Lab - Create and configure host pools and session hosts (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

60 minutes

Lab scenario

You need to create and configure host pools and session hosts in an Azure Active Directory Domain Services (Microsoft Entra DS) environment.

Objectives

After completing this lab, you will be able to:

- Configure an Azure Virtual Desktop environment in a Microsoft Entra DS domain.
- Validate Azure Virtual Desktop environment in a Microsoft Entra DS domain.

Lab files

- None

Instructions

Exercise 1: Configure an Azure Virtual Desktop environment

The main tasks for this exercise are as follows:

1. Prepare AD DS domain and the Azure subscription for deployment of an Azure Virtual Desktop host pool
2. Deploy an Azure Virtual Desktop host pool
3. Configure Azure Virtual Desktop application groups
4. Configure Azure Virtual Desktop workspaces

Task 1: Prepare AD DS domain and the Azure subscription for deployment of an Azure Virtual Desktop host pool

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 defined in the previous lab

5. Within the Bastion 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 with 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 displaying the Azure portal, open a PowerShell session in the **Cloud Shell** and run the following register the **Microsoft.DesktopVirtualization** resource provider:

```
Register-AzResourceProvider -ProviderNamespace Microsoft.DesktopVirtualization
```

7. Within the Bastion session to **az140-cl-vm11a**, in the Microsoft Edge displaying the Azure portal, search for and select **Virtual networks** and, from the **Virtual networks** blade, select the **az140-aadds-vnet11a** entry.

8. On the **az140-aadds-vnet11a** blade, select **Subnets**, on the **Subnets** blade, select **+ Subnet**, on the **Add subnet** blade, in the **Name** text box, type **hp1-Subnet**, leave all other settings with their default values, and select **Save**.

Task 2: Deploy an Azure Virtual Desktop host pool

1. Within the Bastion session to **az140-cl-vm11a**, in the Microsoft Edge window displaying the Azure portal, search for and select **Azure Virtual Desktop**, on the **Azure Virtual Desktop** blade, in the vertical menu on the left side, in the **Manage** section, select **Host pools** and, on the **Azure Virtual Desktop | Host pools** blade, select **+ Create**.

2. On the **Basics** tab of the **Create a host pool** blade, specify the following settings and select **Next: Virtual Machines >**:

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	the name of a new resource group **az140-21a-RG**
Host pool name	**az140-21a-hp1**
Location	the name of the Azure region into which you deployed the Microsoft Entra DS instance earlier in this lab
Validation environment	**No**
Preferred app group type	**Desktop**
Host pool type	**Pooled**
Max session limit	**12**
Load balancing algorithm	**Breadth-first**

> **Note**: If a user has both RemoteApp and Desktop apps published, the preferred app group type determines which of them will appear in their feed.

3. On the **Virtual machines** tab of the **Create a host pool** blade, specify the following settings (leave others with their defaults) and select **Next: Workspace >** (replace the *<Azure_AD_domain_name>* placeholder with the name of the Microsoft Entra tenant associated with the subscription into which you deployed the Microsoft Entra DS instance and replace the `<password>` placeholder with the password you set when creating the aadadmin1 account):

> **Note**: Ensure that you remember the password you used. You will need it later in this and subsequent labs.:

Setting	Value
Add virtual machines	**Yes**
Resource group	**Defaulted to same as host pool**
Name prefix	**az140-21-p1**
Virtual machine location	the name of the Azure region into which you deployed resources in the first exercise of this lab
Availability options	**No infrastructure redundancy required**
Security type	**Trusted launch virtual machines**

