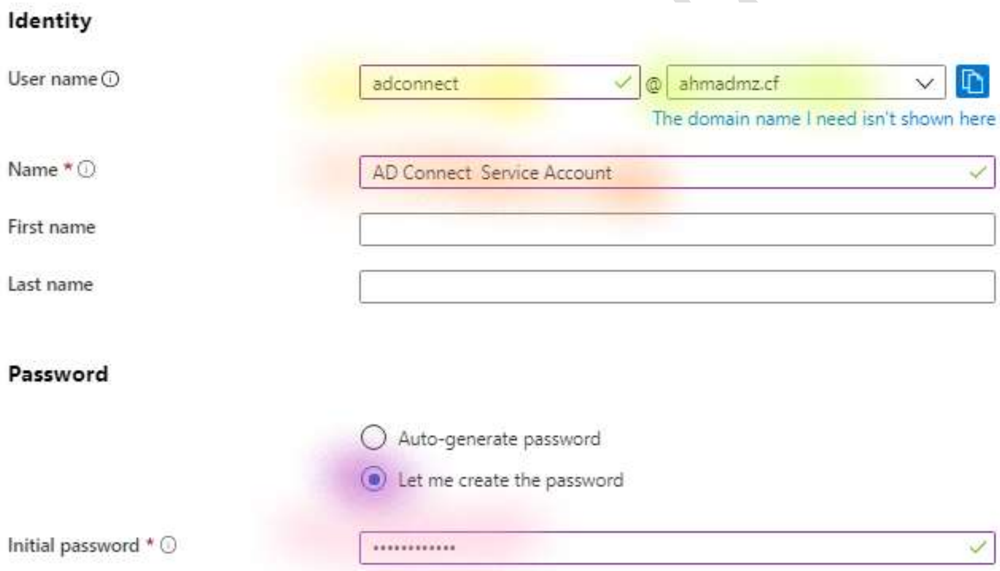
   a. **User Name: Provide username adconnect**

      Note: You can see your Azure AD default directory domain name are showing after **@**

   b. **Name:** Provide name of the new user **AD Connect Service Account**

   c. Select **Let me create the password**

      i. Provide the Password as **P@ssword@123**



Identity

User name ⓘ: adconnect ✓ @ ahmadmz.cf

The domain name I need isn't shown here

Name * ⓘ: AD Connect Service Account ✓

First name:

Last name:

Password

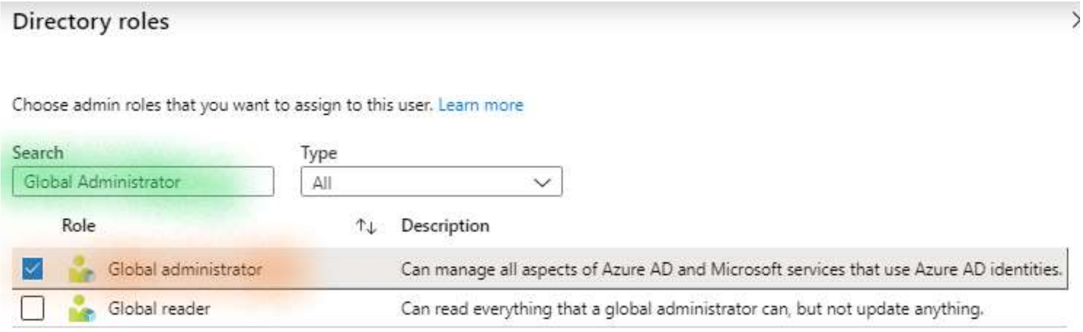
○ Auto-generate password

● Let me create the password

Initial password * ⓘ: •••••••••••• ✓

   d. **Roles**: Select **Users**

      i. Search and Select **Global Administrator**



Directory roles

Choose admin roles that you want to assign to this user. Learn more

Search: Global Administrator

Type: All

	Role	Description
☑	Global administrator	Can manage all aspects of Azure AD and Microsoft services that use Azure AD identities.
☐	Global reader	Can read everything that a global administrator can, but not update anything.

4. Select **Create**

Step 6: Sign-in using Azure AD using ADCONNECT

1. Open the below URL from **new browser**

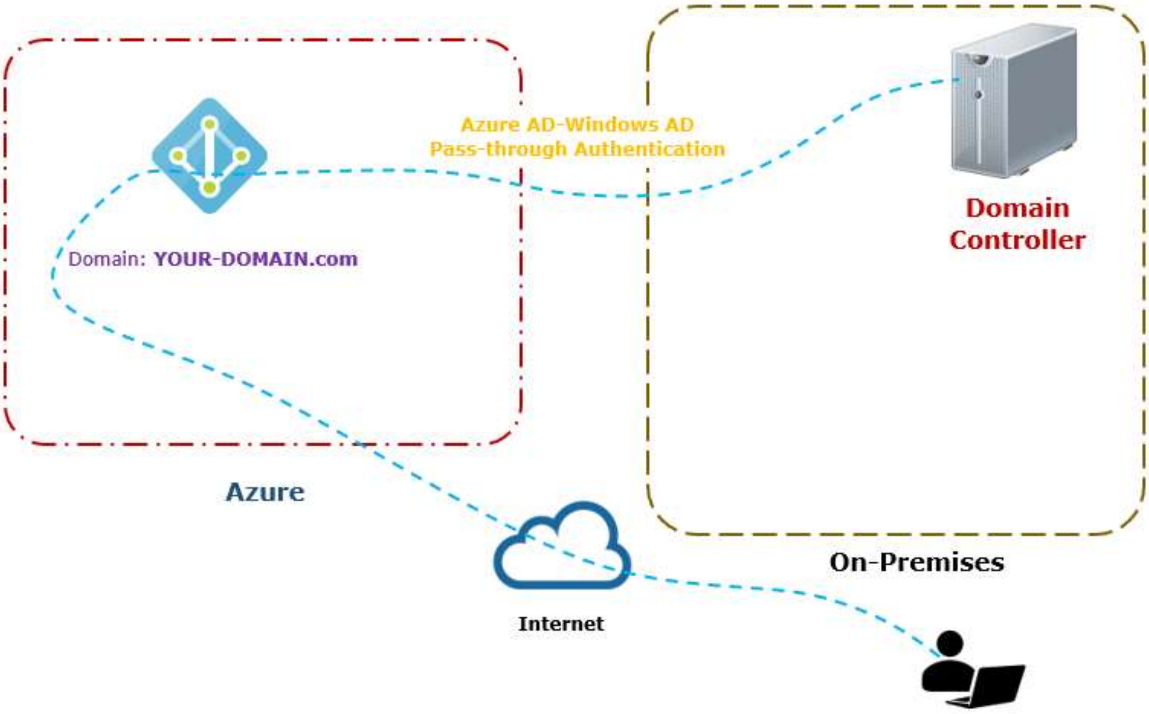
   portal.azure.com

2. Login with Azure AD Id **adconnect@<YOUR-AD-DOMAIN.com>** and password **P@ssword@123**

   Note: Replace **YOUR-AD-DOMAIN.com** with you Azure AD Domain Name. Like **ahmadmz.cf.**

3. While logged-in, it will ask to change the Password. Change the **password of adconnect** Azure AD User

Step 7: Install Azure AD Connect in OnP-DC01



1. From the **OnP-DC01** virtual machine, Go to **Start** menu, right click on **Start** & **Run**
2. In the open, **write powershell.exe**
3. From the **powershell**, write below command to Disable IE Enhanced Security Configuration to allow file download

