# Exercise Setup – MSIX app attach.

Task 1. Prepare Active Directory in Azure VM using ARM template

This task is prerequisite for deploying Windows Virtual Desktop. For faster deployment we will use GitHub template.

1. Select the following link

<https://github.com/Azure/azure-quickstart-templates/tree/master/active-directory-new-domain>

1. Select **Deploy to Azure** button.
2. You’ll be prompted to sign in your Azure subscription
3. On the **Custom deployment** page provide the following information:

|  |  |
| --- | --- |
| **Subscription** | Select your Azure subscription. |
| **Resource Group** | Select **Create new** and provide a name for the resource group such as **WVD-rg**. |
| **Region** | From the drop-down menu, select the location where you want to deploy the new VM. |
| **Admin Username** | Student |
| **Admin Password** | Pa55w.rd1234 |
| **Domain Name** | Contoso.com |
| **Dns Prefix** | *Uniquename* |
| **Vm Size** | Accept default Standard\_D2s\_v3 |
| **\_artifacts Location** | Accept default values |
| **\_artifacts Location Sas Token** | Leave it empty |
| **Location** | Accept the default value of **[resourceGroup().location]**. |
| **Virtual Machine Name** | Accept default name **adVM** |
| **Virtual Network Name** | Accept default name **adVnet** |
| **Virtual Network Address range** | Accept default range **10.0.0.0/16** |
| **Load Balancer Front End IP Name** | Accept default **LBFE** |
| **Backend Address Pool Name** | Accept default **LBBE** |
| **Inbound Nat Rules Name** | Accept default **adRDP** |
| **Network Interface Name** | Accept default **adNic** |
| **Private IP Address** | Accept default **10.0.0.4** |
| **Subnet name** | Accept default **adSubnet** |
| **Sunet range** | Accept default **10.0.0.0/24** |
| **Public IP Address Name** | Accept default **adPublicIP** |
| **Availability Set Name** | Accept default **adAvailabilitySet** |
| **Load Balancer Name** | Accept default **adLoadBalancer** |

1. Select the **Review + create**, and then select **Create**.

**Note**

Wait for the deployment to complete. The deployment should take 45 minutes.

### Task 2: Check the resources created

1. In the Azure portal, search for **Resource groups**.
2. Select **azure-sentinel-rg**.
3. Sort the list of resources by **Type**.
4. The resource group should contain the resources listed in the following table.

|  |  |  |
| --- | --- | --- |
| Name | Type | Description |
| **adAvailabilitySet** | Availability set | VM is placed in availability set. |
| **adVM\_DataDisk** | Disk | VM disk that contains data. |
| **adVM\_OSDisk** | Disk | VM disk that contains OS. |
| **adLoadBalancer** | Load balancer | Load balancer |
| **adNic** | Network Interface | Network interface for the VM. |
| **adPublicIP** | Public IP address | Public IP address for the Load Balancer. |
| **adVM** | Virtual machine | Virtual machine used in the demonstration. |
| **adVnet** | Virtual Network | Virtual network for the VM. |

**Note**

The resources deployed and configuration steps completed in this exercise are required in the next exercise. If you intended completing the next exercise do not delete the resources from this exercise.

### Task 3: Create user for joining VM in active directory.

1. In the Azure portal, search for virtual machine, and select **adVM.**
2. From the toolbar select **Connect,**  and from the drop menu select **RDP.**
3. In the **Connect with RDP** grid, from the **IP address** drop down menu select **Load balancer public IP address**
4. Select **Download RDP File.**
5. Open the rdp connection, select **Connect** and provide the following credentials:

