# Lab - Implement and manage storage for AVD (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
- The completed lab **Prepare for deployment of Azure Virtual Desktop (Microsoft Entra DS)**

## Estimated Time

30 minutes

## Lab scenario

You need to implement and manage storage for a Azure Virtual Desktop deployment 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

## 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 Microsoft Entra DS authentication for the Azure Storage account
4. Configure the Azure Files share permissions
5. Configure the Azure Files directory and file level 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. 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.

3. 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**.

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

| Setting | Value |
|---|---|
| User Name | **aadadmin1@adatum.com** |
| Password | Password previously defined |

5. Within the Bastion session to the **az140-cl-vm11a** Azure VM, start Microsoft Edge, navigate to the Azure portal, and sign in by providing user principal name of the **aadadmin1** user account and the password you set when creating this account.

> **Note**: You can identify the user principal name (UPN) attribute of the **aadadmin1** account by reviewing its properties dialog box from the Active Directory Users and Computers console or by switching back to your lab computer and reviewing its properties from the Microsoft Entra tenant blade in the Azure portal.

6. Within the Bastion session to **az140-cl-vm11a**, 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 | the name of a new resource group **az140-22a-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 |
| Location | the name of an Azure region hosting the Azure Virtual Desktop lab environment |
| Performance | **Standard** |
| Replication | **Locally redundant storage (LRS)** |

> **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 two minutes.

#### Task 2: Create an Azure Files share

1. Within the Bastion session to **az140-cl-vm11a**, 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 vertical menu on the left side, 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 **Create** (leave other settings with their default values):

   | Setting | Value |
   |---|---|
   | Name | **az140-22a-profiles** |

#### Task 3: Enable Microsoft Entra DS authentication for the Azure Storage account

1. Within the Bastion session to **az140-cl-vm11a**, in the Microsoft Edge window, in the Azure portal, on the blade displaying the properties of the storage account you created in the previous task, in the vertical menu on the left side, in the **Data storage** section, select **File shares**.
2. In the **File share settings** section, next to the **Active Directory** label, select the **Not configured** link.
3. In the **Enable an Active Directory source** section, in the rectangle labeled **Azure Active Directory Domain Services**, select **Set up**.
4. On the **Identity-based access** blade, select the **Enabled** option, and select **Save**.

#### Task 4: Configure the Azure Files RBAC-based permissions

1. Within the Bastion session to **az140-cl-vm11a**, 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**, and in the list of shares, select the **az140-22a-profiles** entry.

2. On the **az140-22a-profiles** blade, in the vertical menu on the left side, select **Access Control (IAM)**.

3. On the **az140-22a-profiles | Access Control (IAM)** blade, select **+ Add** and, in the drop-down menu, select **Add role assignment**.

4. On the **Add role assignment** blade, select **Storage File Data SMB Share Contributor**, and select **Next**:

5. On the **Members** blade, select **Assign access to** and then click on **+ Select members**.

6. On the **Select Members** blade, in the **Select** text box, type **az140-wvd-ausers**, and then click **Select**.

7. On the **Members** blade, select **Review + assign** two times.

8. Repeat steps 3-8 above, specify the following settings:

| Setting | Value |
|---|---|
| Role | **Storage File Data SMB Share Elevated Contributor** |
| Select | **az140-wvd-aadmins** |

> **Note**: You will use the **aadadmin1** user account, which is a member of the **az140-wvd-aadmins** group to configure file share permissions.

#### Task 5: Configure the Azure Files directory and file level permissions

1. Within the Bastion session to **az140-cl-vm11a**, start **Command Prompt** and, from the **Command Prompt** window, run the following to map a drive to the target share (replace the `<storage-account-name>` placeholder with the name of the storage account):

```
net use Z: \\<storage-account-name>.file.core.windows.net\az140-22a-profiles
```

2. Within the Bastion session to **az140-cl-vm11a**, open File Explorer, navigate to the newly mapped Z: drive, display its **Properties** dialog box, select the **Security** tab, select **Edit**, select **Add**, in the **Select Users, Computers, Service Accounts, and Groups** dialog box, ensure that the **From this location** textbox contains the **adatum.com** entry, in the **Enter the object name to select** textbox, type **az140-wvd-ausers** and click **OK**.

3. Back on the **Security** tab of the dialog box displaying permissions of the mapped drive, ensure that the **az140-wvd-ausers** entry is selected, select the **Modify** checkbox in the **Allow** column, click **OK**, review the message displayed in the **Windows Security** text box, and click **Yes**.

4. Back on the **Security** tab of the dialog box displaying permissions of the mapped drive, select **Edit**, select **Add**, in the **Select Users, Computers, Service Accounts, and Groups** dialog box, ensure that the **From this location** textbox contains the **adatum.com** entry, in the **Enter the object name to select** textbox, type **az140-wvd-aadmins** and click **OK**.

5. Back on the **Security** tab of the dialog box displaying permissions of the mapped drive, ensure that the **az140-wvd-aadmins** entry is selected, select the **Full control** checkbox in the **Allow** column, and click **OK**.

6. On the **Security** tab of the dialog box displaying permissions of the mapped drive, select **Edit**, in the list of groups and user names, select the **Authenticated users** entry, and select **Remove**.

7. While still on the Edit screen, in the list of groups and user names, select the **Users** entry, select **Remove**, click **OK**, and then click **OK** twice to complete the process.

> **Note**: Alternatively, you could set permissions by using the **icacls** command-line utility.