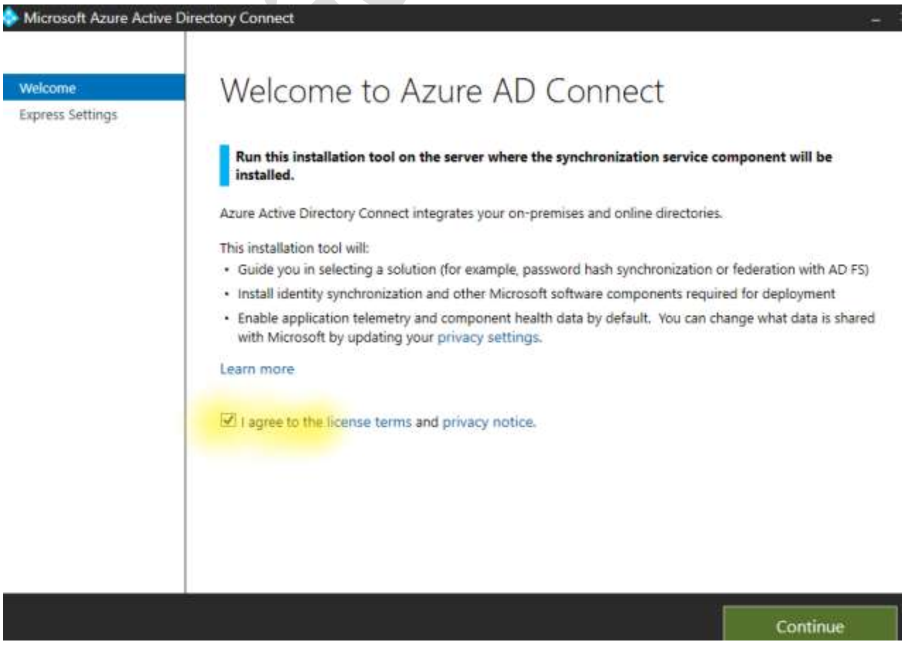
```
function Disable-InternetExplorerESC {
   $AdminKey = "HKLM:\SOFTWARE\Microsoft\Active Setup\Installed Components\{A509B1A7-37EF-4b3f-8CFC-
4F3A74704073}"
   $UserKey = "HKLM:\SOFTWARE\Microsoft\Active Setup\Installed Components\{A509B1A8-37EF-4b3f-8CFC-
4F3A74704073}"
   Set-ItemProperty -Path $AdminKey -Name "IsInstalled" -Value 0
   Set-ItemProperty -Path $UserKey -Name "IsInstalled" -Value 0
   Stop-Process -Name Explorer
   Write-Host "IE Enhanced Security Configuration (ESC) has been disabled." -ForegroundColor Green
}

Disable-InternetExplorerESC
```

4. Open the below URL to download the **Microsoft Azure Active Directory Connect**

   https://www.microsoft.com/en-us/download/details.aspx?id=47594

5. Install the **Microsoft Azure Active Directory Connect**

   1. Enable **I agree ....**
   2. Select **Continue**



Welcome to Azure AD Connect

Run this installation tool on the server where the synchronization service component will be installed.

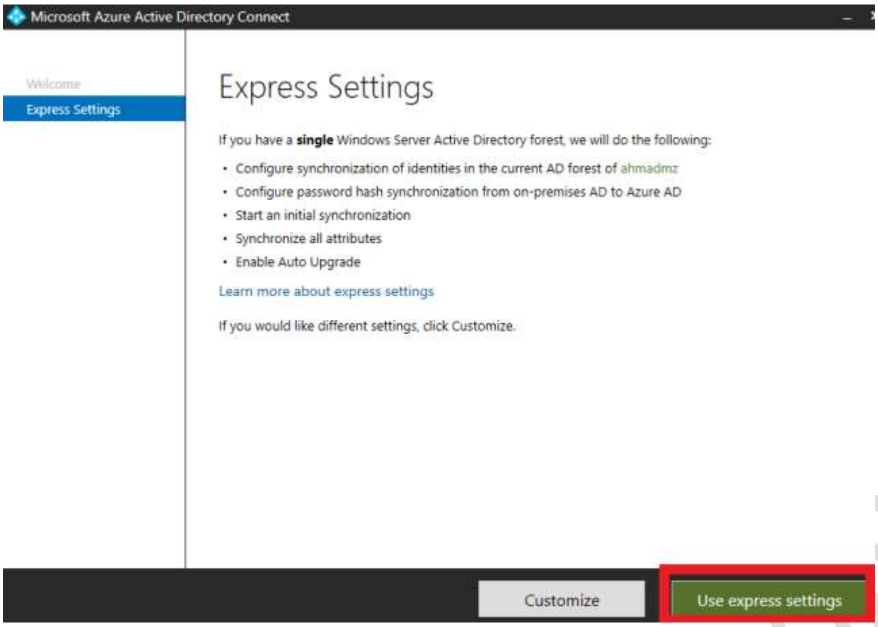
Azure Active Directory Connect integrates your on-premises and online directories.

This installation tool will:
- Guide you in selecting a solution (for example, password hash synchronization or federation with AD FS)
- Install identity synchronization and other Microsoft software components required for deployment
- Enable application telemetry and component health data by default. You can change what data is shared with Microsoft by updating your privacy settings.

Learn more

☑ I agree to the license terms and privacy notice.

3. Select **Use express setting**



Microsoft Azure Active Directory Connect

Express Settings

If you have a **single** Windows Server Active Directory forest, we will do the following:

- Configure synchronization of identities in the current AD forest of ahmadmz
- Configure password hash synchronization from on-premises AD to Azure AD
- Start an initial synchronization
- Synchronize all attributes
- Enable Auto Upgrade

Learn more about express settings

If you would like different settings, click Customize.

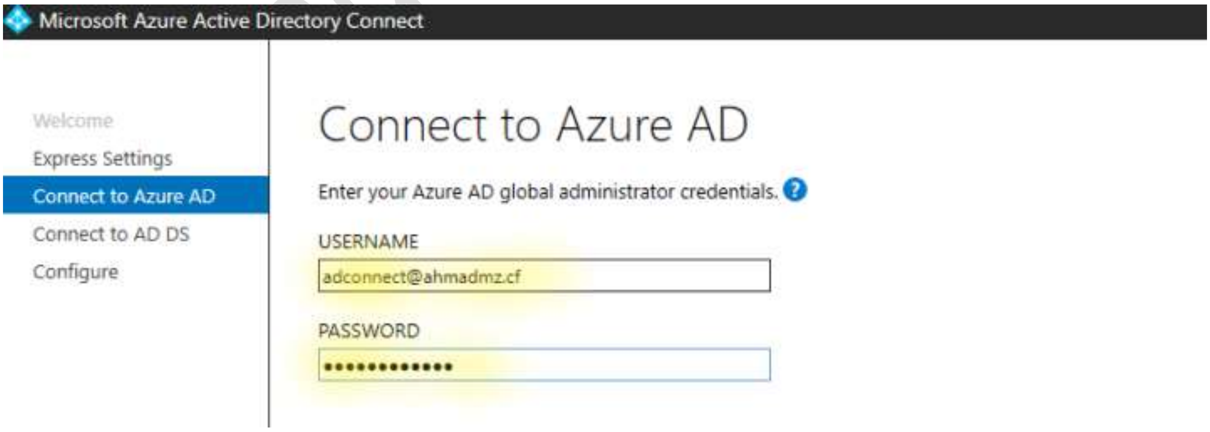
4. In **Connect to Azure AD**, provide the below details:

   i. **Username**: Provide **adconnect@<YOUR-AD-DOMAIN.com>**

   Note: Replace **YOUR-AD-DOMAIN.com** with you Azure AD Domain Name. Like **ahmadmz.cf**.

   ii. **Password**: Provide your **password**

   iii. Select **Next**



Microsoft Azure Active Directory Connect

Connect to Azure AD

Enter your Azure AD global administrator credentials.

USERNAME
adconnect@ahmadmz.cf

PASSWORD
•••••••••••••

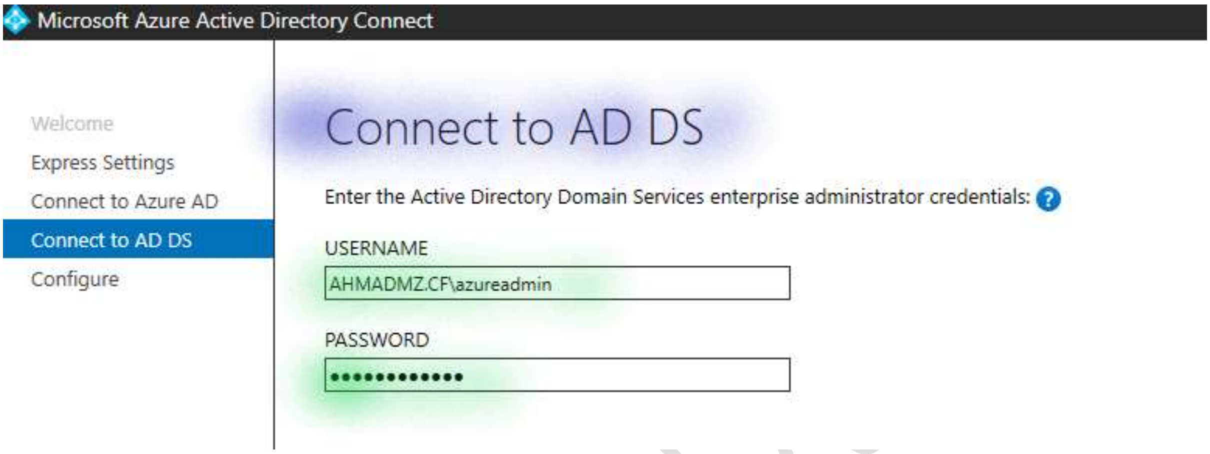
5. In **Connect to AD DS**, provide the below details:

   i. **Username**: Provide **<YOUR-AD-DS-DOMAIN.com>\master**

Note: Replace **YOUR-AD-DS-DOMAIN.com** with you Windows Active Directory Domain Name. Like **ahmadmz.cf**.

