Lab - Implement and manage storage for AVD (AD DS)

Student lab manual

Lab dependencies

- An Azure subscription you will be using in this lab.
- A Microsoft account or a Microsoft Entra account with the Owner or Contributor role in the Azure subscription you will be using in this lab and with the Global Administrator role in the Microsoft Entra tenant associated with that Azure subscription.
- The completed lab **Prepare for deployment of Azure Virtual Desktop (AD DS)**

Estimated Time

30 minutes

Lab scenario

You need to implement and manage storage for a Azure Virtual Desktop deployment in an AD DS environment.

Objectives

After completing this lab, you will be able to:

- Configure Azure Files to store profile containers for Azure Virtual Desktop

Lab files

- None

Instructions

Exercise 1: Configure Azure Files to store profile containers for Azure Virtual Desktop

The main tasks for this exercise are as follows:

1. Create an Azure Storage account
2. Create an Azure Files share
3. Enable AD DS authentication for the Azure Storage account
4. Configure the Azure Files RBAC-based permissions
5. Configure the Azure Files file system permissions

Task 1: Create an Azure Storage account

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, search for and select **Virtual machines** and, from the **Virtual machines** blade, select **az140-dc-vm11**.

3. On the **az140-dc-vm11** blade, select **Connect**, in the drop-down menu, select **Connect via Bastion**.

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

Setting	Value
User Name	**Student@adatum.com**
Password	**Pa55w.rd1234**

5. Within the Bastion session to **az140-dc-vm11**, start Microsoft Edge and navigate to the Azure portal. If prompted, sign in by using the Microsoft Entra credentials of the user account with the Owner role in the subscription you are using in this lab.

6. Within the Bastion session to **az140-dc-vm11**, in the Microsoft Edge window displaying the Azure portal, search for and select **Storage accounts** and, on the **Storage accounts** blade, select **+ Create**.

7. On the **Basics** tab of the **Create storage account** blade, specify the following settings (leave others with their default values):

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	create a **new** resource group called **az140-22-RG**
Storage account name	any globally unique name between 3 and 15 in length consisting of lower case letters and digits, starting with a letter
Region	the name of an Azure region hosting the Azure Virtual Desktop lab environment
Performance	**Standard**
Redundancy	**Geo-redundant storage (GRS)**
Make read access to data available in the event of regional unavailability	enabled

> **Note**: Make sure that the length of the storage account name does not exceed 15 characters. The name will be used to create a computer account in the Active Directory Domain Services (AD DS) domain that is integrated with the Microsoft Entra tenant associated with the Azure subscription containing the storage account. This will allow for AD DS-based authentication when accessing file shares hosted in this storage account.

8. On the **Basics** tab of the **Create storage account** blade, select **Review + Create**, wait for the validation process to complete, and then select **Create**.

> **Note**: Wait for the Storage account to be created. This should take about 2 minutes.

Task 2: Create an Azure Files share

1. Within the Bastion session to **az140-dc-vm11**, in the Microsoft Edge window displaying the Azure portal, navigate back to the **Storage accounts** blade and select the entry representing the newly created storage account.
2. On the storage account blade, in the **Data storage** section, select **File shares** and then select **+ File share**.
3. On the **New file share** blade, specify the following settings and select **Next : Backup >** (leave other settings with their default values):

Setting	Value
Name	**az140-22-profiles**
Access tier	**Transaction optimized**

4. On the **Backup** blade, deselect the **Enable backup** checkbox, select **Review + Create**, wait for the validation process to complete, and then select **Create**.

Task 3: Enable AD DS authentication for the Azure Storage account

1. Within the Bastion session to **az140-dc-vm11**, open another tab in the Microsoft Edge window, navigate to the Azure Files samples GitHub repository, download [the most recent version of the compressed **AzFilesHybrid.zip** PowerShell module, and extract its content into **C:\Allfiles\Labs\02** folder (create the folder if needed).
2. Within the Bastion session to **az140-dc-vm11**, start **Windows PowerShell ISE** as administrator and, from the **Administrator: Windows PowerShell ISE** script pane, run the following to remove the **Zone.Identifier** alternate data stream, which has a value of **3**, indicating that it was downloaded from the Internet:

```
Get-ChildItem -Path C:\Allfiles\Labs\02 -File -Recurse | Unblock-File
```

3. From the **Administrator: Windows PowerShell ISE** console, run the following to disable Windows Account Manager:

```
Update-AzConfig -EnableLoginByWam $false
```

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

```
Connect-AzAccount
```

5. When prompted, provide the credentials of an Entra ID user account with the Owner role in the subscription you are using in this lab.

6. From the **Administrator: Windows PowerShell ISE** script pane, run the following to set the variables necessary to run the subsequent script:

```
$subscriptionId = (Get-AzContext).Subscription.Id
$resourceGroupName = 'az140-22-RG'
$storageAccountName = (Get-AzStorageAccount -ResourceGroupName
$resourceGroupName)[0].StorageAccountName
```

7. From the **Administrator: Windows PowerShell ISE** script pane, run the following to create an AD DS computer object that represents the Azure Storage account you created earlier in this task and is used to implement its AD DS authentication:

> **Note**: If you receive an error when running this script block, ensure that you are in the same directory as the CopyToPSPath.ps1 script. Depending on how the files were extracted earlier in this lab, they might be in a sub-folder named AzFilesHybrid. In the PowerShell context, change directories to the folder using **cd AzFilesHybrid**.

```
Set-Location -Path 'C:\Allfiles\Labs\02'
.\CopyToPSPath.ps1
Import-Module -Name AzFilesHybrid
Join-AzStorageAccountForAuth `
   -ResourceGroupName $ResourceGroupName `
   -StorageAccountName $StorageAccountName `
   -DomainAccountType 'ComputerAccount' `
   -OrganizationalUnitDistinguishedName 'OU=WVDInfra,DC=adatum,DC=com'
```

