Lab - Deploy host pools and session hosts by using the Azure portal (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

60 minutes

Lab scenario

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

Objectives

After completing this lab, you will be able to:

- Implement an Azure Virtual Desktop environment in an AD DS domain
- Validate an Azure Virtual Desktop environment in an AD DS domain

Lab files

- None

Instructions

Exercise 1: Implement an Azure Virtual Desktop environment in an AD DS domain

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. Manage the Azure Virtual Desktop host pool session hosts
4. Configure Azure Virtual Desktop application groups
5. 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. 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 **Bastion**, on the **Bastion** tab of the **az140-dc-vm11 | Connect** blade, select **Use Bastion**.
4. When prompted, provde the following credentials and select **Connect**:

Setting	Value
User Name	**Student**
Password	**Pa55w.rd1234**

5. Within the Bastion session to **az140-dc-vm11**, start **Windows PowerShell ISE** as administrator.
6. Within the Bastion session to **az140-dc-vm11**, from the **Administrator: Windows PowerShell ISE** console, run the following to create an organizational unit that will host the computer objects of the Azure Virtual Desktop hosts:

```
New-ADOrganizationalUnit 'WVDInfra' -path 'DC=adatum,DC=com' -
ProtectedFromAccidentalDeletion $false
```

7. From the **Administrator: Windows PowerShell ISE** console, run the following to identify the user principal name of the **aduser1** account:

```
(Get-AzADUser -DisplayName 'aduser1').UserPrincipalName
```

> **Note**: Record the user principal name you identified in this step. You will need it later in this lab.

8. From the **Administrator: Windows PowerShell ISE** console, run the following to register the **Microsoft.DesktopVirtualization** resource provider:

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

9. 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.

10. Within the Bastion session to **az140-dc-vm11**, in the Azure portal, use the **Search resources, services, and docs** text box at the top of the Azure portal page to search for and navigate to **Virtual networks** and, on the **Virtual networks** blade, select **az140-adds-vnet11**.

11. On the **az140-adds-vnet11** blade, select **Subnets**, on the **Subnets** blade, select **+ Subnet**, on the **Add subnet** blade, specify the following settings (leave all other settings with their default values) and click **Save**:

Setting	Value
Name	**hp1-Subnet**
Starting address	**10.0.1.0**
Size	**/24 (256 addresses)**

Task 2: Deploy an Azure Virtual Desktop host pool

1. Within the Bastion session to **az140-dc-vm11**, in the Microsoft Edge window displaying the Azure portal, search for and select **Azure Virtual Desktop**, on the **Azure Virtual Desktop** blade, 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 >** (leave other settings 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 **az140-21-RG**
Host pool name	**az140-21-hp1**
Location	the name of the Azure region into which you deployed resources in the first exercise of this lab or a region close to it
Validation environment	**No**
Preferred app group type	**Desktop**
Host pool type	**Pooled**
Load balancing algorithm	**Breadth-first**
Max session limit	**12**

> **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 and select **Next: Workspace >** (leave other settings with their default values):

Setting	Value
Add virtual machines	**Yes**
Resource group	**Defaulted to same as host pool**
Name prefix	**az140-21-p1**
Virtual machine type	Azure virtual machine
Virtual machine location	the name of the Azure region into which you deployed resources in the previous lab
Availability options	**No infrastructure redundancy required**
Security type	**Trusted launch virtual machines**
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**
OS disk size	**Default size (128GiB)**
Boot Diagnostics	**Enable with managed storage account (recommended)**
Virtual network	**az140-adds-vnet11**
Subnet	**hp1-Subnet (10.0.1.0/24)**
Network security group	**Basic**
Public inbound ports	**No**
Select which directory you would like to join	**Active Directory**
AD domain join UPN	**student@adatum.com**
Password	**Pa55w.rd1234**
Confirm password	**Pa55w.rd1234**
Specify domain or unit	**Yes**
Domain to join	**adatum.com**
Organizational Unit path	**OU=WVDInfra,DC=adatum,DC=com**
User name	**Student**
Password	**Pa55w.rd1234**

Setting	Value
Confirm password	**Pa55w.rd1234**

4. On the **Workspace** tab of the **Create a host pool** blade, confirm the following setting 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 might take about 10-15 minutes.