ii. **Password**: Provide password **Lab@password**

iii. Select **Next**



Connect to AD DS

Enter the Active Directory Domain Services enterprise administrator credentials:

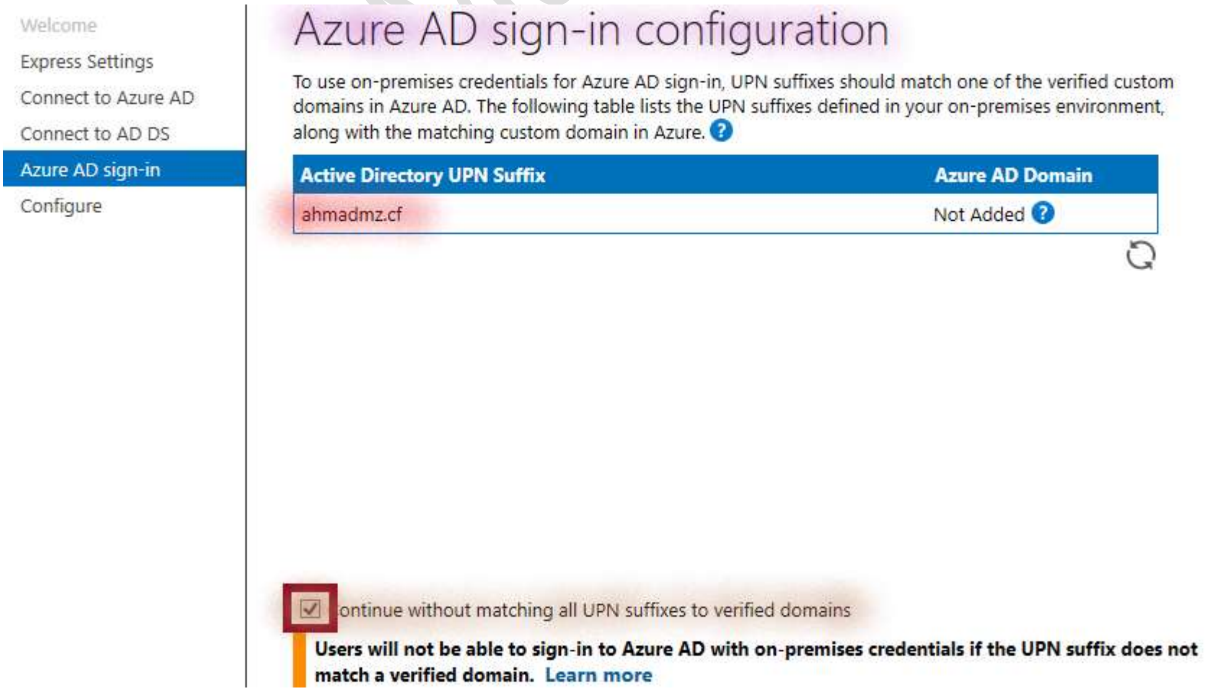
USERNAME: AHMADMZ.CF\azureadmin

PASSWORD: •••••••••••••

6. (**Optional**) If your Domain name is not verified, you get below option.

   i. Enable **Continue without matching all UPN……**

   ii. Select **Next**



Azure AD sign-in configuration

To use on-premises credentials for Azure AD sign-in, UPN suffixes should match one of the verified custom domains in Azure AD. The following table lists the UPN suffixes defined in your on-premises environment, along with the matching custom domain in Azure.

Active Directory UPN Suffix	Azure AD Domain
ahmadmz.cf	Not Added

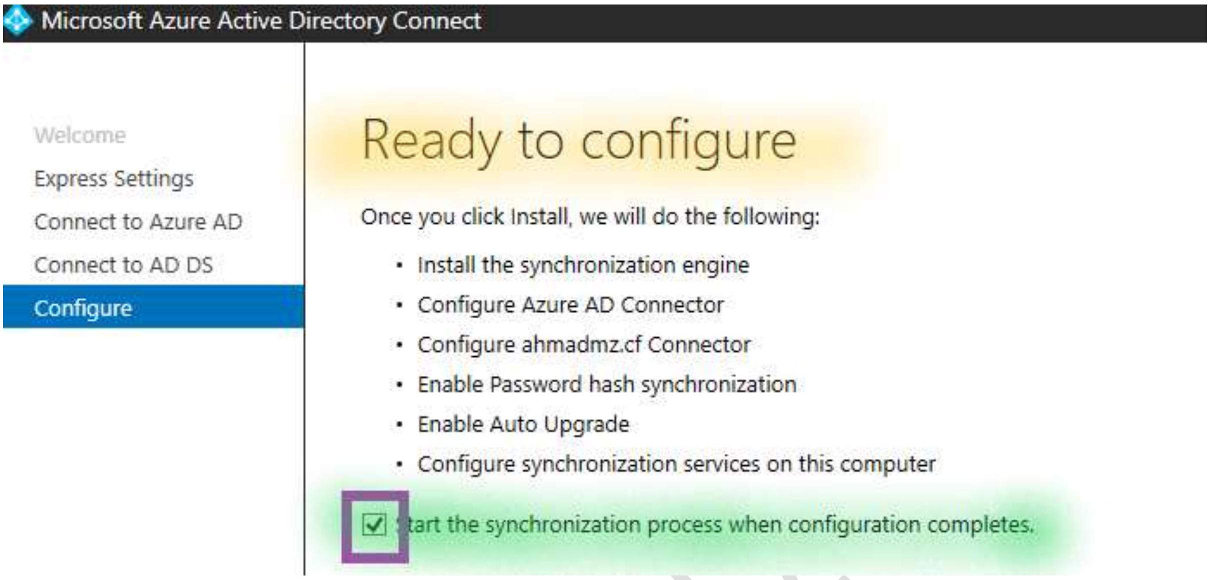
☑ Continue without matching all UPN suffixes to verified domains

Users will not be able to sign-in to Azure AD with on-premises credentials if the UPN suffix does not match a verified domain. Learn more

7. In **Ready to configure**, provide the below details:

i. Enable **Start the synchronisation ………….**

ii. Select **Next**



Ready to configure

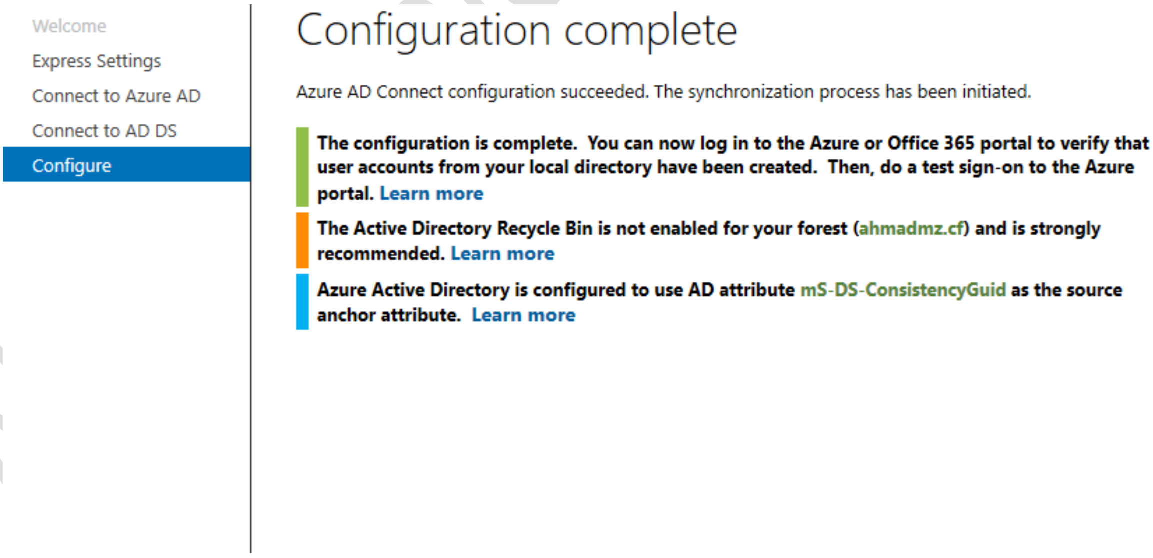
Once you click Install, we will do the following:

- Install the synchronization engine
- Configure Azure AD Connector
- Configure ahmadmz.cf Connector
- Enable Password hash synchronization
- Enable Auto Upgrade
- Configure synchronization services on this computer

☑ Start the synchronization process when configuration completes.

8. Once configuration completed, you will get the below message:

i. Press **Exit**



Configuration complete

Azure AD Connect configuration succeeded. The synchronization process has been initiated.