* Username: **Student**
* Password: **Password1234**

1. Once that you sign in **adVM,** select the **Start** menu and open **Server Manage.**
2. On the **Server Manage > Local Server,** from the navigation menu on the left side select **Local Server,** and then click the link for **IE Enhanced Security Configuration.**
3. On the **Internet Explorer Enhanced Security Configuration,** select the **Off** checkbox for both **Administrators** and **Users** and select **Ok.**
4. On the **Server Manage > Local Server,** from the **Tools,** open **Active Directory Users and Computers** snap in.
5. On the **Active Directory Users and Computers**, right click **Contoso.com** domain and from the menu select **New,** then select **Organizational Unit.**
6. On the **New Object – Organizational Unit** in the **Name** field, type **IT** ad select **OK.**
7. On the **Active Directory Users and Computers**, expand **contoso.com,** right click **IT** organization unit and from the menu select **New,** then select **User.**
8. On the **New Object – User**, type **wvdadmin** for **First name** and **User Logon name** field and select **Next.** For **Password** and **Confirm password** fields type **Pa55w.rd1234**,clear the checkbox for **User must change password at next logon** and select **Next.** Select **Finish** to create a new user.
9. On the **Active Directory Users and Computers,** select **IT** organization unit, then right click **wvdadmin** user and from the menu select **Add to a group.**
10. On the **Select Groups** window, in the **Enter the object names to select** field type **Enterprise Admins** and select **OK.** Select **OK** to confirm.
11. On the **Active Directory Users and Computers**, right click **IT** organization unit and from the menu select **New,** then select **Group.**
12. On the **New Object – Group,** in the **Group name** field type **MSIXComputers** and select **OK.**
13. Minimize **Active Directory Users and Computers** snap in.

### Task 4: Create a Global Administrator Account

1. From the taskbar open Internet Explorer and type [**https://portal.azure.com**](https://portal.azure.com)to open Azure Portal.
2. In the Azure portal, search for and select **Azure Active Directory**.
3. On the Azure Active Directory blade, in the **Manage** section, click **Users**.
4. From the toolbar select **+ New user.**
5. Create a new user with the following settings (leave others with their defaults):

**Note**: **Copy to clipboard** the full **User name**. You will need it later in this task.

| **Setting** | **Value** |
| --- | --- |
| User name | **globaladmin** |
| Name | **globaladmin** |
| Let me create the password | **Enabled** |
| Initial password | **Pa55w.rd124** |
| Roles | Select **User** link and search for and select **Global Administrator** |
| Usage location | **United States** |
| Job title | **Cloud Administrator** |
| Department | **IT** |

1. In the Azure portal, search for and select **Subscription.**
2. Select your subscription.
3. Select **Access Control (IAM)** and then **Add**. From the drop down select **Add role assignments**.
4. In the **Add role assignment** screen:
   1. Role: **Owner**
   2. Assign access to: **User, Group, or Service Principal**
   3. Select: Select **globaladmin**
5. Click Save
6. Open an **InPrivate** browser window and sign in to the Azure portal using the newly created user account. When prompted to update the password, change the password for the user. Use the following password **Pa55w.rd12345** or similar complex password.

**Note**: Rather than typing the user name, you can paste the content of Clipboard.

1. Sign out of the **globaladmin** user from the Azure portal and close the InPrivate browser window.

### Task 4: Install AD Connect

Note: You need to install Azure AD connect in the **adVM** machine.

1. Open Internet Explorer and navigate to the following URL:

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

1. Click **Download**.
2. Click **Run**.
3. Once downloaded the installer will open.
4. Once it has installed AD Connect configuration will start. Click the **I agree to the license term and privacy notice** check box and click **Continue**.
5. On the **Express Settings** page select **Use express settings**.
6. On the **Connect to Azure AD** page enter the **globaladmin** user following your tenant name. Use the password that you setup in the previous step for the global admin.

For example: User name: **globaladmin@contoso2806.onmicrosoft.com**

Password: **Pa55w.rd12345**

1. On the **Connect to AD DS** page provide the following information:

Username: **Contoso\wvdadmin**

Password: **Pa55w.rd1234**

1. Click **Next**.
2. On the **Azure AD sign in configuration** page click **Continue without matching all UPN suffixes to verified domain** check box and click **Next**.
3. On the **Ready to configure** page click **Install**
4. Once the installation is complete click **Exit**.