8. From the **Administrator: Windows PowerShell ISE** script pane, run the following to verify that the AD DS authentication is enabled on the Azure Storage account:

```
$storageaccount = Get-AzStorageAccount -ResourceGroupName $resourceGroupName
-Name $storageAccountName
$storageAccount.AzureFilesIdentityBasedAuth.ActiveDirectoryProperties
$storageAccount.AzureFilesIdentityBasedAuth.DirectoryServiceOptions
```

9. Verify that that the output of the command `$storageAccount.AzureFilesIdentityBasedAuth.ActiveDirectoryProperties` returns `AD`, representing the directory service of the storage account, and that the output of the `$storageAccount.AzureFilesIdentityBasedAuth.DirectoryServiceOptions` command, representing the directory domain information, resembles the following format (the values of `DomainGuid`, `DomainSid`, and `AzureStorageSid` will differ):

```
DomainName        : adatum.com
NetBiosDomainName : adatum.com
ForestName        : adatum.com
DomainGuid        : 47c93969-9b12-4e01-ab81-1508cae3ddc8
DomainSid         : S-1-5-21-1102940778-2483248400-1820931179
AzureStorageSid   : S-1-5-21-1102940778-2483248400-1820931179-2109
```

10. Within the Bastion session to **az140-dc-vm11**, switch to the Microsoft Edge window displaying the Azure portal, on the blade displaying the storage account, select **File shares** and verify that the **Identity-based access** setting is **Configured**.

> **Note**: You might have to refresh the browser page for the change to be reflected within the Azure portal.

Task 4: Configure the Azure Files RBAC-based permissions

1. Within the Bastion session to **az140-dc-vm11**, in the Microsoft Edge window displaying the Azure portal, on the blade displaying properties of the storage account you created earlier in this exercise, in the vertical menu on the left side, in the **Data storage** section, select **File shares**.
2. On the **File shares** blade, in the list of shares, select the **az140-22-profiles** entry.
3. On the **az140-22-profiles** blade, in the vertical menu on the left side, select **Access Control (IAM)**.
4. On the **Access Control (IAM)** blade of the storage account, select **+ Add** and, in the drop-down menu, select **Add role assignment**,
5. On the **Add role assignment** blade, on the **Role** tab, specify the following settings and select **Next**:

Setting	Value
Job function role	**Storage File Data SMB Share Contributor**

6. On the **Add role assignment** blade, on the **Members** tab, click **+ Select members**, specify the following settings and click **Select**.

Setting	Value
Select	**az140-wvd-users**

7. On the **Add role assignment** blade, select **Review + assign**, and then select **Review + assign**.
8. On the **Access Control (IAM)** blade of the storage account, select **+ Add** and, in the drop-down menu, select **Add role assignment**,
9. On the **Add role assignment** blade, on the **Role** tab, specify the following settings and select **Next**:

Setting	Value
Job function role	**Storage File Data SMB Share Elevated Contributor**

10. On the **Add role assignment** blade, on the **Members** tab, click **+ Select members**, specify the following settings and click **Select**.

Setting	Value
Select	**az140-wvd-admins**

11. On the **Add role assignment** blade, select **Review + assign**, and then select **Review + assign**.

Task 5: Configure the Azure Files file system permissions

1. Within the Bastion session to **az140-dc-vm11**, switch to the **Administrator: Windows PowerShell ISE** window and, from the **Administrator: Windows PowerShell ISE** script pane, run the following to create a variable referencing the name and key of the storage account you created earlier in this exercise:

```
$resourceGroupName = 'az140-22-RG'
$storageAccount = (Get-AzStorageAccount -ResourceGroupName
$resourceGroupName)[0]
$storageAccountName = $storageAccount.StorageAccountName
$storageAccountKey = (Get-AzStorageAccountKey -ResourceGroupName
$resourceGroupName -Name $storageAccountName).Value[0]
```

2. From the **Administrator: Windows PowerShell ISE** script pane, run the following to create a drive mapping to the file share you created earlier in this exercise:

```
$fileShareName = 'az140-22-profiles'
net use Z: "\\$storageAccountName.file.core.windows.net\$fileShareName"
/u:AZURE\$storageAccountName $storageAccountKey
```

3. From the **Administrator: Windows PowerShell ISE** console, run the following to view the current file system permissions:

```
icacls Z:
```

> **Note**: By default, both **NT Authority\Authenticated Users** and **BUILTIN\Users** have permissions that would allow users read other users' profile containers. You will remove them and add minimum required permissions instead.

4. From the **Administrator: Windows PowerShell ISE** script pane, run the following to adjust the file system permissions to comply with the principle of least privilege:

```
$permissions = 'ADATUM\az140-wvd-admins'+':(F)'
cmd /c icacls Z: /grant $permissions
```

```
$permissions = 'ADATUM\az140-wvd-users'+':(M)'
cmd /c icacls Z: /grant $permissions
$permissions = 'Creator Owner'+':(OI)(CI)(IO)(M)'
cmd /c icacls Z: /grant $permissions
icacls Z: /remove 'Authenticated Users'
icacls Z: /remove 'Builtin\Users'
```

> **Note**: Alternatively, you could set permissions by using File Explorer.