The configuration is complete. You can now log in to the Azure or Office 365 portal to verify that user accounts from your local directory have been created. Then, do a test sign-on to the Azure portal. Learn more

The Active Directory Recycle Bin is not enabled for your forest (ahmadmz.cf) and is strongly recommended. Learn more

Azure Active Directory is configured to use AD attribute mS-DS-ConsistencyGuid as the source anchor attribute. Learn more

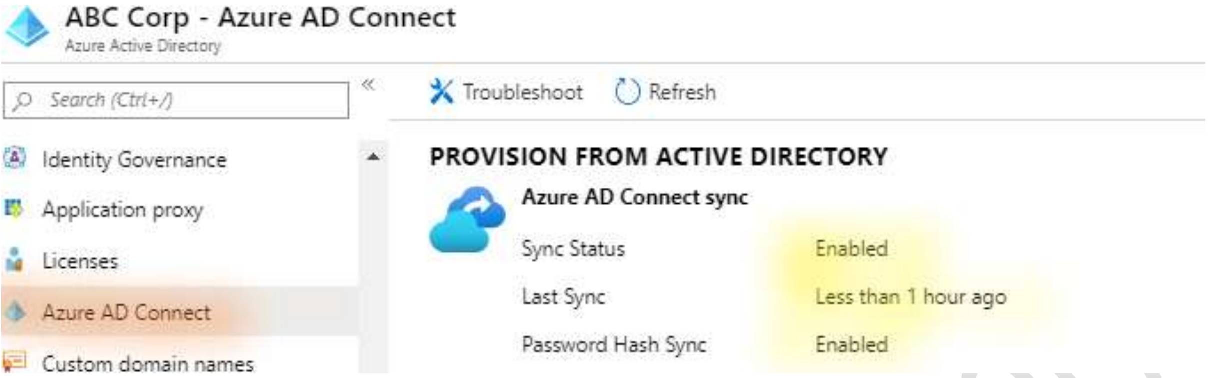
Step 8: Verify Directory Synchronisation

I. Check from Azure AD Connect

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

2. Select **Azure AD Connect**, under **manage**

Note: Here you will see Password Hash Sync is enabled.



PROVISION FROM ACTIVE DIRECTORY

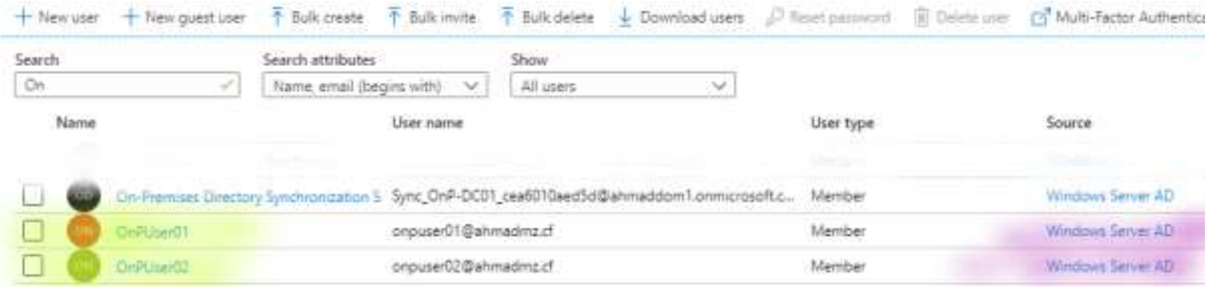
Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

II. **Verify the Windows AD users in Azure AD**

1. Go to the left-side, select **Azure Active Directory**
2. Select **Users**, under **manage**

Note: Here you will see the Windows AD users.



Search: On

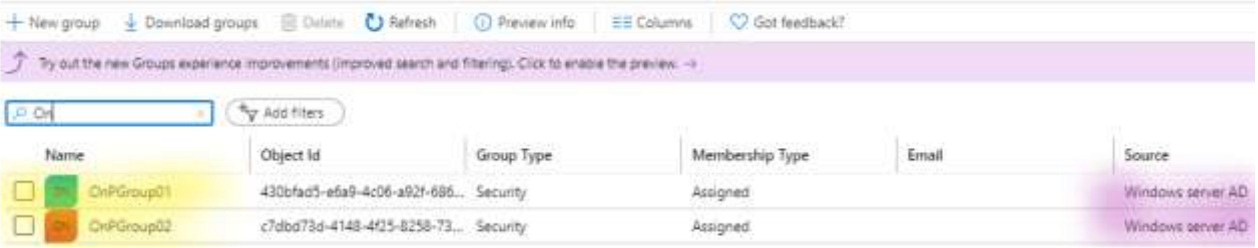
Search attributes: Name, email (begins with)

Show: All users

	Name	User name	User type	Source
□	On-Premises Directory Synchronization S	Sync_OnP-DC01_cea6010aed5d@ahmaddom1.onmicrosoft.c...	Member	Windows Server AD
□	OnPUser01	onpuser01@ahmadmz.cf	Member	Windows Server AD
□	OnPUser02	onpuser02@ahmadmz.cf	Member	Windows Server AD

3. Go to the left-side, select **Azure Active Directory**
4. Select **Groups**, under **manage**

Note: Here you will see the Windows AD Groups.



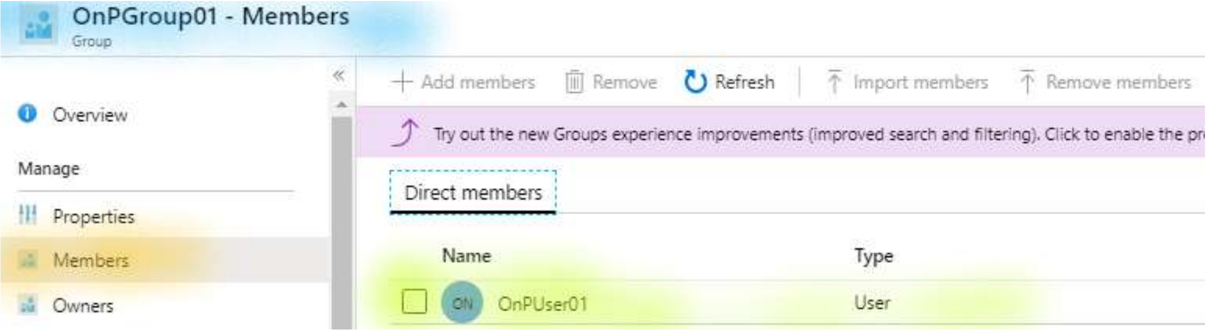
Try out the new Groups experience improvements (improved search and filtering). Click to enable the preview. →

On

	Name	Object Id	Group Type	Membership Type	Email	Source
□	OnPGroup01	430bfad5-e6a9-4c06-a92f-686...	Security	Assigned		Windows server AD
□	OnPGroup02	c7dbd73d-4148-4f25-8258-73...	Security	Assigned		Windows server AD

5. Open the **OnPGroup1**
6. Select the **Members**, under the **manage**

Note: Here you will see the **OnPUser01** user added in the group.



OnPGroup01 - Members
Group

Try out the new Groups experience improvements (improved search and filtering). Click to enable the pr

Direct members

Name	Type
☐ ON OnPUser01	User

III.**Login in Azure AD**

7. Open the below **URL** from new browser

   portal.azure.com

8. Login with Azure AD Id **OnPUser01@<YOUR-AD-DOMAIN.com>** and password **P@ssword@123**
   1.

   Note: Replace **YOUR-AD-DOMAIN.com** with you Azure AD Domain Name. Like **ahmadmz.cf**.

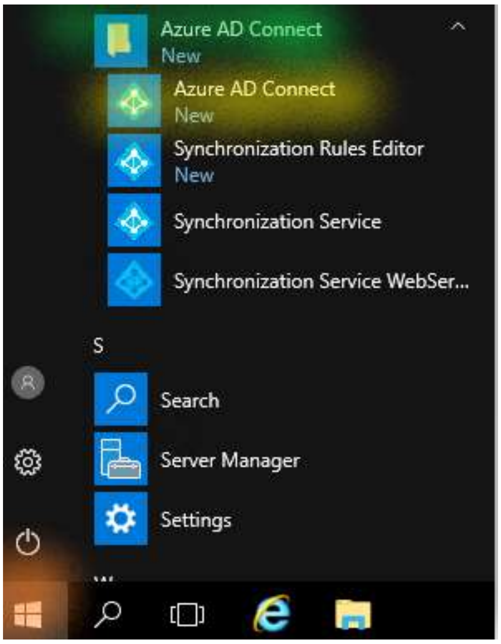
   Note: You will not be asked for to change the Password.