### Task 5. Deploy Windows Virtual Desktop using Azure portal

1. On the Azure portal, search for and select **Windows Virtual Desktop.**
2. On the **Windows Virtual Desktop** page, select **Create a host pool.**
3. On the **Create a host pool** page, in the **Basic** tab provide the following information:

|  |  |
| --- | --- |
| **Subscription** | Select your Azure subscription. |
| **Resource Group** | Select **WVD-rg**. |
| **Host pool name** | **Contoso-pool** |
| **Location** | Select the same location where you create a VM in the first task |
| **Validation Environment** | Select **Yes** |
| **Host pool type** | From the dropdown menu select **Pooled** |
| **Max session limit** | 5 |
| **Load balancing algorithm** | **Breadh-first** |

1. Select **Next: Virtual Machines >.**
2. On the **Virtual Machines** tab, for **Add virtual machines** select **Yes** checkbox and then provide the following information’s:

|  |  |
| --- | --- |
| **Resource Group** | Select **WVD-rg**. |
| **Virtual machine location** | Select the same location where you create a VM in the first task |
| **Virtual machine size** | Accept default value |
| **Number of VMs** | 1 |
| **Name prefix** | **test** |
| **Image type** | Ensure that **Gallery** is selected |
| **Image** | From the dropdown menu select **Windows 10 Enterprise multi-session, Version 2004** |
| **OS disk Type** | Accept default value |
| **Virtual network** | **adVNET** |
| **Subnet** | **adSubnet(10.0.0.0/24)** |
| **Public IP** | **No** |
| **Network security group** | **Basic** |
| **Public inbound ports** | **No** |
| **Specify domain or unit** | **No** |
| **AD domain join UPN** | [**wvdadmin@contoso.com**](mailto:wvdadmin@contoso.com) |
| **Password** | **Pa55w.rd1234** |
| **Confirm password** | **Pa55w.rd1234** |

1. Select **Next: Workspace >**
2. On the **Workspace** tab, for **Register desktop app group** select **Yes** checkbox. Then select **Create new**, provide Workspace name, for example **Contoso-Apps** and then select **OK.**
3. Select **Next: Tags >**
4. On the **Tags** tab provide **Name** and **Value** for the tags and select **Next: Review + create >**
5. Once the validation passed select **Create** to finish creation of Windows Virtual Desktop.
6. Wait for the deployment to complete. It can take up to 15 minutes for deployment to finish.

### Task 6. Setup MSIX app attach file share

1. On the Azure portal, search for and select **Storage accounts.**
2. From the toolbar select **+ Add** and provide the following information:

|  |  |
| --- | --- |
| **Subscription** | Select your Azure subscription. |
| **Resource Group** | Select **WVD-rg**. |
| **Storage account name** | Provide unique name for example **contoso-*yourname*** |
| **Location** | Select the same location where you create a VM in the first task |
| **Performance** | Standard |
| **Account kind** | **Storage V2 (general purpose v2)** |
| **Replication** | From the dropdown menu select **Locally-redundant storage (LRS)** |

1. Select **Review + Create** and then **Create.**
2. Wait for the deployment to finish. Select **Go to resource.**
3. On the Storage account select **File shares,** and then from the toolbar select **+ File Share.**
4. On the **New file share** grid, provide name, for example **msiximages** and then select **Create.**
5. Switch to **adVM** virtual machine.
6. Open **Active Directory Users and Computers** from the **Tools** menu of the **Server Manager.**
7. Expand **contoso.com** and select **Computers** container. Verify that you have one computer with name **test-0.**
8. Right click **test-0** computer and from the menu select **Add to a group**
9. On the **Select Groups** window, in the **Enter the object names to select** field type **MSIXComputer** and select **OK.** Select **OK** to confirm.
10. On the **adVM** open the start menu and right click **Windows PowerShell,** from the menu select **More** and then select **Run as administrator.** Type the following commands:

Powershell:

Import-Module 'C:\Program Files\Microsoft Azure AD Sync\Bin\ADSync\ADSync.psd1'

Start-ADSyncSyncCycle -PolicyType Delta

1. Verify that you receive **Result: Success**
2. Switch to your browser that has Azure Portal page open.
3. On the Azure portal, search for and select **Virtual Machines.**
4. Select the checkbox of **test-0** VM and from the toolbar select **Restart.** Select **Yes** to confirm the restart of the VM.
5. On the Azure portal, search for and select **Storage Accounts.**
6. Select the account that you create for example **contoso-*yourname*.**
7. Select **Access Control (IAM)** and then **Add**. From the drop down select **Add role assignments**.
8. In the **Add role assignment** screen:
   1. Role: **Storage File Data SMB Share Contributor**
   2. Assign access to: **User, Group, or Service Principal**
   3. Select: Select **MSIXComputers** the AD group that you created which contains your session hosts
9. Click Save

### Task 7. Join storage account to AD DS

In this step we are going to join our storage account to AD DS. The full article is available [here](https://github.com/Azure-Samples/azure-files-samples/releases). Please note our steps here have been modified to achieve the desired scenario.

