Lab - Implement and manage Azure Virtual Desktop profiles (Microsoft Entra DS)

Student lab manual

Lab dependencies

- An Azure subscription
- A Microsoft account or a Microsoft Entra account with the Global Administrator role in the Microsoft Entra tenant associated with the Azure subscription and with the Owner or Contributor role in the Azure subscription
- A Azure Virtual Desktop environment provisioned in the lab **Introduction to Azure Virtual Desktop (Microsoft Entra DS)**

Estimated Time

30 minutes

Lab scenario

You need to implement Azure Virtual Desktop profile management in a Microsoft Entra DS environment.

Objectives

After completing this lab, you will be able to:

- Configure Azure Files to store profile containers for Azure Virtual Desktop in a Microsoft Entra DS environment
- Implement FSLogix based profiles for Azure Virtual Desktop in a Microsoft Entra DS environment

Lab files

- None

Instructions

Exercise 1: Implement FSLogix based profiles for Azure Virtual Desktop

The main tasks for this exercise are as follows:

1. Configure local Administrators group on Azure Virtual Desktop session host VMs
2. Configure FSLogix-based profiles on Azure Virtual Desktop session host VMs
3. Test FSLogix-based profiles with Azure Virtual Desktop
4. Delete Azure lab resources

Task 1: Configure local Administrators group on Azure Virtual Desktop session host VMs

1. From your lab computer, start a web browser, navigate to the Azure portal, and sign in by providing credentials of a user account with the Owner role in the subscription you will be using in this lab.

2. In the Azure portal, open the **Cloud Shell** pane by selecting the toolbar icon directly to the right of the search textbox.

3. If prompted to select either **Bash** or **PowerShell**, select **PowerShell**.

   > **Note**: If this is the first time you are starting **Cloud Shell** and you are presented with the **You have no storage mounted** message, select the subscription you are using in this lab, and select **Create storage**.

4. From the PowerShell session in the **Cloud Shell** pane, run the following to start the Azure Virtual Desktop session host Azure VMs you will be using in this lab:

   ```
   Get-AzVM -ResourceGroup 'az140-21a-RG' | Start-AzVM
   ```

   > **Note**: Wait until the Azure VMs are running before you proceed to the next step.

5. From the PowerShell session in the **Cloud Shell** pane, run the following to enable PowerShell Remoting on the Session Hosts.

   ```
   Get-AzVM -ResourceGroup 'az140-21a-RG' | Enable-AzVMPSRemoting
   ```

6. Close the Cloud Shell

7. From your lab computer, in the Azure portal, search for and select **Virtual machines** and, from the **Virtual machines** blade, select the **az140-cl-vm11a** entry. This will open the **az140-cl-vm11a** blade.

8. On the **az140-cl-vm11a** blade, select **Connect**, in the drop-down menu, select **Bastion**, on the **Bastion** tab of the **az140-cl-vm11a | Connect** blade, select **Use Bastion**.

9. When prompted, provde the following credentials and select **Connect**:

Setting	Value
User Name	**aadadmin1@adatum.com**
Password	Password previously configured

10. Within the Bastion session to **az140-cl-vm11a**, in the Start menu, navigate to the **Windows Administration Tools** folder, expand it, and select **Active Directory Users and Computers**.

11. In the **Active Directory Users and Computers** console, right-click the domain node, select **New**, followed by **Organizational Unit**, in the **New Object - Organizational Unit** dialog box, in the **Name** textbox, type **ADDC Users**, and select **OK**.

12. In the **Active Directory Users and Computers** console, right-click the **ADDC Users**, select **New**, followed by **Group**, in the **New Object - Group** dialog box, specify the following settings and select

OK:

Setting	Value
Group name	**Local Admins**
Group name (pre-Windows 2000)	**Local Admins**
Group scope	**Global**
Group type	**Security**

13. In the **Active Directory Users and Computers** console, display the properties of the **Local Admins** group, switch to the **Members** tab, select **Add**, in the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select**, type **aadadmin1;wvdaadmin1** and select **OK**.