Step 9: Enable Password Writeback

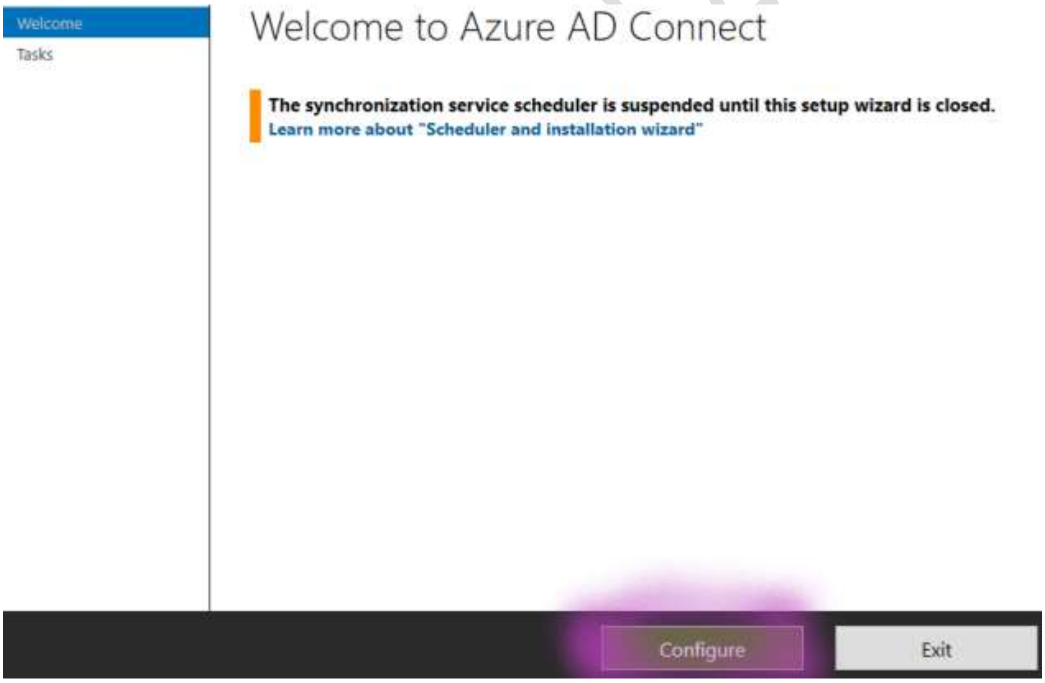
1. Login into **OnP-DC01** virtual machine via **RDP**

2. Click on the **Start**

3. **Expand Azure AD Connect** & Select **Azure AD Connect**



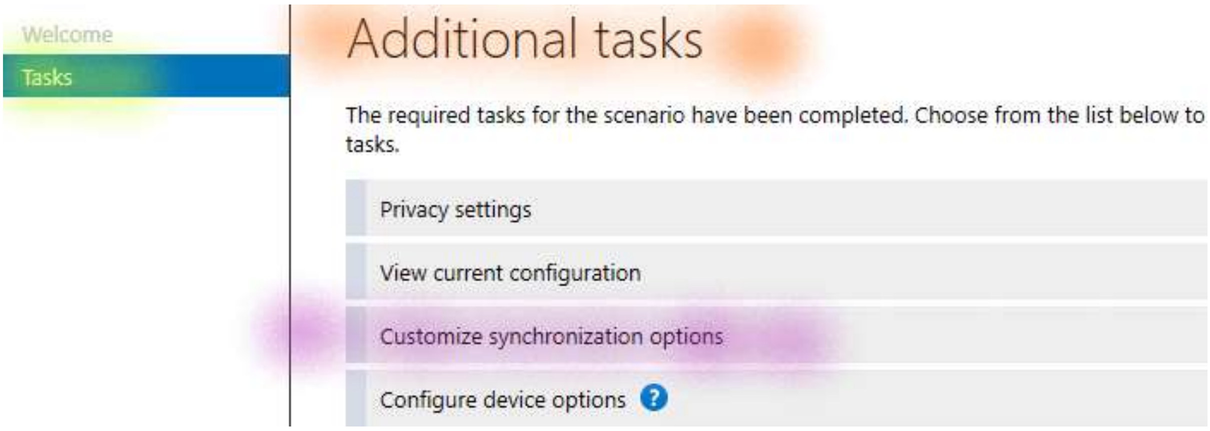
4. On the **Welcome** page, select **Configure**



Welcome to Azure AD Connect

The synchronization service scheduler is suspended until this setup wizard is closed.
Learn more about "Scheduler and installation wizard"

5. On the **Additional tasks** page, select **Customize synchronization options**
6. Select **Next**



Additional tasks

The required tasks for the scenario have been completed. Choose from the list below to tasks.

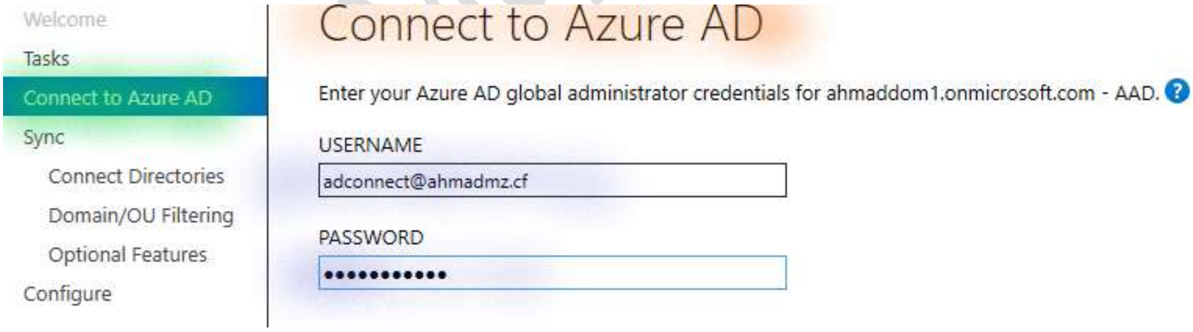
7. On the **Connect to Azure AD** page, enter below details:

   i. **Username**: Provide **adconnect@<YOUR-AD-DOMAIN.com>**

      Note: Replace **YOUR-AD-DOMAIN.com** with you Azure AD Domain Name. Like **ahmadmz.cf.**

   ii. **Password**: Provide your **password**

8. Select **Next**



Connect to Azure AD

Enter your Azure AD global administrator credentials for ahmaddom1.onmicrosoft.com - AAD.

USERNAME

adconnect@ahmadmz.cf

PASSWORD

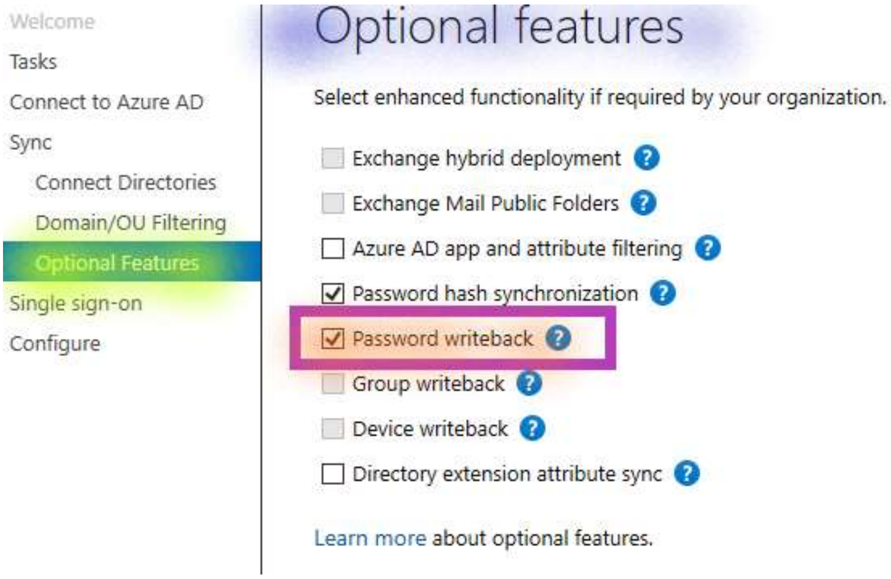
•••••••••••

9. On the **Connect directories** pages, select **Next**

10. On the **Domain/OU filtering** pages, select **Next**

11. On the **Optional features** page:

    a. Select the box next to **Password writeback**
    b. Select **Next**



Optional features

Select enhanced functionality if required by your organization.