Setting	Value
Image	**Windows 11 Enterprise multi-session + Microsoft 365 Apps, version 22H2**
Virtual machine size	**Standard DC2s_v3**
Number of VMs	**2**
OS disk type	**Standard SSD**
Virtual network	**az140-aadds-vnet11a**
Subnet	**hp1-Subnet (10.10.1.0/24)**
Network security group	**Basic**
Public inbound ports	**No**
Select which directory you would like to join	**Active Directory**
AD domain join UPN	**aadadmin1@adatum.com**
Password	Use password for aadadmin1
Specify domain or unit	**Yes**
Domain to join	**adatum.com**
Organizational Unit path	**OU=AADDC Computers,DC=adatum,DC=com**
Virtual Machine Administrator account username	**student**
Virtual Machine Administrator account password	**Pa55w.rd1234**

4. On the **Workspace** tab of the **Create a host pool** blade, specify the following settings and select **Review + create**:

Setting	Value
Register desktop app group	**No**

5. On the **Review + create** tab of the **Create a host pool** blade, select **Create**.

> **Note**: Wait for the deployment to complete. This should take about 15 minutes.

Task 3: Configure Azure Virtual Desktop application groups

1. Within the Bastion session to **az140-cl-vm11a**, in the Azure portal, search for and select **Azure Virtual Desktop** and, on the **Azure Virtual Desktop** blade, select **Application groups**.

2. On the **Azure Virtual Desktop | Application groups** blade, select the auto-generated **az140-21a-hp1-DAG** desktop application group.

3. On the **az140-21a-hp1-DAG** blade, in the vertical menu on the left side, in the **Manage** section, select **Assignments**.
4. On the **az140-21a-hp1-DAG | Assignments** blade, select **+ Add**.
5. On the **Select Microsoft Entra users or user groups** blade, select **az140-wvd-apooled** and click **Select**.
6. Navigate back to the **Azure Virtual Desktop | Application groups** blade, and select **+ Create**.
7. On the **Basics** tab of the **Create an application group** blade, specify the following settings and select **Next: Applications >**:

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	**az140-21a-RG**
Host pool	**az140-21a-hp1**
Application group type	**RemoteApp**
Application group name	**az140-21a-hp1-Office365-RAG**

8. On the **Applications** tab of the **Create an application group** blade, select **+ Add applications**.
9. On the **Add application** blade, specify the following settings and select **Save**:

Setting	Value
Application source	**Start menu**
Application	**Word**
Description	**Microsoft Word**
Require command line	**No**

10. Back on the **Applications** tab of the **Create an application group** blade, select **+ Add applications**.
11. On the **Add application** blade, specify the following settings and select **Save**:

Setting	Value
Application source	**Start menu**
Application	**Excel**
Description	**Microsoft Excel**
Require command line	**No**

12. Back on the **Applications** tab of the **Create an application group** blade, select **+ Add applications**.
13. On the **Add application** blade, specify the following settings and select **Save**:

Setting	Value
Application source	**Start menu**
Application	**PowerPoint**
Description	**Microsoft PowerPoint**
Require command line	**No**

14. Back on the **Applications** tab of the **Create an application group** blade, select **Next: Assignments >**.

15. On the **Assignments** tab of the **Create an application group** blade, select **+ Add Microsoft Entra users or user groups**.

16. On the **Select Microsoft Entra users or user groups** blade, select **az140-wvd-aremote-app** and click **Select**.

17. Back on the **Assignments** tab of the **Create an application group** blade, select **Next: Workspace >**.

18. On the **Workspace** tab of the **Create a workspace** blade, specify the following setting and select **Review + create**:

Setting	Value
Register application group	**No**

19. On the **Review + create** tab of the **Create an application group** blade, select **Create**.

> **Note**: Now you will create an application group based on file path as the application source

20. Within the Bastion session to **az140-cl-vm11a**, in the web browser window displaying the Azure portal, search for and select **Azure Virtual Desktop** and, on the **Azure Virtual Desktop** blade, select **Application groups**.