14. Within the Bastion session to **az140-cl-vm11a**, in the Start menu, navigate to the **Windows Administration Tools** folder, expand it, and select **Group Policy Management**.

15. In the **Group Policy Management** console, navigate to the **AADDC Computers** OU, right-click the **AADDC Computers GPO** icon and select **Edit**.

16. In the **Group Policy Management Editor** console, expand **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, right-click **Restriced Groups**, and select **Add Group**.

17. In the **Add Group** dialog box, in the **Group** text box, select **Browse**, in the **Select Groups** dialog box, in the **Enter the object names to select**, type **Local Admins** and select **OK**.

18. Back in the **Add Group** dialog box, select **OK**.

19. In the **ADATUM\Local Admins Properties** dialog box, in the section labeled **This group is a member of**, select **Add**, in the **Group Membership** dialog box, type **Administrators**, select **OK**, and select **OK** again to finalize the change.

    > **Note**: Make sure to use the section labeled **This group is a member of**

20. Within the Bastion session to the az140-cl-vm11a Azure VM, start PowerShell ISE as Administrator and run the following to restart the two Azure Virtual Desktop hosts in order to trigger Group Policy processing:

    ```
    $servers = 'az140-21-p1-0','az140-21-p1-1'
    Restart-Computer -ComputerName $servers -Force -Wait
    ```

21. Wait for the script to complete. This should take about 3 minutes.

Task 2: Configure FSLogix-based profiles on Azure Virtual Desktop session host VMs

1. Within the Bastion session to **az140-cl-vm11a**, start a Remote Desktop session to **az140-21-p1-0** and, when prompted, sign in with the **ADATUM\wvdaadmin1** user name and the password you set when creating this user account.

> **Note**: If the RDP connection is unable to connect, use the Azure Portal to connect to the VM using Bastion.

2. Within the Remote Desktop session to **az140-21-p1-0**, start Microsoft Edge, browse to FSLogix download page, download FSLogix compressed installation binaries, extract them into the **C:\Source** folder, navigate to the **x64\Release** subfolder and use **FSLogixAppsSetup.exe** to install Microsoft FSLogix Apps with the default settings.

> **Note**: Installation of FXLogic might not be necessary, depending on whether the image already includes it. An FX Logix installation requires a reboot.

3. Within the Remote Desktop session to **az140-21-p1-0**, start **Windows PowerShell ISE** as administrator and, from the **Administrator: Windows PowerShell ISE** script pane, run the following to install the latest version of the PowerShellGet module (select **Yes** when prompted for confirmation):

```
[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12
Install-Module -Name PowerShellGet -Force -SkipPublisherCheck
```

4. From the **Administrator: Windows PowerShell ISE** console, run the following to install the latest version of the Az PowerShell module (select **Yes to All** when prompted for confirmation):

```
Install-Module -Name Az -AllowClobber -SkipPublisherCheck
```

5. From the **Administrator: Windows PowerShell ISE** console, run the following to modify the execution policy:

```
Set-ExecutionPolicy RemoteSigned -Force
```

6. From the **Administrator: Windows PowerShell ISE** console, run the following to sign in to your Azure subscription:

```
Connect-AzAccount
```

7. When prompted, sign in with the Microsoft Entra credentials of the user account with the Owner role in the subscription you are using in this lab.

