

Hands-On Lab

Azure Identity

Table of Contents

Before you Begin	2
Azure Subscription	2
Which directory am I using?	2
Setup an IaaS Domain Controller via JSON Template	2
Install the domain controller	3
Connect to the Domain Controller and create a user account	3
Create a virtual machine	5
Join the VM to the domain	6
Install Azure Active Directory	8
Create a Sync Account	9
Sync Azure AD with Windows Server AD (AD DS)	10
Install Azure Active Directory Connect	10
Configure Azure Active Directory Connect	10
Validate Synchronization	12
If Time Permits ... Advanced features	13
Add Facebook from the Azure AD gallery	13
Configure single sign-on for Facebook from the Azure AD gallery	13
Assign users to Facebook	13
Capture the User Access URL	13
Test Access	13

Before you Begin

Azure Subscription

With the 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**
- **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.

Your subscription doesn't support virtual machine creation in West US. Choose a different location. Supported locations are: East US, South Central US, West Europe, Southeast Asia, West US 2, West Central US.
[Learn more](#)

Which directory am I using?

In this lab you will eventually create three different directories and keeping track which one you are in can be confusing. The directories that you will have are:

- 1) The **default directory** associated with your Azure Subscription.
- 2) The directory associated with the **Active Directory Domain Services** that you create*.
- 3) The directory/organization name associated with the **Azure Active Directory** domain that you create.

The easiest way to indicate the content of your current directory is to look at the upper right-hand corner of the Azure portal. The first line will indicate the ID you used to logon to your current Microsoft Azure subscription and the second line indicates your current directory.

tampappe@outlook.c...
DIRECTORYNAME

*Please note that the Active Directory Domain Services domain name that you will create ***will never*** be displayed in this part of the UI. Only the default directory associated with your Azure Subscription and the directory associated with the Azure Active Directory domain that you create.

Setup an IaaS Domain Controller via JSON Template

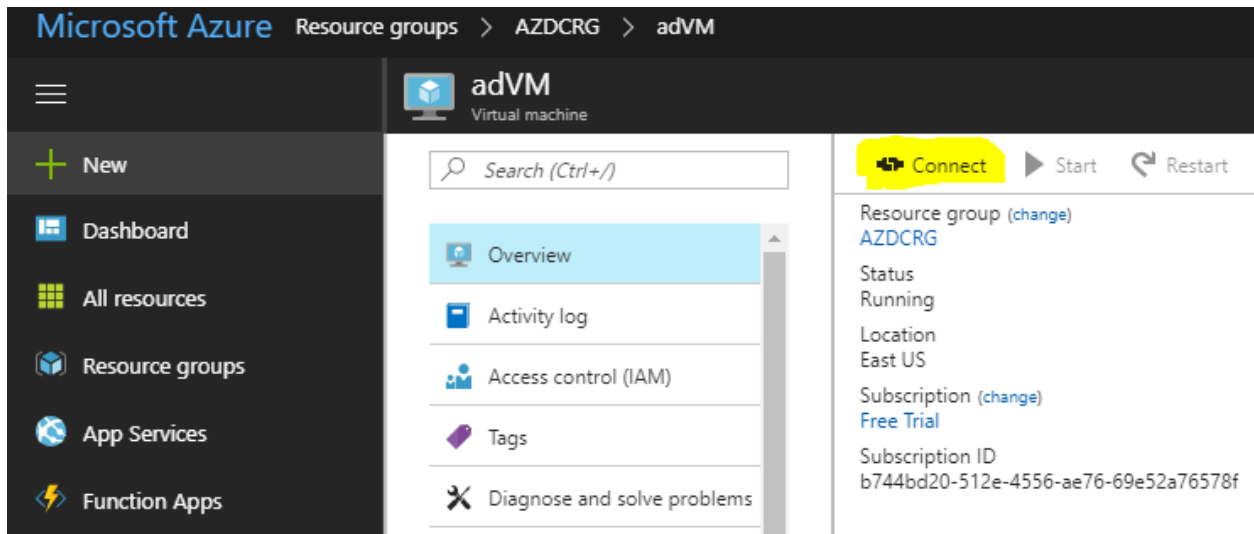
We will setup an IaaS VM with Active Directory via a JSON template from GitHub. Although this domain controller is in the cloud, we'll use it to simulate an on-prem domain controller.