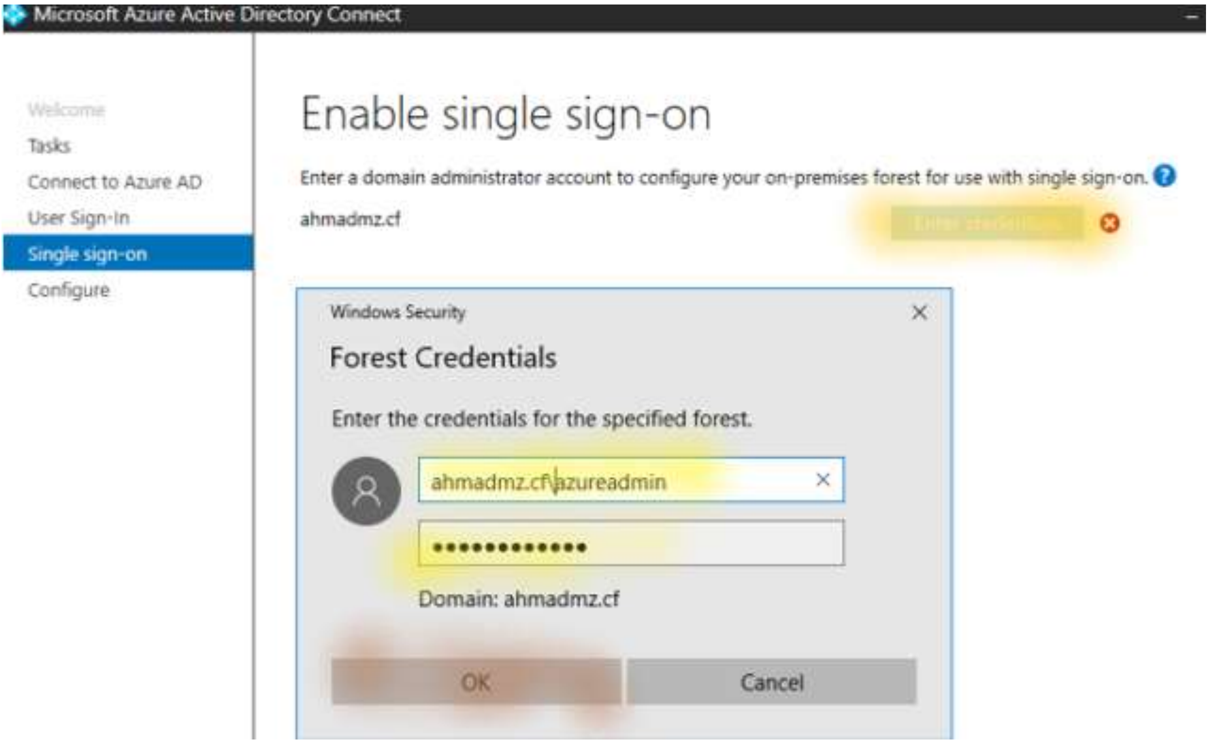
- □ Exchange hybrid deployment
- □ Exchange Mail Public Folders
- □ Azure AD app and attribute filtering
- ☑ Password hash synchronization
- ☑ Password writeback
- □ Group writeback
- □ Device writeback
- □ Directory extension attribute sync

Learn more about optional features.

3. On the **Single Sign-On** page:
    a. Select **Enter credentials**
    b. Provide **below credentials**
        i. **Username**: Provide **<YOUR-AD-DS-DOMAIN.com>\master**

        Note: Replace **YOUR-AD-DS-DOMAIN.com** with you Windows Active Directory Domain Name. Like **ahmadmz.cf**.

        ii. **Password**: Provide password **Lab@password**
        iii. Select **OK**
    c. Select **Next**



Enable single sign-on

Enter a domain administrator account to configure your on-premises forest for use with single sign-on.

ahmadmz.cf

Forest Credentials

Enter the credentials for the specified forest.

ahmadmz.cf\azureadmin

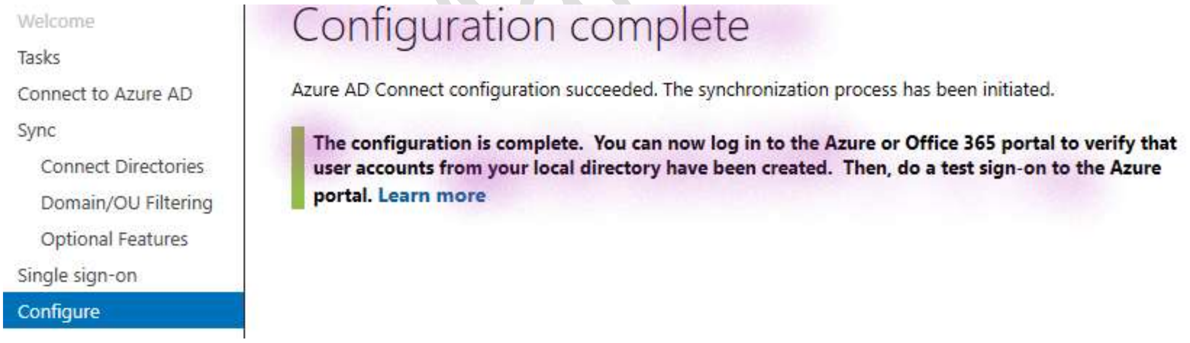
•••••••••••••

Domain: ahmadmz.cf

4. On the **Ready to configure** page, select **Configure**

   Note: Wait for the process to complete

5. When you see the configuration finish, select **Exit**



Configuration complete

Azure AD Connect configuration succeeded. The synchronization process has been initiated.

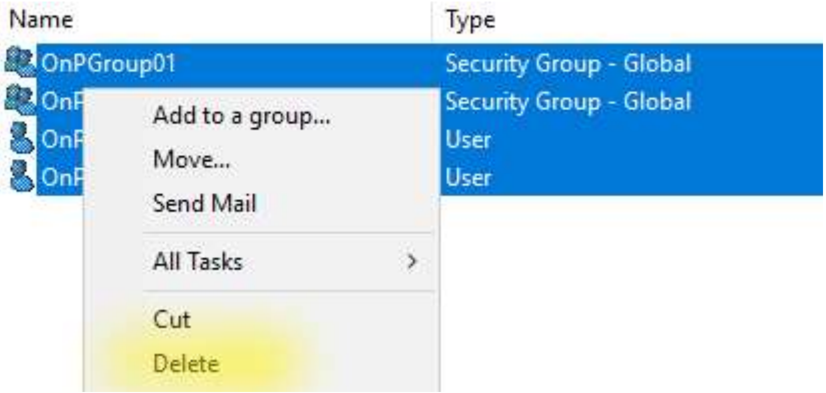
The configuration is complete. You can now log in to the Azure or Office 365 portal to verify that user accounts from your local directory have been created. Then, do a test sign-on to the Azure portal. Learn more

Step 10. Delete Azure AD Connect

1. Login in to **OnP-DC01** virtual machine via **RDP**
2. From the **OnP-DC01** virtual machine, Go to **Start** menu, right click on **Start** & **Run**
3. In the open, **write** **dsa.msc** (Active Directory Users and Computers)
4. Expand **YOUR-DOMAIN.com** and select the **Lab103-AD-OU** Organisational Unit

Note: Here you can see the Groups & Users.

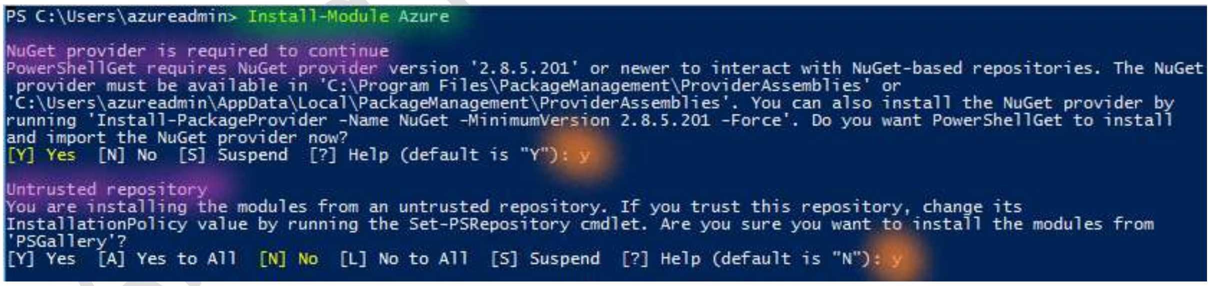
5. Select **Users** & **Group** and select **Delete**



6. From the **OnP-DC01** virtual machine, Go to **Start** menu, right click on **Start** & **Run**
7. In the open, **write** **powershell.exe**
8. Install PowerShell Modules
    a. Install **Azure Module**

    Import-Module Azure

        i. Select **Y**, once asked for NuGet provider is required to continue
        ii. Select **Y**, once asked for Untrusted repository



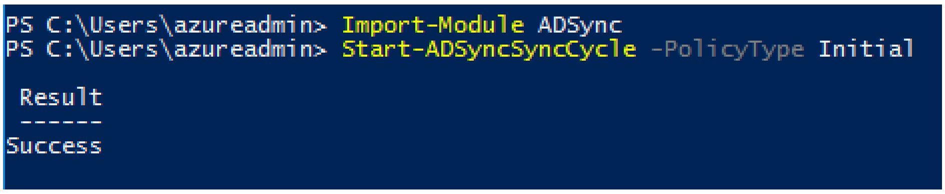
```
PS C:\Users\azureadmin> Install-Module Azure

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
 provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\azureadmin\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by
running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install
and import the NuGet provider now?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): y
```

9. **Execute** the below commands
    a. Import the **ADSync Module**

    Import-Module ADSync

    b. Initiate the **Manual Sync**

    Start-ADSyncSyncCycle -PolicyType Initial



```
PS C:\Users\azureadmin> Import-Module ADSync
PS C:\Users\azureadmin> Start-ADSyncSyncCycle -PolicyType Initial

 Result
 ------
Success
```

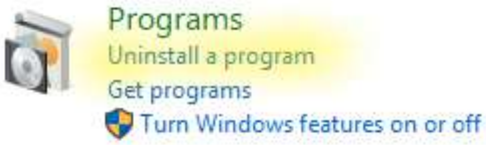
10. Go to the left-side, select **Azure Active Directory**
    a. **Select Users, under manage**

    Note: Here you will see the Windows AD Users are deleted now.

    b. **Select Groups, under manage**

    Note: Here you will see the Windows AD Groups are deleted now.

