Hands-On Lab

Table of Contents

[Change Log 2](#_Toc526796855)

[Before you Begin 2](#_Toc526796856)

[Setup an IaaS Domain Controller via JSON Template 2](#_Toc526796857)

[Install the domain controller 2](#_Toc526796858)

[Connect to the Domain Controller and create a user account 3](#_Toc526796859)

[Create a virtual machine 5](#_Toc526796860)

[Join the VM to the domain 6](#_Toc526796861)

[Check the DNS Setting 6](#_Toc526796862)

[Configure DNS 6](#_Toc526796863)

[Join the Domain 6](#_Toc526796864)

[Install Azure Active Directory 7](#_Toc526796865)

[Create a Sync Account 8](#_Toc526796866)

[Sync Azure AD with Windows Server AD (AD DS) 9](#_Toc526796867)

[Install Azure Active Directory Connect 9](#_Toc526796868)

[Configure Azure Active Directory Connect 9](#_Toc526796869)

[Validate Synchronization 10](#_Toc526796870)

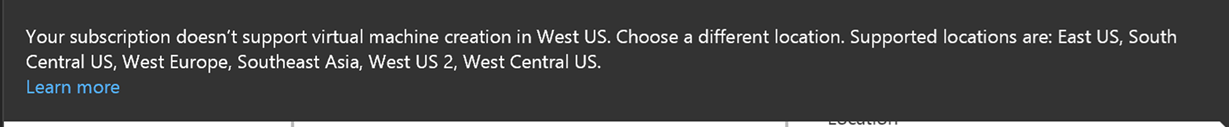
# Change Log

|  |  |  |
| --- | --- | --- |
| Date | Version | Comments |
| October 2018 | 1 | Original Document |

# Before you Begin

If you are using a Microsoft Azure subscription that was provided to you by Microsoft, you are limited to a specific set of Microsoft Azure regions that you can use. **Please use either the East US, South Central US, West Europe, Southeast Asia, West US 2, or West Central US locations.**

Otherwise you will receive the following error in the portal if you select an unsupported region and attempt to build anything in Microsoft Azure.



# Setup an IaaS Domain Controller via JSON Template

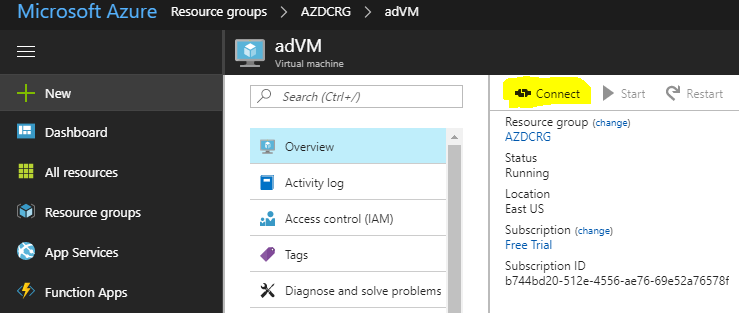
We will setup an IaaS VM with Active Directory via a JSON template from GitHub. Although this domain controller is the in the cloud, we’ll use it to simulate an on-prem domain controller.

## Install the domain controller

1. Surf to <https://azure.microsoft.com/en-us/resources/templates/active-directory-new-domain/>
2. Select **Deploy to Azure**.
3. Enter the following information:
   1. Resource Group: Create New: AZDCRG
   2. Location: Pick a supported location
   3. Admin Username: <yourname> you should write this down
   4. Admin Password: <pickyourown> you should write this down
   5. Domain name: Enter a FQDN such as *mydomainname.com* and keep the name **shorter than 15 characters (that’s a NetBIOS restriction)**
   6. DNS Prefix: <pickyourown> (e.g. use the letter “a” and then the last four digits of your cell phone, *a1234*)
4. Click **I agree to the terms and conditions stated above** and then **Purchase**. Monitor the deployment by clicking on the “Deploying Template deployment” tile within the Azure Portal.
   1. Confirm that you don’t have any validation errors. If you do, correct them before moving forward.
   2. If the deployment fails, examine the logs. You’ll need to delete the Resource Group before you try running the template again.
   3. If the template takes you back to the Microsoft Azure portal and the deployment begins, monitor the status for any errors.
5. The deployment and build of the VM will take upwards of 30 minutes depending on several factors. Don’t forget that we’re not only spinning up a VM but we are also installing and configuring DNS and running DCPromo. Please return to the instructor’s presentation.