Install the domain controller

1. Browse to <https://azure.microsoft.com/en-us/resources/templates/active-directory-new-domain/>
2. Select **Deploy to Azure**.
3. Enter the following information:
 - a. Resource Group: *(create new)* RG-DEMO-Identity
 - b. Location: East US
 - c. Admin Username: ADDSAdmin
 - d. Admin Password: Password-<initials>!<last 4 of cell> *(i.e. Password-ABC!5945)*
 - e. Domain name: Enter a FQDN such as <first and middle initials> <first 9 characters of last name>.com *(i.e. abclover.com)* and keep the name **shorter than 15 characters (that's a NetBIOS restriction)**
 - f. DNS Prefix: <initials> *(i.e. abc)*
Note: Domain Name and DNS Prefix are case sensitive and only accept lowercase
 - g. VM Size: Standard_D2s_v3
4. Click **I agree to the terms and conditions stated above**, select **Pin to dashboard** and then **Purchase**.
 - a. Confirm that you don't have any validation errors. If you do, correct them before moving forward.
 - b. If the deployment fails, examine the logs. You'll need to delete the Resource Group before you try running the template again.
 - c. If the template takes you back to the Microsoft Azure portal and the deployment begins, monitor the status for any errors.
 - d. If you clicked out of the deployment blade, you can check the status and errors by selecting **Microsoft Azure → Resource Groups → RG-DEMO-Identity** then within the resource group blade, click on **Deployments** under Settings and finally click on the name of the deployment that is still running or has an error.
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

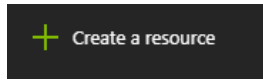
1. Connect to the adVM virtual machine by selecting **Microsoft Azure → Resource Groups → RG-DEMO-Identity → adVM → Connect**.

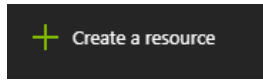


2. Since the VM is behind a load balancer, you will need to select the VM's loadbalancer public address to connect. Select the public IP and then **Download RDP File** and connect.
3. Logon with your domain account (*abclover.com\ADDSAdmin*) and the password you set.
4. When prompted, click **No** on the Network Discovery blade.
5. Within Server Manager, click **Tools** and then **Active Directory Users and Computers**.
6. Expand the tree on your domain name and select the **Users** Container.
7. On the toolbar click the icon to create a new user in the current container. 
8. Create a New User with the following information:
 - a. First Name: On
 - b. Last Name: Prem
 - c. Full Name: On Prem
 - d. User Logon Name: onprem
9. Click **Next** and set the password to Complex.Password. Uncheck **User must change password at next logon**, and set the **Password never expires** checkbox.
10. Click **Next** then **Finish**.
11. Minimize the RDP window.

Create a virtual machine

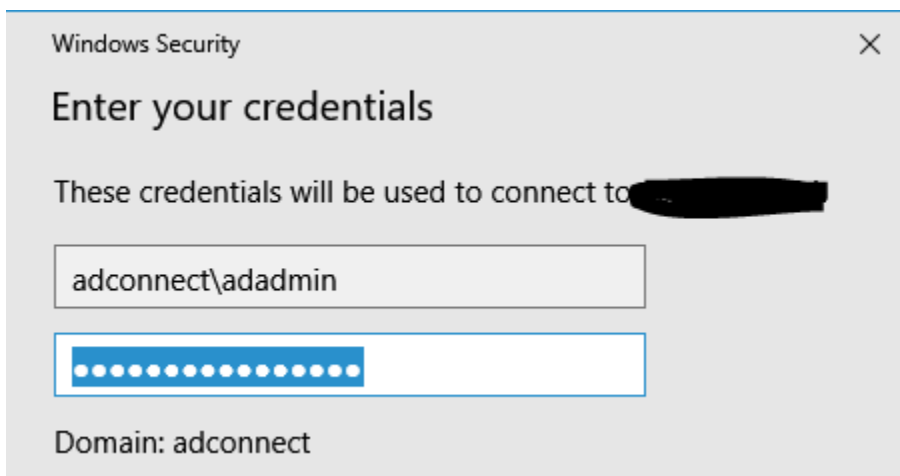
We are creating a small VM to be used later to host the Azure AD Connector service.




1. Return to the Azure portal and click the  button 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**:
 - a. Resource Group: RG-Demo-Identity
 - b. Name: ADConnect
 - c. Region: East US
 - d. Size: Standard DS1 v2
 - e. User name: ADAdmin
 - f. Password: Complex.Password
4. Click **Review + Create>**
5. On the Create page, click **Create** to start the virtual machine deployment.
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

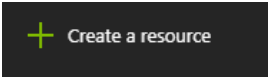
1. By default, VMs are deployed with a Network Security Group that blocks all inbound traffic. Before we can connect to the VM, we must allow RDP connections to the VM's public IP address.
2. Click on **All Services → Virtual Machines → ADConnect → Networking** found under Settings
3. Click **Add inbound security rule**
4. Click Basic at the top and configure as follows:
 - a. Service: RDP
 - b. Port Ranges: 3389
 - c. Priority: 200
 - d. Name: RDP
5. Click **Add**
6. Once the new inbound rule is successfully created, click on **Overview** and then **Connect**
7. Connect to the ADConnect VM and logon as **ADAdmin**. If you receive a connection error, wait 30 seconds and try again.