11. From the **OnP-DC01** virtual machine, Go to **Start** menu, right click on **Start** & **Run**
12. In the open, **write Control Panel**
13. From the Control panel, Select **Uninstall a program** under **Programs**



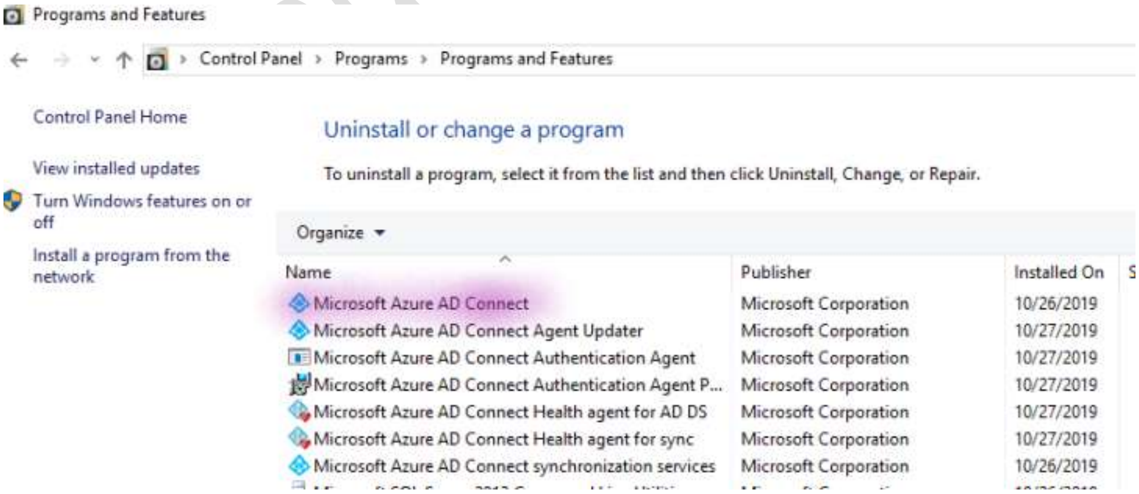
Programs

Uninstall a program

Get programs

Turn Windows features on or off

14. Select **Microsoft Azure AD Connect** to **Uninstall**



Programs and Features

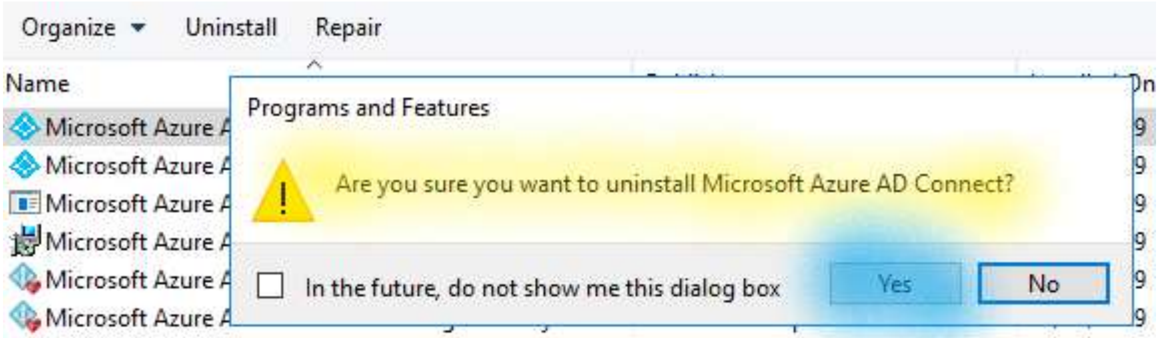
Control Panel › Programs › Programs and Features

Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Organize

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On
Microsoft Azure AD Connect	Microsoft Corporation	10/26/2019
Microsoft Azure AD Connect Agent Updater	Microsoft Corporation	10/27/2019
Microsoft Azure AD Connect Authentication Agent	Microsoft Corporation	10/27/2019
Microsoft Azure AD Connect Authentication Agent P...	Microsoft Corporation	10/27/2019
Microsoft Azure AD Connect Health agent for AD DS	Microsoft Corporation	10/27/2019
Microsoft Azure AD Connect Health agent for sync	Microsoft Corporation	10/27/2019
Microsoft Azure AD Connect synchronization services	Microsoft Corporation	10/26/2019

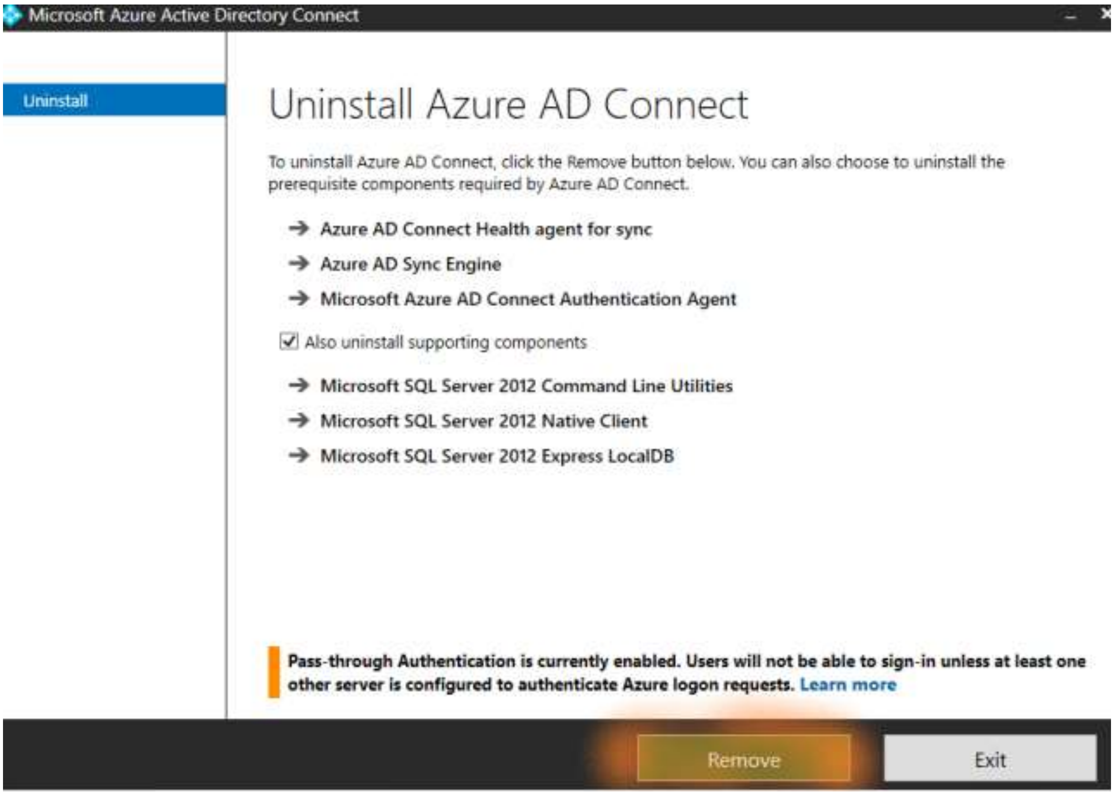


Programs and Features

Are you sure you want to uninstall Microsoft Azure AD Connect?

☐ In the future, do not show me this dialog box

15.It will open the new Window. Select **Remove** to remove the Azure AD Connect



Uninstall Azure AD Connect

To uninstall Azure AD Connect, click the Remove button below. You can also choose to uninstall the prerequisite components required by Azure AD Connect.