21. On the **Azure Virtual Desktop | Application groups** blade, select **+ Create**.

22. On the **Basics** tab of the **Create an application group** blade, specify the following settings and select **Next: Applications >**:

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	**az140-21a-RG**
Host pool	**az140-21a-hp1**
Application group type	**RemoteApp**
Application group name	**az140-21a-hp1-Utilities-RAG**

23. On the **Applications** tab of the **Create an application group** blade, select **+ Add applications**.

24. On the **Add application** blade, specify the following settings and select **Save**:

Setting	Value
Application source	**File path**
Application path	**C:\Windows\system32\cmd.exe**
Application name	**Command Prompt**
Display name	**Command Prompt**
Icon path	**C:\Windows\system32\cmd.exe**
Icon index	**0**
Description	**Windows Command Prompt**
Require command line	**No**

25. Back on the **Applications** tab of the **Create an application group** blade, select **Next: Assignments >**.

26. On the **Assignments** tab of the **Create an application group** blade, select **+ Add Microsoft Entra users or user groups**.

27. On the **Select Microsoft Entra users or user groups** blade, select **az140-wvd-aremote-app** and **az140-wvd-aadmins** and click **Select**.

28. Back on the **Assignments** tab of the **Create an application group** blade, select **Next: Workspace >**.

29. On the **Workspace** tab of the **Create a workspace** blade, specify the following setting and select **Review + create**:

Setting	Value
Register application group	**No**

30. On the **Review + create** tab of the **Create an application group** blade, select **Create**.

Task 4: Configure Azure Virtual Desktop workspaces

1. Within the Bastion session to **az140-cl-vm11a**, in the Microsoft Edge window displaying the Azure portal, search for and select **Azure Virtual Desktop** and, on the **Azure Virtual Desktop** blade, select **Workspaces**.

2. On the **Azure Virtual Desktop | Workspaces** blade, select **+ Create**.

3. On the **Basics** tab of the **Create a workspace** blade, specify the following settings and select **Next: Application groups >**:

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	**az140-21a-RG**
Workspace name	**az140-21a-ws1**

Setting	Value
Friendly name	**az140-21a-ws1**
Location	the name of the Azure region into which you deployed resources in this lab

4. On the **Application groups** tab of the **Create a workspace** blade, specify the following settings:

Setting	Value
Register application groups	**Yes**

5. On the **Workspace** tab of the **Create a workspace** blade, select **+ Register application groups**.

6. On the **Add application groups** blade, select the plus sign next to the **az140-21a-hp1-DAG**, **az140-21a-hp1-Office365-RAG**, and **az140-21a-hp1-Utilities-RAG** entries and click **Select**.

7. Back on the **Application groups** tab of the **Create a workspace** blade, select **Review + create**.

8. On the **Review + create** tab of the **Create a workspace** blade, select **Create**.

Exercise 2: Validate Azure Virtual Desktop environment

The main tasks for this exercise are as follows:

1. Install Microsoft Remote Desktop client (MSRDC) on a Windows 10 computer
2. Subscribe to a Azure Virtual Desktop workspace
3. Test Azure Virtual Desktop apps

Task 1: Install Microsoft Remote Desktop client (MSRDC) on a Windows 10 computer

1. Within the Bastion session to **az140-cl-vm11a**, start Microsoft Edge and navigate to Windows Desktop client download page and, when prompted, run its installation by following prompts. Select the option **Install for all users on this machine**.
2. Once the installation completes, start the Remote Desktop client.

Task 2: Subscribe to a Azure Virtual Desktop workspace

1. In the **Remote Desktop** client window, select **Subscribe** and, when prompted, sign in with the **aaduser1** credentials (using its userPrincipalName attribute as the user name and the password you set when creating this account).

   > **Note**: Alternatively, in the **Remote Desktop** client window, select **Subscribe with URL**, in the **Subscribe to a Workspace** pane, in the **Email or Workspace URL**, type **https://rdweb.wvd.microsoft.com/api/arm/feeddiscovery**, select **Next**, and, once prompted, sign in with the **aaduser1** credentials (using its userPrincipalName attribute as the user name and **Pa55w.rd1234** as its password).