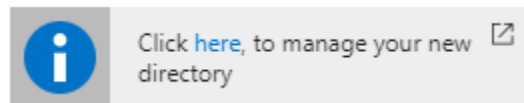


8. When prompted, click **No** on the Network discovery blade.
9. The DNS Server on ADCONNECT is not set to see the domain controller (adVM), so we need to change that setting. Within Server Manager, click on **Local Server**.
10. Click on **IPv4 address assigned by DHCP, IPv6 enabled** setting for the Ethernet connection.
11. Right-click on the network adapter and choose **Properties**.
12. Next to Ethernet, select **IPv4 address assigned by DHCP, IPv6 enabled**.
13. Right-click **Ethernet** and then click **Properties**.
14. Select **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**
15. Select the radio button for **Use the following DNS Server addresses:** and set the Preferred DNS server to 10.0.0.4 and click **OK** and then **Close**.

16. 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.
17. Once the VM is successfully restarted, connect to the ADConnect VM and logon as **ADAdmin** to ensure connectivity works.
18. Within Server Manager, click on **Local Server**.
19. Click on **WORKGROUP**, then **Change** to rename this computer or join it to a domain.
20. Click the radio button for Domain, enter your fully-qualified domain name (*abclover.com*), and click **Ok**.
21. In the Windows Security box enter the Domain Admin credentials you specified in the template (*abclover.com\ADDSAdmin*).
22. 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  and then select **Identity**, then **Azure Active Directory**.
2. Enter:
 - a. **Organization name** create a unique name (*i.e. BootCamp*)
 - b. **Initial domain name** (e.g. your initials plus last four of your cellphone). Ensure validation passes (you might have chosen a domain name that already exists).
3. Click **Create**. It will take several minutes for the directory to be created.
4. Once complete, select "**Click here to manage your new directory**".



5. Notice that in the upper right hands corner of the screen, the email address for the subscription has stayed the same but the directory listed below it has changed to the Azure Active Directory that we just created (*i.e. Bootcamp*).
6. Under **Manage** choose **Users** then **All users**.
7. Click on the name displayed, then **Directory role**. Notice they are the Global administrator.

 Save  Discard

Directory role ⓘ

- ☐ User
- ☒ Global administrator
- ☐ Limited administrator

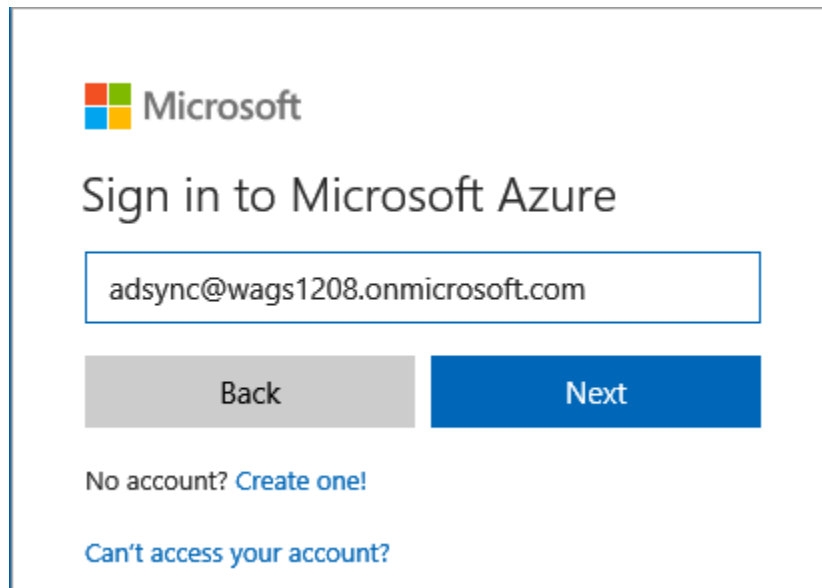
Global administrators have full control over all directory resources.