## Connect to the Domain Controller and create a user account

1. Connect to the adVM virtual machine and logon with your domain account by selecting Microsoft Azure / Resource Groups / AZDCRG / adVM / Connect.



1. Click on **Download RDP File**.
2. Logon with the fully qualified credentials you wrote down earlier (e.g. *yourname*@*yourdomain.com*). You may have to choose **More options** to enter your new set of credentials.
3. If prompted, click **No** on the Network Discovery blade.
4. Within Server Manager, click **Tools** and then **Active Directory Users and Computers**.
5. Expand the tree and select the **Users Container**.
6. On the toolbar click the icon to create a new user in the current container. 
7. Create a New User with the following information:
   1. First Name: On
   2. Last Name: Prem
   3. Full Name: On Prem
   4. User Logon Name: onprem
8. Click **Next** andset the password to Complex.Password. Uncheck **User must change password at next logon,** and set the **Password never expires** checkbox.
9. Click **Next** then **Finish**.
10. Minimize the RDP window.

# Create a virtual machine

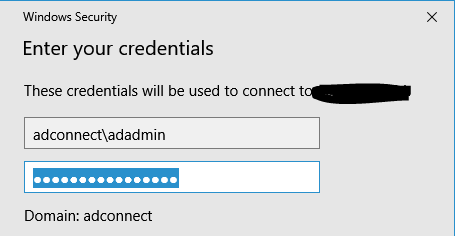
We are creating a small VM to be used later to host the Azure AD Connector service.

1. Return to the Azure portal and click the **New** or **Create a Resource** button (the Plus) found on the upper left-hand corner of the Azure portal.
2. Select **Compute** from the **New** blade, select **Windows Server 2016 Datacenter** from the **Compute** blade.
3. Fill out the virtual machine **Basics** form and click **Ok**:
   1. Virtual machine name: ADConnect
   2. User name: ADAdmin
   3. Password: Complex.Password
   4. Use existing Resource Group: AZDCRG
   5. Public inbound ports: Allow
   6. Select inbound ports: RDP
4. Click **Review + create**, and when validation fails, go to the **Management** Tab and **Create** new for the diagnostics storage account. Enter a unique name for the storage account and click **OK**.
5. Click **Review + create**, and when validation passes, click **Create**.
6. To monitor deployment status, click the “Deploying Windows Server 2016 Datacenter” tile. The VM can be found on the Azure portal dashboard, or by selecting **Virtual Machines** from the left-hand menu. It should take less than 10 minutes to spin up the VM.
7. When the VM has been created, the status changes from **Deploying** to **Running**.

## Join the VM to the domain

### Check the DNS Setting

1. Connect to the ADConnect VM and logon as **ADAdmin**.



1. If prompted, click **No** on the Network discovery blade.
2. Depending on which region you chose for setup, the ADConnect VM may or may not have the DNS server set to a value we need.
3. The DNS Server on ADCONNECT may not be set to see the domain controller (adVM), so we need to check that setting.
4. Open a Command prompt and enter **ipconfig /all |more**.
5. If the DNS Server is set to 10.0.0.4, continue to step 14.

### Configure DNS

1. Within Server Manager, click on **Local Server**.
2. Click on **IPv4 address assigned by DHCP, IPv6 enabled** setting for the Ethernet connection.
3. Right-click on the network adapter and choose **Properties.**
4. Select **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties.**
5. Select the radio button for **Use the following DNS Server addresses:** andSet the DNS server to 10.0.0.4 and click **OK** and then **Close**.
6. You will lose connection to the ADConnect VM, this is expected. Once you are back at the Microsoft Azure Portal, click **Restart** to restart the ADConnect VM.
7. Once the VM is successfully restarted, connect to the ADConnect VM and logon as **ADAdmin**.