Task 3: Manage the Azure Virtual Desktop host pool session hosts

1. Within the Bastion session to **az140-dc-vm11**, 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**.
2. On the **Azure Virtual Desktop | Host pools** blade, in the list of host pools, select **az140-21-hp1**.
3. On the **az140-21-hp1** blade, in the in the vertical menu bar, in the **Manage** section, select **Session hosts** and verify that the pool consists of two hosts.
4. On the **az140-21-hp1 | Session hosts** blade, select **+ Add**.
5. On the **Basics** tab of the **Add virtual machines to a host pool** blade, review the preconfigured settings and select **Next: Virtual Machines**.
6. On the **Virtual Machines** tab of the **Add virtual machines to a host pool** blade, specify the following settings and select **Review + create** (leave others with their default settings):

Setting	Value
Resource group	**az140-21-RG**
Name prefix	**az140-21-p1**
Virtual machine location	the name of the Azure region into which you deployed the first two session host VMs
Availability options	**No infrastructure redundancy required**
Security type	**Trusted launch virtual machines**
Image	**Windows 11 Enterprise multi-session + Microsoft 365 Apps, version 22H2**
Number of VMs	**1**
OS disk type	**Standard SSD**

Setting	Value
OS disk size	**Default size (128GiB)**
Boot Diagnostics	**Enable with managed storage account (recommended)**
Virtual network	**az140-adds-vnet11**
Subnet	**hp1-Subnet (10.0.1.0/24)**
Network security group	**Basic**
Public inbound ports	**No**
Select which directory you would like to join	**Active Directory**
AD domain join UPN	**student@adatum.com**
Password	**Pa55w.rd1234**
Confirm password	**Pa55w.rd1234**
Specify domain or unit	**Yes**
Domain to join	**adatum.com**
Organizational Unit path	**OU=WVDInfra,DC=adatum,DC=com**
User name	**Student**
Password	**Pa55w.rd1234**
Confirm password	**Pa55w.rd1234**

> **Note**: As you likely noticed, it's possible to change the image and prefix of the VMs as you add session hosts to the existing pool. In general, this is not recommended unless you plan to replace all VMs in the pool.

7. On the **Review + create** tab of the **Add virtual machines to a host pool** blade, select **Create**

> **Note**: Wait for the deployment to complete before you proceed to the next task. This might take about 10 minutes.

Task 4: Configure Azure Virtual Desktop application groups

1. Within the Bastion session to **az140-dc-vm11**, 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**.

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

3. On the **az140-21-hp1-DAG** blade, select **Assignments**.

4. On the **az140-21-hp1-DAG | Assignments** blade, select **+ Add**.

5. On the **Select Microsoft Entra users or user groups** blade, select **Groups**, select **az140-wvd-pooled** and click **Select**.

6. Navigate back to the **Azure Virtual Desktop | Application groups** blade, 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	**az140-21-RG**
Host pool	**az140-21-hp1**
Application group type	**Remote App**
Application group name	**az140-21-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 **Review + add**, then select **Add**:

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 **Review + add**, then select **Add**:

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 **Review + add**, then select **Add**:

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 **Groups**, then select **az140-wvd-remote-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**: Wait for the Application Group to be created. This should take less than 1 minute.