[Learn more about directory roles](#)

8. Close this blade and the All users blade to return to the Overview blade.

Create a Sync Account

1. Under **Manage** choose **Users** and then **All users**.
2. Click on **+New User**.
 - a. **Name:** AD Sync Account
 - b. **User name:** adsync (e.g. *adsync@abc1234.onmicrosoft.com*)
 - c. **Directory Role:** Global administrator (Click **Ok**)
 - d. Click on Show Password and copy the password.
3. Click **Create**.
4. Open an InPrivate or Incognito browser and surf to <https://portal.azure.com>.
5. Sign in as you're the AD Sync Account you just created using the temporary password.



Microsoft

Sign in to Microsoft Azure

adsync@wags1208.onmicrosoft.com

Back Next

No account? [Create one!](#)

[Can't access your account?](#)

6. Update your password to 'Complex.Password' and then click **Update password and sign in**.
7. Close your private or incognito browser.

Sync Azure AD with Windows Server AD (AD DS)

Install Azure Active Directory Connect

1. Ensure that you are in the correct directory by checking the upper right-hand corner of the Microsoft Azure portal. Switch if necessary.
2. Connect to the **ADConnect** VM and logon with your **Active Directory Domain Services domain account (i.e. `domainname\username`)**. Once again, if you don't see the ADConnect VM by clicking on Virtual Machines, you must switch to the default directory associated with your subscription. Click in the upper right-hand corner of the screen to change directories.
3. When Server Manager opens select **Local Server** and turn off **IE Enhanced Security Configuration**.
4. Open Internet Explorer, accept the defaults, and surf to <http://go.microsoft.com/fwlink/?LinkId=615771>
5. 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 **Express Settings** 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. Don't forget you just changed the password to the ADSync account. 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 back 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.

5. If you receive the following error, make sure you are logged onto the ADConnect VM using the domain account and not the local admin account.

The provided credentials are valid, however, we were unable to establish a connection to the current local computer's forest. Please make sure UDP and TCP ports 389 are open in the Domain Controller (s) associated with the current local computer's forest. The user has to perform this manual check on the Windows Firewall with Advanced Security administrative window on every Domain Controller. There must not be any firewall rules blocking these ports. [Learn more](#)

6. On the **Azure AD sign-in configuration** screen, select the checkbox for **Continue without any verified domains** and click **Next**.
7. On the **Ready to Configure** screen click **Install**.

8. 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 **users**. Make sure you're looking at the right directory.
2. 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.

NAME	USER NAME	USER TYPE	SOURCE
 AD Sync Account	adsync@ppewags.onmicrosoft.com	Member	Azure Active Directory
 jwagner@microsoft.com Wagner	jwagner@microsoft.com	Member	Azure Active Directory
 On-Premises Directory Synchronization Service Account	Sync_ADCONNECT_7fcd1bd3d1ee@ppewags.onmicrosoft.com	Member	Windows Server AD
 On Prem	onprem@ppewags.onmicrosoft.com	Member	Windows Server AD

If Time Permits ... Advanced features

Now that you have established synchronization between Active Directory Domain Services and Azure Active Directory, you can publish cloud-based applications to users and take advantage of some advanced features. In this scenario you will enable SSO to Facebook.

Add Facebook from the Azure AD gallery

- 1) From the Azure portal select your **Azure Active Directory** and then click **Enterprise Applications** from the Azure Active Directory left-hand navigation menu.
- 2) Click the **New application** button at the top-right corner on the Enterprise Applications pane.
- 3) In the Enter a name textbox from the Add from the gallery section, enter **Facebook**.
- 4) Click **Add** to add the application.
- 5) After a brief period of time, you be able to see the application's configuration pane.

Configure single sign-on for Facebook from the Azure AD gallery

- 1) Click the Single sign-on from the application's left-hand navigation menu.
- 2) Change the Single Sign-on Mode to **Password-based Sign-on** and click **Save**.

Assign users to Facebook

- 1) Click on **Users and Groups**.
- 2) Click on **Add user**.
- 3) Click on **Users**, select On Prem, and then **Select**.
- 4) Click **Assign**.

Capture the User Access URL

- 1) Under Manage click **Properties** and click the button to copy the URL under User access URL:

User access URL ⓘ

<https://myapps.microsoft.com/signin/Faceboo...>



Test Access

- 1) Open an InPrivate browser session and browse to the User access URL.
- 2) Logon as On Prem (onprem@yourAzureAD.onmicrosoft.com the password of Complex.Password)
- 3) Install the extension, if required. If using Microsoft Edge you may have to Launch the extension and then turn it on when prompted.
- 4) Close and then launch all Edge browsers and once again logon as On Prem to the User access URL.
- 5) Enter your *personal credentials* to Facebook, not On Prem's since they do not have a Facebook account.

- 6) Facebook should open.
- 7) Close Microsoft Edge and complete step 1.
- 8) Facebook should automatically appear without the need to logon.