### Join the Domain

1. Within Server Manager, click on **Local Server**.
2. Click on **WORKGROUP,** then **Change** to rename this computer or join it to a domain.
3. Click the radio button for Domain, enter your fully-qualified domain name, such as *mydomainname.com,* and click **Ok**.
4. In the Windows Security box enter the AD Domain Admin credentials you specified in the template.
5. Click **Ok** on the Welcome screen, **Ok** on the Restart window, **Close**, then **Restart Now**.

# Install Azure Active Directory

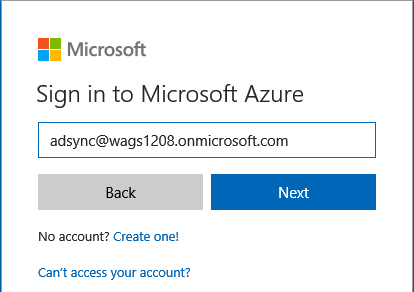
1. In the Azure Portal, click the **+New or +Create a resource** and then select **Identity**, then **Azure Active Directory**.
2. Enter:
   1. **Organization name** (e.g. MyDirectory)
   2. **Initial domain name** (e.g. your initials plus last four of your cellphone)

Ensure validation passes as your namespace needs to be unique within the \*.onmicrosoft.com namespace. We often see students choosing a domain name that already exists. you should write this initial domain name name down

1. Click **Create**. It will take several minutes for the directory to be created.
2. Once complete, click “**Click here to manage your new directory**”.

# Create a Sync Account

1. In Azure Active Directory, under **Manage** choose **Users** and then under **All users c**lick on **+New User**.
   1. **Name:** AD Sync Account
   2. **User name:** adsync (e.g. *adsync@abc1234.onmicrosoft.com*)
   3. **Directory Role**: Global administrator (Click Ok)
   4. Click on Show Password and copy the password.
2. Click **Create**.
3. Open an InPrivate or Incognito browser and surf to <https://portal.azure.com>.
4. Login as you’re the AD Sync Account you just created using the temporary password.



1. Change your password to a complex password and then click **Update password and sign in**.
2. Close your private or incognito browser.

# Sync Azure AD with Windows Server AD (AD DS)

## Install Azure Active Directory Connect

1. Connect to the ADConnect VM and logon as your previously created domain account (i.e. (*domainname\username*). If you don’t see the VM, you must switch from the directory you just created to the default directory associated with your subscription. Click in the upper right-hand corner of the screen to change directories.
2. When Server Manager opens select **Local Server** and turn off **IE Enhanced Security Configuration.**
3. Open Internet Explorer, accept the defaults, and surf to <http://go.microsoft.com/fwlink/?LinkId=615771>
4. Click **Download**, then **Run** when prompted.

## Configure Azure Active Directory Connect

1. On the **Welcome to Azure AD Connect** screen select **I agree** then **Continue**.
2. Review the screen and select **Use express settings**.
3. On the **Connect to Azure AD** screen enter you Azure AD Credentials … this would be the adsync account you created. Click **Next** and confirm the credential are validated.
4. On the **Connect to AD DS** screen, enter the Active Directory Domain Services domain administrator credentials. This would be the account you created in the template. Click **Next** and confirm the credential are validated.

If you get an error about the current security context is not associated with an Active Directory domain or forest, you more than likely didn’t logon with a domain account but rather a local account. Logout and login with a domain account and restart at step 1 in this section.

1. On the **Azure AD sign-in configuration** screen, select the checkbox for **Continue without any verified domains** and click **Next**.
2. On the **Ready to Configure** screen click **Install**.
3. Click **Exit** when complete. It may take 5-10 minutes for Azure AD Connect to complete installation.

## Validate Synchronization

1. Switch to the Azure portal and examine your Azure AD Directory by clicking on the directory and choosing All users. Note that you should see accounts sourced from Active Directory that have synchronized to Azure Active Directory (e.g. On Prem). You may need to switch directories to point to the right directory.