   > **Note**: The user principal name of **aaduser1** should be in the format **aaduser1@**<*Azure_AD_domain_name*>, where the <*Azure_AD_domain_name*> placeholder

> matches the name of the Microsoft Entra tenant associated with the subscription into which you deployed the Microsoft Entra DS instance.

2. In the **Stay signed in to all your apps** window, clear the checkbox **Allow my organization to manage my device** checkbox and select **No, sign in to this app only**.

3. Verify that the **Remote Desktop** page displays the SessionDesktop included in the auto-generated az140-21-hp1-DAG desktop application group published to the workspace and associated with the user account **aduser1** via its group membership.

   > **Note**: This is expected, because the **Preferred app group type** of the host pool is currently set to **Desktop**.

Task 3: Test Azure Virtual Desktop apps

1. 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.

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

   > **Note**: If you are presented with the **Welcome to Microsoft Teams** sign-in prompt, close it.

2. Within the **Session Desktop** session, right-click **Start**, select **Run**, in the **Open** text box of the **Run** dialog box, type **cmd** and select **OK**.

3. Within the **Session Desktop** session, at the Command Prompt, type **hostname** and press the **Enter** key to display the name of the computer on which the Remote Desktop session is running.

4. Verify that the displayed name is either **az140-21-p1-0**, **az140-21-p1-1** or **az140-21-p1-2**.

5. At the Command Prompt, type **logoff** and press the **Enter** key to log off from the Session Desktop.

   > **Note**: Next, you will modify the **Preferred app group type** by setting it to **RemoteApp**.

6. Within the Bastion session to **az140-cl-vm11a**, in the web browser window displaying the Azure portal, search for and select **Azure Virtual Desktop** and, on the **Azure Virtual Desktop** blade, in the vertical menu bar, in the **Manage section**, select **Host pools**.

7. On the **Azure Virtual Desktop | Host pools** blade, in the list of host pools, select **az140-21-hp1**.

8. On the **az140-21-hp1** blade, in the in the vertical menu bar, in the **Settings** section, select **Properties**, in the **Preferred app group type**, select **Remote App**, and then select **Save**.

9. Within the Bastion session to **az140-cl-vm11**, in the **Remote Desktop** client window, select the ellipsis symbol in the upper right corner and, in the drop-down menu, select **Refresh**.

10. Verify that the **Remote Desktop** page displays individual apps included in the two application groups you created and published to the workspace, which are also associated with the user account **aduser1** via its group membership.

> **Note**: This is expected, because the **Preferred app group type** of the host pool is now set to **RemoteApp**.

11. Within the Bastion session to **az140-cl-vm11a**, in the **Remote Desktop** client window, in the list of applications, double-click **Command Prompt** and verify that it launches a **Command Prompt** window. When prompted to authenticate, type the password you set when creating the **aduser1** user account, select the checkbox **Remember me**, and select **OK**.

12. At the Command Prompt, type **logoff** and press the **Enter** key to log off from the current Remote App session.

Exercise 3: Stop and deallocate Azure VMs provisioned and used in the lab

The main tasks for this exercise are as follows:

1. Stop and deallocate Azure VMs provisioned and used in the lab

> **Note**: In this exercise, you will deallocate the Azure VMs provisioned and used in this lab to minimize the corresponding compute charges

Task 1: Deallocate Azure VMs provisioned and used in the lab

1. Switch to the lab computer and, in the web browser window displaying the Azure portal, open the **PowerShell** shell session within the **Cloud Shell** pane.

2. From the PowerShell session in the Cloud Shell pane, run the following to list all Azure VMs created and used in this lab:

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

3. From the PowerShell session in the Cloud Shell pane, run the following to stop and deallocate all Azure VMs you created and used in this lab:

```
Get-AzVM -ResourceGroup 'az140-21a-RG' | Stop-AzVM -NoWait -Force
```

> **Note**: The command executes asynchronously (as determined by the -NoWait parameter), so while you will be able to run another PowerShell command immediately afterwards within the same PowerShell session, it will take a few minutes before the Azure VMs are actually stopped and deallocated.