8. From the **Administrator: Windows PowerShell ISE** script pane, run the following to retrieve the name of the Azure Storage account you configured earlier in this lab:

```
$resourceGroupName = 'az140-22a-RG'
$storageAccountName = (Get-AzStorageAccount -ResourceGroupName
```

```
$resourceGroupName)[0].StorageAccountName
```

9. Within the Remote Desktop session to **az140-21-p1-0**, from the **Administrator: Windows PowerShell ISE** script pane, run the following to configure profile registry settings:

```
$profilesParentKey = 'HKLM:\SOFTWARE\FSLogix'
$profilesChildKey = 'Profiles'
$fileShareName = 'az140-22a-profiles'
New-Item -Path $profilesParentKey -Name $profilesChildKey –Force
New-ItemProperty -Path $profilesParentKey\$profilesChildKey -Name 'Enabled'
-PropertyType DWord -Value 1
New-ItemProperty -Path $profilesParentKey\$profilesChildKey -Name
'VHDLocations' -PropertyType MultiString -Value
"\\$storageAccountName.file.core.windows.net\$fileShareName"
```

> **Note** If the command generates an error, continue on to next step.

10. Within the Remote Desktop session to **az140-21-p1-0**, right-click **Start**, in the right-click menu, select **Run**, in the **Run** dialog box, in the **Open** text box, type the following and select **OK** to launch the **Local Users and Groups** window:

```
lusrmgr.msc
```

11. In the **Local Users and Groups** console, note the four groups which names start with the **FSLogix** string:

    - FSLogix ODFC Exclude List
    - FSLogix ODFC Include List
    - FSLogix Profile Exclude List
    - FSLogix Profile Include List

12. In the **Local Users and Groups** console, double-click the **FSLogix Profile Include List** group enty, note that it includes the **\Everyone** group, and select **OK** to close the group **Properties** window.

13. In the **Local Users and Groups** console, double-click the **FSLogix Profile Exclude List** group enty, note that it does not include any group members by default, and select **OK** to close the group **Properties** window.

> **Note**: To provide consistent user experience, you need to install and configure FSLogix components on all Azure Virtual Desktop session hosts. You will perform this task in the unattended manner on the other session host in our lab environment.

14. Within the Remote Desktop session to **az140-21-p1-0**, from the **Administrator: Windows PowerShell ISE** script pane, run the following to install FSLogix components on the **az140-21-p1-1** session host:

```

```

```
$server = 'az140-21-p1-1'
$localPath = 'C:\Source\x64'
$remotePath = "\\$server\C$\Source\x64\Release"
Copy-Item -Path $localPath\Release -Destination $remotePath -Filter '*.exe'
-Force -Recurse
Invoke-Command -ComputerName $server -ScriptBlock {
   Start-Process -FilePath $using:localPath\Release\FSLogixAppsSetup.exe -
ArgumentList '/quiet' -Wait
}
```

15. Within the Remote Desktop session to **az140-21-p1-0**, start **Windows PowerShell ISE** as administrator and, from the **Administrator: Windows PowerShell ISE** script pane, run the following to configure profile registry settings on the **az140-21-p1-1** session host:

```
$profilesParentKey = 'HKLM:\SOFTWARE\FSLogix'
$profilesChildKey = 'Profiles'
$fileShareName = 'az140-22a-profiles'
Invoke-Command -ComputerName $server -ScriptBlock {
   New-Item -Path $using:profilesParentKey -Name $using:profilesChildKey –
Force
   New-ItemProperty -Path $using:profilesParentKey\$using:profilesChildKey -
Name 'Enabled' -PropertyType DWord -Value 1
   New-ItemProperty -Path $using:profilesParentKey\$using:profilesChildKey -
Name 'VHDLocations' -PropertyType MultiString -Value
"\\$storageAccountName.file.core.windows.net\$using:fileShareName"
}
```

> **Note**: Before you test the FSLogix-based profile functionality, you need to remove the locally cached profile of the ADATUM\wvdaadmin1 account you will be using for testing from the Azure Virtual Desktop session hosts you used in the previous lab.