1. Remote into the **test-0** VM. Since **test-0** VM does not have a public IP, you should first be connected to **adVM** and then from start menu open **Remote Desktop Connection.**
2. Use the following credentials to remote in **test-0:**

Username: **Contoso\student**

Password: **Pa55w.rd1234**

**Note**: Run the script using an on-premises AD DS credential that is synced to your Azure AD. The on-premises AD DS credential must have either the storage account owner or the contributor Azure role permissions.

1. Open the start menu and select **Microsoft Edge**. Type the following URL:

<https://github.com/Azure-Samples/azure-files-samples/releases>

1. Select the latest version of **AzFilesHybrid.zip** and select **Open.** Extract all files in **c:\AzFilesHybrid.**
2. From the start menu open **PowerShell**in elevated mode.
3. Run the following commands to set the execution policy:

Set-ExecutionPolicy Unrestricted

Cd c:\AzFilesHybrid

.\CopyToPSPath.ps1

Import-Module AZFilesHybrid

**Note**: You may be prompted to run scripts and to install updated version of PowerShellGet. Accept all. You may be also prompted to close and open PowerShell session to use the new version.

1. Once that you reopen Windows PowerShell attempt to run the following commands:

cd c:\AzFilesHybrid

Import-Module AZFilesHybrid

Add-AzAccount

1. Use global administrator credentials for example:

Username: [**globaladmin@contoso2608.onmicrosoft.com**](mailto:globaladmin@contoso2608.onmicrosoft.com)

**Password: Pa55w.rd12345**

1. Once that you are authenticate with **globaladmin** retrieve the Subscription ID and replace the values for the following variables.

Get-AzSubscription

$SubscriptionId = "<your-subscription-id-here>"

$ResourceGroupName = "WVD-rg"