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

20. Within the Bastion session to **az140-dc-vm11**, 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	**az140-21-RG**
Host pool	**az140-21-hp1**
Application group type	**RemoteApp**
Application group name	**az140-21-hp1-Utilities-RAG**

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

24. On the **Add application** blade, on the **Basics** tab, specify the following settings and select **Next**:

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

25. On the **Icon** tab, specify the following settings and select **Review + add**, then select **Add**:

Setting	Value
Icon path	**C:\Windows\system32\cmd.exe**
Icon index	0

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

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

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

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

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

Setting	Value
Register application group	**No**

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

Task 5: Configure Azure Virtual Desktop workspaces

1. Within the Bastion session to **az140-dc-vm11**, 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	**az140-21-RG**
Workspace name	**az140-21-ws1**
Friendly name	**az140-21-ws1**
Location	the name of the Azure region into which you deployed resources in the first exercise of this lab or a region close to it

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 **az140-21-hp1-DAG**, **az140-21-hp1-Office365-RAG**, and **az140-21-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-dc-vm11**, in the browser window displaying the Azure portal, search for and select **Virtual machines** and, on the **Virtual machines** blade, select the **az140-cl-vm11** entry.
2. On the **az140-cl-vm11** blade, scroll down to the **Operations** section and select **Run Command**.
3. On the **az140-cl-vm11 | Run command** blade, select **EnableRemotePS** and select **Run**.

> **Note**: Wait for the command to complete before you proceed to the next step. This might take about 1 minute. You may get red text errors addressing the Public profile being used and not the Domain profile, if so, you can ignore and go to the next step.

4. Within the Bastion session to **az140-dc-vm11**, from the **Administrator: Windows PowerShell ISE** script pane, run the following to add all members of the **ADATUM\az140-wvd-users** to the local **Remote Desktop Users** group on the Azure VM **az140-cl-vm11** running Windows 10 which you deployed in the lab **Prepare for deployment of Azure Virtual Desktop (AD DS)**.

```
$computerName = 'az140-cl-vm11'
Invoke-Command -ComputerName $computerName -ScriptBlock {Add-
LocalGroupMember -Group 'Remote Desktop Users' -Member 'ADATUM\az140-wvd-
users'}
```

5. Switch to your lab computer, from the lab computer, in the browser window displaying the Azure portal, search for and select **Virtual machines** and, on the **Virtual machines** blade, select the **az140-cl-vm11** entry.

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

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

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

> **Note** The initial sign-in may take 5-10 minutes to complete.

8. Within the Bastion session to **az140-cl-vm11**, start Microsoft Edge and navigate to Windows Desktop client download page and, when prompted, select **Run** to start its installation. On the **Installation Scope** page of the **Remote Desktop Setup** wizard, select the option **Install for all users of this machine** and click **Install**. If prompted by User Account Control for administrative credentials, authenticate by using the **ADATUM\Student** username with **Pa55w.rd1234** as its password.

9. Once the installation completes, ensure that the **Launch Remote Desktop when setup exits** checkbox is selected and click **Finish** to 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 **aduser1** credentials, by providing its userPrincipalName attribute that you identified earlier in this lab 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://client.wvd.microsoft.com/api/arm/feeddiscovery**, select **Next**, and, once prompted, sign in with the **aduser1** credentials (using its userPrincipalName attribute as the user name and the password you set when creating this account).

2. 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-vm11**, 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. From your lab computer, switch to the Bastion session to **az140-dc-vm11**.
7. Within the Bastion session to **az140-dc-vm11**, 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**.
8. On the **Azure Virtual Desktop | Host pools** blade, in the list of host pools, select **az140-21-hp1**.
9. 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**.
10. From your lab computer, switch to the Bastion session to **az140-cl-vm11**.
11. 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**.
12. 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**.

13. Within the Bastion session to **az140-cl-vm11**, 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**.

14. At the Command Prompt, type **hostname** and press the **Enter** key to display the name of the computer on which the Command Prompt is running.

> **Note**: Verify that the displayed name is **az140-21-p1-0**, **az140-21-p1-1** or **az140-21-p1-2**, rather than **az140-cl-vm11**.

15. 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 in the lab

The main tasks for this exercise are as follows:

1. Stop and deallocate Azure VMs provisioned in the lab

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

Task 1: Deallocate Azure VMs provisioned 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 in this lab:

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

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

```
Get-AzVM -ResourceGroup 'az140-21-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.