16. Switch to the Bastion session to **az140-cl-vm11a**, within the Bastion session to **az140-cl-vm11a**, switch to the **Administrator: Windows PowerShell ISE** window and, from the **Administrator: Windows PowerShell ISE** script pane, run the following to remove the locally cached profile of the ADATUM\aaduser1 account:

```
$userName = 'aaduser1'
$servers = 'az140-21-p1-0','az140-21-p1-1'
Get-CimInstance -ComputerName $servers -Class Win32_UserProfile | Where-
Object { $_.LocalPath.split('\')[-1] -eq $userName } | Remove-CimInstance
```

Task 3: Test FSLogix-based profiles with Azure Virtual Desktop

1. Within the Bastion session to **az140-cl-vm11a**, switch to the Remote Desktop client.

2. Within the Bastion session to **az140-cl-vm11a**, in the **Remote Desktop** client window, in the list of applications, double-click **Command Prompt**, when prompted, provide the password, and verify that it launches a **Command Prompt** window.

   > **Note**: Initially, it might take a few minutes for the application to start, but subsequently, the application startup should be much faster.

3. In the upper left corner of the **Command Prompt** window, right-click the **Command Prompt** icon and, in the drop-down menu, select **Properties**.

4. In the **Command Prompt Properties** dialog box, select the **Font** tab, modify the size and font settings, and select **OK**.

5. From the **Command Prompt** window, type **logoff** and press the **Enter** key to sign out from the Remote Desktop session.

6. Within the Bastion session to **az140-cl-vm11a**, in the **Remote Desktop** client window, in the list of applications, double-click **SessionDesktop** and verify that it launches a Remote Desktop session.

7. Within the **SessionDesktop** session, right-click **Start**, in the right-click menu, select **Run**, in the **Run** dialog box, in the **Open** text box, type **cmd** and select **OK** to launch a **Command Prompt** window:

8. Verify that the **Command Prompt** window properties match those you set earlier in this task.

9. Within the **SessionDesktop** session, minimize all windows, right-click the desktop, in the right-click menu, select **New** and, in the cascading menu, select **Shortcut**.

10. On the **What item would you like to create a shortcut for?** page of the **Create Shortcut** wizard, in the **Type the location of the item** text box, type **Notepad** and select **Next**.

11. On the **What would you like to name the shortcut** page of the **Create Shortcut** wizard, in the **Type a name for this shortcut** text box, type **Notepad** and select **Finish**.

12. Within the **SessionDesktop** session, right-click **Start**, in the right-click menu, select **Shut down or sign out** and then, in the cascading menu, select **Sign out**.

13. Back in the Bastion session to **az140-cl-vm11a**, in the **Remote Desktop** client window, in the list of applications, and double-click **SessionDesktop** to start a new Remote Desktop session.

14. Within the **SessionDesktop** session, verify that the **Notepad** shortcut appears on the desktop.

15. Within the **SessionDesktop** session, right-click **Start**, in the right-click menu, select **Shut down or sign out** and then, in the cascading menu, select **Sign out**.

16. Switch to the Bastion session to **az140-cl-vm11a**, switch to the Microsoft Edge window displaying the Azure portal.

17. In the Microsoft Edge window displaying the Azure portal, navigate back to the **Storage accounts** blade and select the entry representing the storage account you created in the prevous exercise.

18. On the storage account blade, in the **File services** section, select **File shares** and then, in the list of file shares, select **az140-22a-profiles**.

19. On the **az140-22a-profiles** blade, select **Browse** and verify that its content includes a folder which name consists of a combination of the Security Identifier (SID) of the **ADATUM\aaduser1** account followed by the **_aaduser1** suffix.

20. Select the folder you identified in the previous step and note that it contains a single file named **Profile_aaduser1.vhd**.

Exercise 2: Delete Azure lab resources (Optional)

1. Remove Microsoft Entra DS deployment by following instructions described in Delete an Azure Active Directory Domain Services managed domain using the Azure portal.
2. Remove all Azure resource groups you provisioned in the Microsoft Entra DS labs of this course by following instructions described in Azure Resource Manager resource group and resource deletion.