$StorageAccountName = "<storage-account-name-here>"​

1. Run **Join-AzStorageAccountForAuth**

Join-AzStorageAccountForAuth `

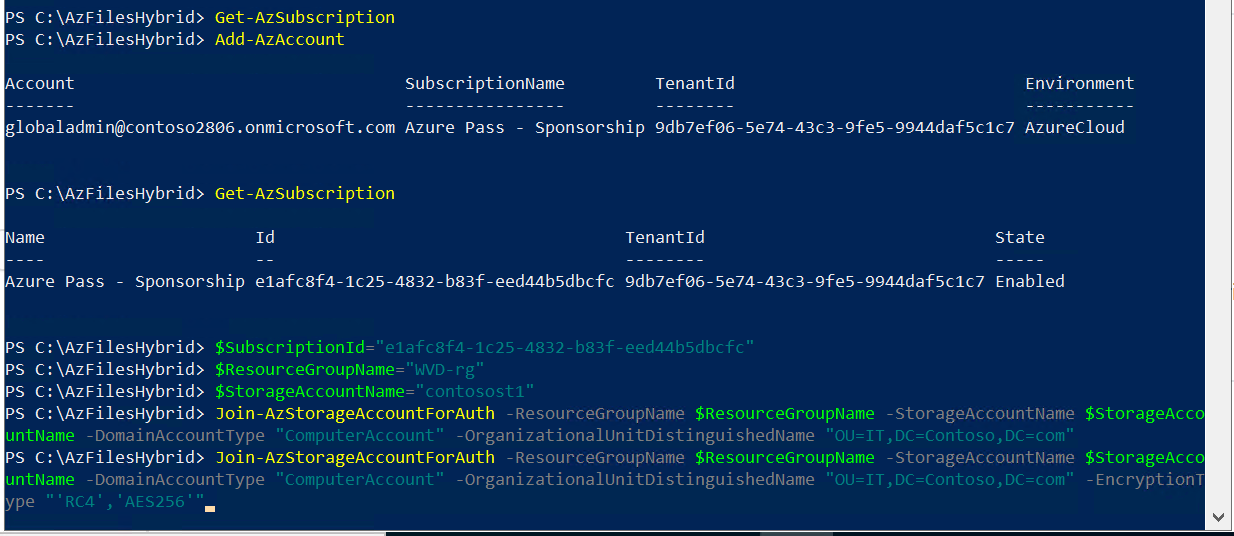
-ResourceGroupName $ResourceGroupName `

-StorageAccountName $StorageAccountName `

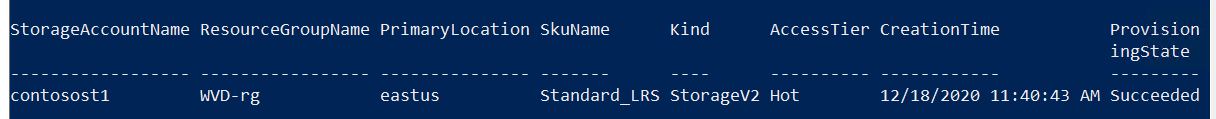
-DomainAccountType "ComputerAccount" `

-OrganizationalUnitDistinguishedName "OU=IT,DC=Contoso,DC=com" `

-EncryptionType "'RC4','AES256'"



1. The output of the above command must look like the screenshot below. If it doesn’t, joining the storage account to AD DS was not successful.



### Task 8. File-level permissions aka NTFS permissions

To be able to authenticate with AD DS computer accounts against an Azure Files storage account, we must also assign NTFS level permission in addition to the RBAC permission we set up earlier.

1. In the Windows PowerShell type the following commands:

$storageaccountkey=Get-AzStorageAccountKey -ResourceGroupName WVD-rg -StorageAccountName contosost

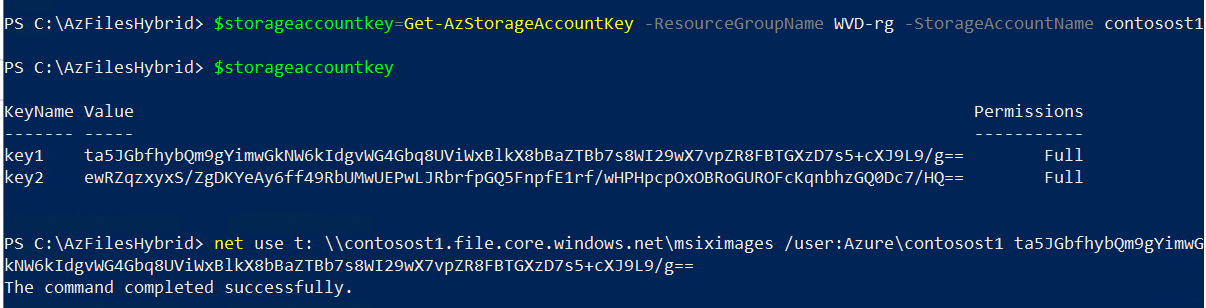
$storageaccountkey

Note: Replace the name of the storage account with the name of the storage account that you create before and with one of the keys that you retrieve from the previous command.