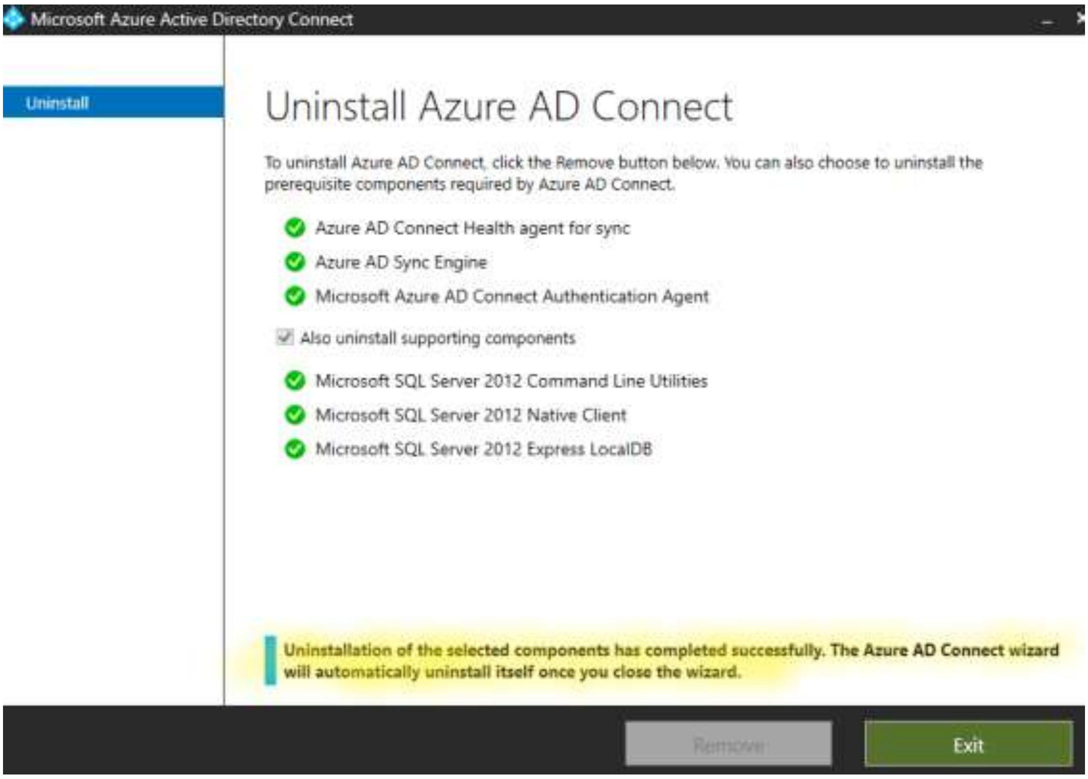
- → Azure AD Connect Health agent for sync
- → Azure AD Sync Engine
- → Microsoft Azure AD Connect Authentication Agent

☑ Also uninstall supporting components

- → Microsoft SQL Server 2012 Command Line Utilities
- → Microsoft SQL Server 2012 Native Client
- → Microsoft SQL Server 2012 Express LocalDB

Pass-through Authentication is currently enabled. Users will not be able to sign-in unless at least one other server is configured to authenticate Azure logon requests. Learn more

16.Once **Uninstall** completed. Select **Exit**



Uninstall Azure AD Connect

To uninstall Azure AD Connect, click the Remove button below. You can also choose to uninstall the prerequisite components required by Azure AD Connect.

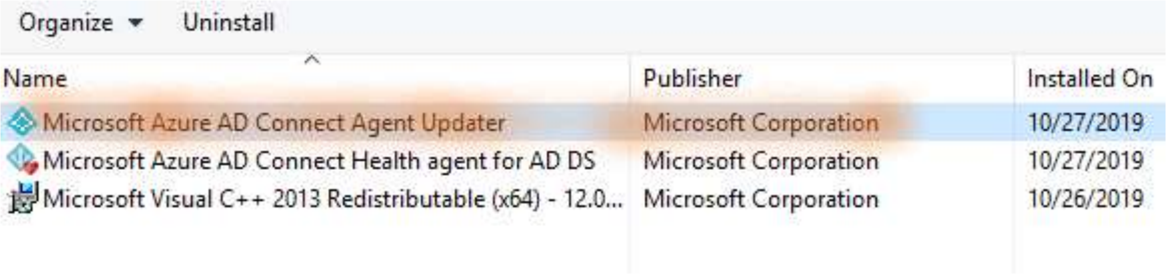
- ✓ Azure AD Connect Health agent for sync
- ✓ Azure AD Sync Engine
- ✓ Microsoft Azure AD Connect Authentication Agent

☑ Also uninstall supporting components

- ✓ Microsoft SQL Server 2012 Command Line Utilities
- ✓ Microsoft SQL Server 2012 Native Client
- ✓ Microsoft SQL Server 2012 Express LocalDB

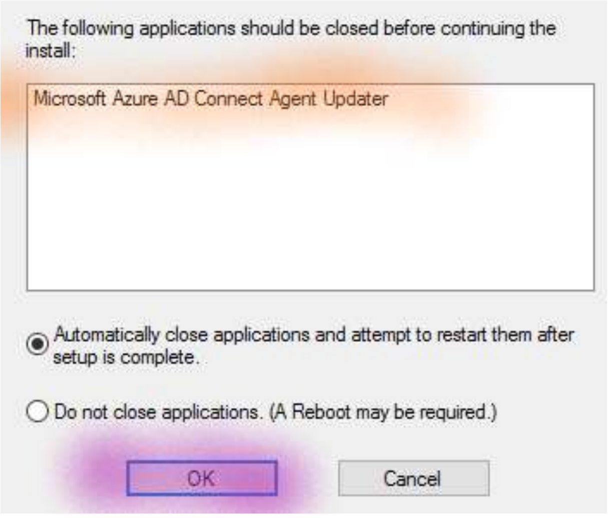
Uninstallation of the selected components has completed successfully. The Azure AD Connect wizard will automatically uninstall itself once you close the wizard.

17. Select **Microsoft Azure AD Connect Agent Updater** to **Uninstall** (If it's showing)



Name	Publisher	Installed On
Microsoft Azure AD Connect Agent Updater	Microsoft Corporation	10/27/2019
Microsoft Azure AD Connect Health agent for AD DS	Microsoft Corporation	10/27/2019
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0...	Microsoft Corporation	10/26/2019

18.Select **Ok**, once asked for closing the application



The following applications should be closed before continuing the install:

Microsoft Azure AD Connect Agent Updater

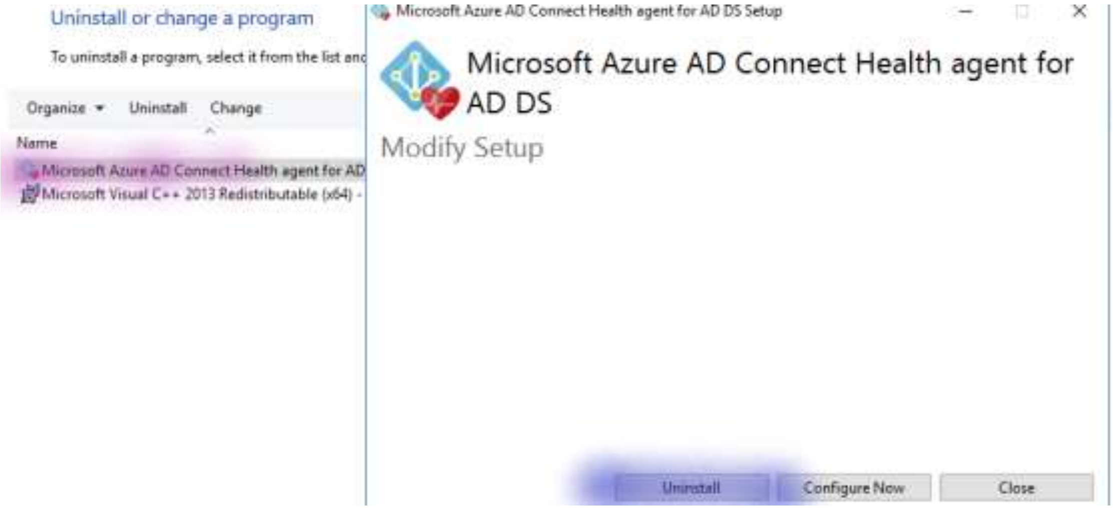
● Automatically close applications and attempt to restart them after setup is complete.

○ Do not close applications. (A Reboot may be required.)

19.Select **Microsoft Azure AD Connect Health Agent for AD DS** to **Uninstall**

20.It will open the new Window. Select **Uninstall**

21.Select **Close**, once it uninstalls successfully


Uninstall or change a program
To uninstall a program, select it from the list and
Organize
Uninstall
Change
Name
Microsoft Azure AD Connect Health agent for AD
Microsoft Visual C++ 2013 Redistributable (x64) -
Microsoft Azure AD Connect Health agent for AD DS Setup
Microsoft Azure AD Connect Health agent for AD DS
Modify Setup
Uninstall
Configure Now
Close

22. Go to the left-side, select **Resource group**

23.Select **RG-103-09-02** & **delete** the resource group