1. Execute the following command replacing the values in it with those applicable to your environment:

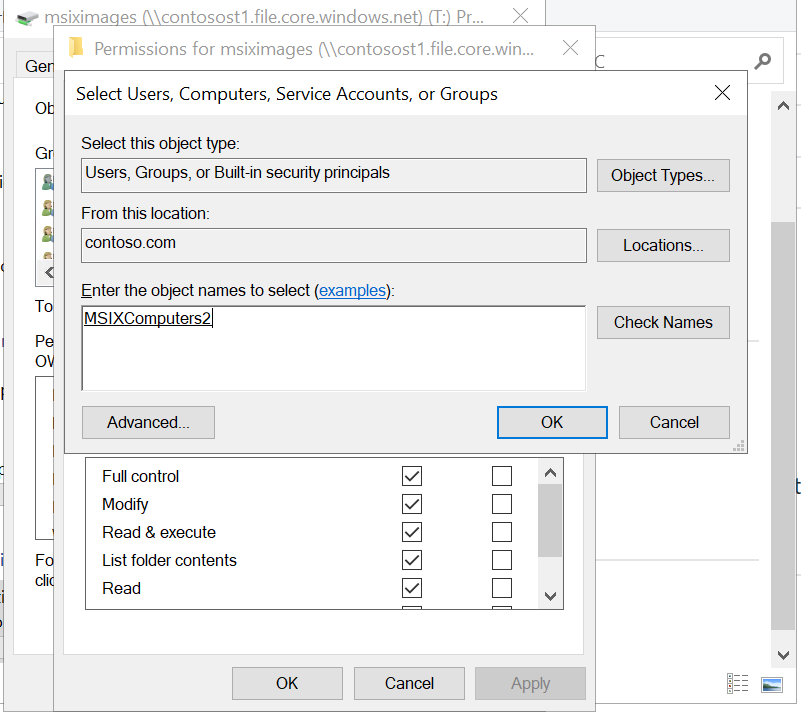
net use T: \\<storage-account-name>.file.core.windows.net\<share-name> /user:Azure\<storage-account-name> <storage-account-key>​

**For example:**



**Note:**Make sure that the output of the command above is “**The command completed successfully**”.

1. Open **File Explorer**and find the drive letter specified in the command above.
2. Right click on the drive letter and select **Properties**and then **Security.**
3. Click **Edit**and after that **Add…**



**Note:**Make sure that domain name matches your AD DS domain name, if it doesn’t the storage account has not been domain joined. When I tested this feature, sometimes takes 3-5 minutes, until storage account appear to be joined in Active Directory.

1. If prompted, enter admin credentials.
2. In the **Select Users, Computers, Service Accounts, or Groups**window select **Location** and choose **contoso.com,** then enter the name of the group **MSIXComputers** and select **OK.**
3. Verify that AD group with the computer accounts has **Read & execute** permissions.
4. Click **Apply**and if prompted by **Windows Security**confirm by pressing **Yes. Select OK.**

### **Task 10. Install public certificate on the VM from the host pool**

**Note: This task deploys signing certificate used to sign MSIX package. If you are using certificate issued from Public Certification Authority, you may skip this step**

1. Ensure that you are still remotely connected in **test-0** VM.
2. Open the browser and type the following URL:

<https://github.com/stgeorgi/msixappattach/blob/master/WVDContosoAppAcchCert/WVDContosoAppAttach.crt>

1. Select **Raw** button.
2. Select and copy every character by using **Ctrl+A** and **Ctrl+C.**
3. From start menu open **Notepad** and paste the text by using **Ctrl+V.**
4. Save the Notepad document on the desktop as **WVDSigning.crt**.

Note: Be sure that you select **Save as type**: **All Files** to be able to save with different extension.

1. Switch to the Desktop of the **test-0** VM.
2. Right click **WVDSigning** file and select **Install Certificate.**
3. On the **Welcome to the Certificate Import Wizard** select the checkbox for **Local Machine** and select **Next.**
4. On the **Certificate Store** page select the checkbox for **Place all certificates in the following store** and then select **Browse.**
5. On the **Select Certificate Store** select **Trusted Root Certification Authorities** and select **OK.**
6. Select **Next** and in the **Completing the Certificate Import Wizard** select **Finish.**
7. Verify that the message **The import was successful** appear.
8. Close the RDP connection for **test-0** VM.

Task 11. Upload MSIX image in the Azure File Share

Note:

For this task to test I’ve used one of the publicly available MSIX images prepared from Stefan Georgiev that are available on the following link:

<https://1drv.ms/u/s!Amut9BnVnw7mkOVMWy-sU8aiaStuxQ?e=AqwZ0D>

You have to download first locally, or if we go in production, we could host on some GitHub location. Decision still is no final.

1. On the Azure portal, search for and select **Storage Accounts.**
2. Select the account that you create for example **contoso-*yourname***  and then select **Storage Explorer (preview).**
3. On the Storage Explorer (preview) page, expand **FILE SHARES** and select your file share **msiximages.**
4. From the toolbar select **Upload** and select the previously downloaded MSIX image. Select to **Upload.**

Note: You can speed up the upload process if you have a locally installed Azure Storage Explorer.